Muster

AWS Prescriptive Guidance

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Prescriptive Guidance: Muster

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

AWS Präskriptive Beratungsmuster

Die Prescriptive Guidance-Muster von Amazon Web Services (AWS) bieten step-by-step Anweisungen, Architektur, Tools und Code für die Implementierung bestimmter Cloud-Migrations-, Modernisierungs- und Bereitstellungsszenarien. Diese Muster, die von Fachexperten unter geprüft werden AWS, richten sich an Entwickler und praktische Anwender, die eine Migration zu planen oder gerade dabei sind, eine Migration zu vorzunehmen. AWS Sie unterstützen auch Benutzer, die bereits im Einsatz sind AWS und nach Möglichkeiten suchen, ihren Cloud-Betrieb zu optimieren oder zu modernisieren.

Sie können diese Muster verwenden, um Ihre lokalen oder Cloud-Workloads unterschiedlicher Komplexität in die Cloud zu verlagern AWS und Ihre Bemühungen um die Einführung, Optimierung und Modernisierung der Cloud zu beschleunigen, unabhängig davon, ob Sie sich in der Machbarkeitsnachweisphase, Planungs- oder Implementierungsphase Ihres Projekts befinden. Zum Beispiel für ein Cloud-Migrationsprojekt:

- In der Planungsphase können Sie die verschiedenen Optionen bewerten, zu denen Sie migrieren können AWS. Sie können das richtige Muster wählen, das Ihren Anforderungen entspricht, je nachdem, ob Sie umziehen, rehosten, eine neue Plattform oder eine neue Architektur einrichten möchten. Sie können sich auch mit den verschiedenen Tools vertraut machen, die für die Migration verfügbar sind, und mit der Planung der Lizenzbeschaffung beginnen oder erste Gespräche mit Anbietern aufnehmen.
- In der Machbarkeitsstudie und in der Implementierungsphase können Sie den step-by-step Anweisungen folgen, die in dem Muster für die Migration Ihres Workloads enthalten sind. AWS Jedes Muster enthält Details wie Voraussetzungen, Zielreferenzarchitekturen, Tools, step-by-step Aufgaben, bewährte Methoden, Problembehandlung und Code.
- Wenn Sie das bereits verwenden AWS Cloud, können Sie Muster finden, die Ihnen helfen, Ihre Nutzung von Cloud-Ressourcen zu modernisieren, zu optimieren, zu skalieren und zu sichern.

Verwenden Sie die folgenden Links oder die Filter- und Suchoptionen auf der AWS Prescriptive Guidance-Startseite, um nach technischen Bereichen aufgeschlüsselte Musterlisten aufzurufen.

- Analysen
- Produktivität des Unternehmens
- Cloud-nativ
- Container und Mikroservices

- Bereitstellung von Inhalten
- Kostenmanagement
- Datenseen
- Datenbanken
- DevOps
- Datenverarbeitung für Endbenutzer
- Hochleistungsrechnen
- Hybride Cloud
- Infrastruktur
- IoT
- Maschinelles Lernen und KI
- Großrechner
- Verwaltung und Unternehmensführung
- Nachrichtenübermittlung und Kommunikation
- Migration
- Modernisierung
- Netzwerkfunktionen
- Betriebssysteme
- Operationen
- SaaS
- Sicherheit, Identität, Compliance
- Serverless
- Softwareentwicklung und Testen
- Speicherung und Sicherung
- Web- und mobile Apps

Alle Veröffentlichungen, einschließlich Leitfäden, Strategien und Mustern, finden Sie auf der AWS Prescriptive Guidance-Startseite.

Analysen

Themen

- Analysieren von Amazon-Redshift-Daten in Microsoft SQL Server Analysis Services
- Analysieren und visualisieren Sie verschachtelte JSON-Daten mit Amazon Athena und Amazon QuickSight
- Automatisieren Sie die Durchsetzung von Verschlüsselungen in AWS Glue mithilfe einer CloudFormation AWS-Vorlage
- Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden
- Berechnen des Risikowerts (VaR) mithilfe von AWS-Services
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL
- Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL
- Tagging von Amazon-EMR-Clustern beim Start erzwingen
- Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Starten eines Spark-Auftrags in einem vorübergehenden EMR-Cluster mithilfe einer Lambda-Funktion
- Migrieren von Apache Cassandra-Workloads zu Amazon Keyspaces mithilfe von AWS Glue
- Migrieren Sie Oracle Business Intelligence 12c von On-Premises-Servern zur AWS Cloud
- Migrieren eines lokalen Apache-Kafka-Clusters zu Amazon MSK mithilfe von MirrorMaker
- Migrieren eines ELK-Stacks zu Elastic Cloud in AWS
- Migrieren von Daten in die AWS Cloud mithilfe von Starburst
- Optimieren Sie die ETL-Erfassung der Eingabedateigröße auf AWS
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- Führen Sie erweiterte Analysen mit Amazon Redshift ML durch
- Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden
- Richten Sie einen nutzbaren Mindestdatenraum ein, um Daten zwischen Organisationen gemeinsam zu nutzen

- Einrichten einer sprachspezifischen Sortierung für Amazon-Redshift-Abfrageergebnisse mithilfe einer skalaren Python-UDF
- Abonnieren einer Lambda-Funktion für Ereignisbenachrichtigungen aus S3-Buckets in verschiedenen AWS-Regionen
- Drei AWS Glue ETL-Auftragstypen für die Konvertierung von Daten in Apache Parquet
- Visualisieren von Amazon-Redshift-Prüfungsprotokollen mit Amazon Athena und Amazon QuickSight
- Visualisieren von IAM-Anmeldeinformationsberichten für alle AWS-Konten mit Amazon QuickSight
- Mehr Muster

Analysieren von Amazon-Redshift-Daten in Microsoft SQL Server Analysis Services

Erstellt von Sunil Vora (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Amazon Redshift	Ziel: Microsoft SQL Server Analysis Services
R-Typ: N/A	Workload: Microsoft	Technologien: Analytik
AWS-Services: Amazon Redshift		

Übersicht

Dieses Muster beschreibt, wie Sie Amazon-Redshift-Daten in Microsoft SQL Server Analysis Services verbinden und analysieren, indem Sie den Intellisoft OLE DB Provider oder den CData ADO.NET Provider für den Datenbankzugriff verwenden.

Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service in Petabytegröße in der Cloud. SQL Server Analysis Services ist ein Online Analytical Processing (OLAP)-Tool, mit dem Sie Daten aus Data Marts und Data Warehouses wie Amazon Redshift analysieren können. Sie können SQL Server Analysis Services verwenden, um OLAP-Kubiken aus Ihren Daten für eine schnelle, erweiterte Datenanalyse zu erstellen.

Voraussetzungen und Einschränkungen

Annahmen

- Dieses Muster beschreibt, wie SQL Server Analysis Services und Intellisoft OLE DB Provider oder CData ADO.NET Provider für Amazon Redshift auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance eingerichtet werden. Alternativ können Sie beide auf einem Host in Ihrem Unternehmensrechenzentrum installieren.

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon-Redshift-Cluster mit Anmeldeinformationen

Architektur

Quelltechnologie-Stack

- Ein Amazon-Redshift-Cluster

Zieltechnologie-Stack

- Microsoft SQL Server Analysis Services

Quell- und Zielarchitektur

Tools

- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft-OLE-DB-Anbieter für Amazon Redshift (Trial) oder CData-ADO.NET-Anbieter für Amazon Redshift (Trial)

Polen

Analysieren von Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die Tabellen und Daten, die importiert werden sollen.	Identifizieren Sie die zu importierenden Amazon-Redshift-Tabellen und ihre Größe.	DBA

Einrichten der EC2-Instance und Installieren von Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine EC2-Instance ein.	Erstellen Sie in Ihrem AWS-Konto eine EC2-Instance in einem privaten oder öffentlichen Subnetz.	Systemadministrator
Installieren Sie Tools für den Datenbankzugriff.	Laden Sie den Intellisoft OLE-DB-Anbieter für Amazon Redshift (oder den CData ADO.NET-Anbieter für Amazon Redshift) herunter und installieren Sie ihn.	Systemadministrator
Installieren Sie Visual Studio.	Laden Sie Visual Studio 2019 (Community Edition) herunter und installieren Sie es.	Systemadministrator
Installieren Sie Erweiterungen.	Installieren Sie die Microsoft Analysis Services Projects-Erweiterung in Visual Studio.	Systemadministrator
Ein Projekt zu erstellen.	Erstellen Sie ein neues tabellarisches Modellprojekt in Visual Studio, um Ihre Amazon-Redshift-Daten zu speichern. Wählen Sie in Visual Studio bei der Erstellung Ihres Projekts die Option Tabellarisches Projekt für Analyseservices aus.	DBA

Erstellen von Datenquellen und Importieren von Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon-Redshift-Datenquelle.	Erstellen Sie eine Amazon-Redshift-Datenquelle, indem Sie den Intellisoft OLE-DB-Anbieter für Amazon Redshift (oder den CData ADO.NET-Anbieter für Amazon Redshift) und Ihre Amazon-Redshift-Anmeldeinformationen verwenden.	Amazon Redshift, DBA
Importieren von Tabellen.	Wählen Sie Tabellen und Ansichten aus Amazon Redshift aus und importieren Sie sie in Ihr SQL Server Analysis Services-Projekt.	Amazon Redshift, DBA

Bereinigen nach der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die EC2-Instance.	Löschen Sie die EC2-Instance, die Sie zuvor gestartet haben.	Systemadministrator

Zugehörige Ressourcen

- Amazon Redshift (AWS-Dokumentation)
- Installieren von SQL Server Analysis Services (Microsoft-Dokumentation)
- Tabellarischer Model Designer (Microsoft-Dokumentation)
- Übersicht über OLAP-Kubikknoten für erweiterte Analysen (Microsoft-Dokumentation)
- Microsoft Visual Studio 2019 (Community Edition)

- Intellisoft OLE DB-Anbieter für Amazon Redshift (Test)
- CData ADO.NET Anbieter für Amazon Redshift (Trial)

Analysieren und visualisieren Sie verschachtelte JSON-Daten mit Amazon Athena und Amazon QuickSight

Erstellt von Anoop Singh (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik; Datenbanken	AWS-Dienste: Amazon Athena; Amazon QuickSight

Übersicht

Dieses Muster erklärt, wie eine verschachtelte Datenstruktur im JSON-Format mithilfe von Amazon Athena in eine tabellarische Ansicht übersetzt und die Daten anschließend in Amazon visualisiert werden. QuickSight

Sie können Daten im JSON-Format für API-gestützte Datenfeeds von Betriebssystemen verwenden, um Datenprodukte zu erstellen. Diese Daten können Ihnen auch dabei helfen, Ihre Kunden und deren Interaktionen mit Ihren Produkten besser zu verstehen, sodass Sie Benutzererlebnisse maßgeschneidert und Ergebnisse vorhersagen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine JSON-Datei, die eine verschachtelte Datenstruktur darstellt (dieses Muster bietet eine Beispieldatei)

Einschränkungen:

- JSON-Funktionen lassen sich gut in bestehende SQL-orientierte Funktionen in Athena integrieren. Sie sind jedoch nicht ANSI SQL-kompatibel, und es wird erwartet, dass die JSON-Datei jeden Datensatz in einer separaten Zeile enthält. Möglicherweise müssen Sie die `ignore.malformed.json` Eigenschaft in Athena verwenden, um anzugeben, ob falsch formatierte JSON-Datensätze in Nullzeichen umgewandelt werden sollen oder ob Fehler generiert werden sollen. Weitere Informationen finden Sie in der Athena-Dokumentation unter Bewährte Methoden zum Lesen von JSON-Daten.

- Dieses Muster berücksichtigt nur einfache und kleine Mengen von Daten im JSON-Format. Wenn Sie diese Konzepte in großem Umfang verwenden möchten, sollten Sie die Datenpartitionierung in Betracht ziehen und Ihre Daten in größeren Dateien konsolidieren.

Architektur

Das folgende Diagramm zeigt die Architektur und den Arbeitsablauf für dieses Muster. Die verschachtelten Datenstrukturen werden in Amazon Simple Storage Service (Amazon S3) im JSON-Format gespeichert. In Athena werden die JSON-Daten einer Athena-Datenstruktur zugeordnet. Anschließend erstellen Sie eine Ansicht, um die Daten zu analysieren und die Datenstruktur in zu visualisieren. QuickSight

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet Amazon S3 zum Speichern der JSON-Datei.
- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können. Dieses Muster verwendet Athena, um die JSON-Daten abzufragen und zu transformieren. Mit einigen Aktionen in der AWS Management Console können Sie Athena auf Ihre Daten in Amazon S3 verweisen und Standard-SQL verwenden, um einmalige Abfragen auszuführen. Athena ist serverlos, sodass keine Infrastruktur eingerichtet oder verwaltet werden muss, und Sie zahlen nur für die Abfragen, die Sie ausführen. Athena skaliert automatisch und führt Abfragen parallel aus, sodass die Ergebnisse auch bei großen Datensätzen und komplexen Abfragen schnell sind.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten auf einem einzigen Dashboard visualisieren, analysieren und melden können. QuickSight ermöglicht es Ihnen, auf einfache Weise interaktive Dashboards zu erstellen und zu veröffentlichen, die Erkenntnisse aus maschinellem Lernen (ML) enthalten. Sie können von jedem Gerät aus auf diese Dashboards zugreifen und sie in Ihre Anwendungen, Portale und Websites einbetten.

Beispiel-Code

Die folgende JSON-Datei bietet eine verschachtelte Datenstruktur, die Sie in diesem Muster verwenden können.


```
{
  "symbol": "AAPL",
  "financials": [
    {
      "reportDate": "2017-03-31",
      "grossProfit": 20591000000,
      "costOfRevenue": 32305000000,
      "operatingRevenue": 52896000000,
      "totalRevenue": 52896000000,
      "operatingIncome": 14097000000,
      "netIncome": 11029000000,
      "researchAndDevelopment": 2776000000,
      "operatingExpense": 6494000000,
      "currentAssets": 101990000000,
      "totalAssets": 334532000000,
      "totalLiabilities": 200450000000,
      "currentCash": 15157000000,
      "currentDebt": 13991000000,
      "totalCash": 67101000000,
      "totalDebt": 98522000000,
      "shareholderEquity": 134082000000,
      "cashChange": -1214000000,
      "cashFlow": 12523000000,
      "operatingGainsLosses": null
    }
  ]
}
```


Epen

Richten Sie einen S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Um einen Bucket zum Speichern der JSON-Datei zu erstellen, melden Sie sich bei der an AWS Managemen	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	t Console, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann Bucket erstellen. Weitere Informati onen finden Sie unter Bucket erstellen in der Amazon S3 S3-Dokumentation.	
Fügen Sie die verschachtelten JSON-Daten hinzu.	Laden Sie Ihre JSON-Datei in den S3-Bucket hoch. Eine JSON-Beispieldatei finden Sie im vorherigen Abschnitt . Anweisungen finden Sie unter Objekte hochladen in der Amazon S3 S3-Dokume ntation.	Systemadministrator

Analysieren Sie Daten in Athena

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle für die Zuordnung der JSON-Date n.	1. Öffnen Sie die Athena-Ko nsole. 2. Erstellen Sie eine Datenbank, indem Sie den Anweisungen in der Athena-Dokumentation folgen. 3. Wählen Sie im Datenbank menü die Datenbank aus, die Sie erstellt haben. 4. Geben Sie im Abfrage-E ditor eine `CREATE TABLE`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisung wie die folgende ein: `CREATE EXTERNAL TABLE financials_json (symbol string, financials array< struct<reportdate: string, grossprofit: bigint, totalrevenue: bigint, totalcash: bigint, totaldebt: bigint, researchanddevelopment: bigint>>) ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe' LOCATION 's3://s3bucket-for-athena/'`  wo `LOCATION` gibt den Speicherort des S3-Buckets an, der die JSON-Datei enthält. 5. Wählen Sie Ausführen, um die Tabelle zu erstellen. Weitere Informationen zum Erstellen von Tabellen finden Sie in der Athena-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ansicht für die Datenanalyse.	1. Öffnen Sie die Athena-Konsole. 2. Erstellen Sie eine Datenbank, indem Sie den Anweisungen in der Athena-Dokumentation folgen. 3. Wählen Sie im Datenbank menü die Datenbank aus, die Sie erstellt haben. 4. Geben Sie im Abfrage-Editor eine `CREATE VIEW` Anweisung wie die folgende ein: `CREATE OR REPLACE VIEW financial_json_view AS SELECT symbol, financials[1].reportdate one_report_date, -- indexes start with 1 financials[1].totalrevenue one_total_revenue, financials[1].reportdate another_report_date, financials[1].totalrevenue another_total_revenue FROM financials_json where symbol='AAPL' ORDER BY 1`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie Run (Ausführen), um die Ansicht zu erstellen. Weitere Informationen zum Erstellen von Ansichten finden Sie in der Athena-Dokumentation.	
Analysieren und validieren Sie die Daten.	1. Öffnen Sie die Athena-Konsole. 2. Führen Sie Abfragen im Abfrage-Editor mithilfe der Ansicht aus, die Sie im vorherigen Schritt erstellt haben. 3. Überprüfen Sie die Daten anhand der JSON-Datei, um sicherzustellen, dass Spaltennamen und Datentypen korrekt zugeordnet sind.	Developer

Visualisieren Sie Daten in QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Athena als Datenquelle in QuickSight ein.	1. Öffnen Sie die QuickSight-Konsole. 2. Wählen Sie Datensätze, Neuer Datensatz aus. 3. Wählen Sie Athena als Datenquelle.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie die Datenbank aus, die die von Ihnen erstellte Ansicht enthält. 5. Wählen Sie die Ansicht aus, für die Sie einen Datensatz erstellen möchten. 6. Wählen Sie auf der Seite Datensatzerstellung abschließen die Option Daten direkt abfragen aus. 7. Wählen Sie Visualize aus.	
Visualisieren Sie Daten in QuickSight.	1. Nachdem Sie den Datensatz visualisiert haben, wählen Sie die Grafiken im linken Bereich aus und wählen Sie Felder für den Datensatz aus. Weitere Informationen finden Sie im Tutorial in der QuickSight Dokumentation. 2. Speichern Sie die Änderungen an der Analyse. 3. Wählen Sie Dashboard veröffentlichen, um die von Ihnen erstellten Grafiken zu veröffentlichen.	Datenanalyst

Zugehörige Ressourcen

- Amazon Athena Athena-Dokumentation
- QuickSight Amazon-Tutorials

- Arbeiten mit verschachteltem JSON (Blogbeitrag)

Automatisieren Sie die Durchsetzung von Verschlüsselungen in AWS Glue mithilfe einer CloudFormation AWS-Vorlage

Erstellt von Diogo Guedes (AWS)

Quellcode-Repository: AWS Glue Encryption Enforcement	Umgebung: Produktion	Technologien: Analytik; Sicherheit, Identität, Compliance
Arbeitslast: Alle anderen Workloads	AWS-Dienste: Amazon EventBridge; AWS Glue; AWS KMS; AWS Lambda; AWS CloudFormation	

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe einer CloudFormation AWS-Vorlage die Durchsetzung von Verschlüsselungen in AWS Glue einrichten und automatisieren. Die Vorlage erstellt alle erforderlichen Konfigurationen und Ressourcen für die Durchsetzung der Verschlüsselung. Zu diesen Ressourcen gehören eine Erstkonfiguration, eine durch eine EventBridge Amazon-Regel erstellte präventive Kontrolle und eine AWS-Lambda-Funktion.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Berechtigungen zur Bereitstellung der CloudFormation Vorlage und ihrer Ressourcen

Einschränkungen

Diese Sicherheitskontrolle ist regional. Sie müssen die Sicherheitskontrolle in jeder AWS-Region bereitstellen, in der Sie die Durchsetzung der Verschlüsselung in AWS Glue einrichten möchten.

Architektur

Zieltechnologie-Stack

- Amazon CloudWatch Logs (von AWS Lambda)
- EventBridge Amazon-Regel
- CloudFormation AWS-Stapel
- AWS CloudTrail
- Von AWS Identity and Access Management (IAM) verwaltete Rolle und Richtlinie
- AWS Key Management Service (AWS KMS)
- AWS-KMS-Alias
- AWS Lambda-Funktion
- AWS Systems Manager Parameter Store

Zielarchitektur

Das folgende Diagramm zeigt, wie die Durchsetzung von Verschlüsselungen in AWS Glue automatisiert werden kann.

Das Diagramm zeigt den folgenden Workflow:

1. Eine CloudFormation Vorlage erstellt alle Ressourcen, einschließlich der Erstkonfiguration und der Erkennungskontrolle für die Durchsetzung der Verschlüsselung in AWS Glue.
2. Eine EventBridge Regel erkennt eine Statusänderung in der Verschlüsselungskonfiguration.
3. Eine Lambda-Funktion wird zur Auswertung und Protokollierung über Logs CloudWatch aufgerufen. Bei der Erkennung von Nichtkonformitäten wird der Parameter Store mit einem Amazon-Ressourcennamen (ARN) für einen AWS-KMS-Schlüssel wiederhergestellt. Der Service wird bei aktivierter Verschlüsselung auf den Status „konform“ zurückgesetzt.

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS verwenden, CloudFormation StackSets um diese Vorlage in mehreren Konten bereitzustellen, für die Sie die Durchsetzung der Verschlüsselung in AWS Glue aktivieren möchten.

Tools

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS CloudTrail unterstützt Sie dabei, Betriebs- und Risikoprüfungen, Governance und Compliance Ihres AWS-Kontos zu ermöglichen.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten.

Code

Der Code für dieses Muster ist im Repository GitHub aws-custom-guardrail-event-driven verfügbar.

Bewährte Methoden

AWS Glue unterstützt die Datenverschlüsselung im Ruhezustand für die Erstellung von Jobs in AWS Glue und die Entwicklung von Skripten mithilfe von Entwicklungsendpunkten.

Beachten Sie die folgenden bewährten Methoden:

- Konfigurieren Sie ETL-Jobs und Entwicklungsendpunkte so, dass sie AWS-KMS-Schlüssel verwenden, um verschlüsselte Daten im Ruhezustand zu schreiben.
- Verschlüsseln Sie die im AWS Glue Glue-Datenkatalog gespeicherten Metadaten mithilfe von Schlüsseln, die Sie über AWS KMS verwalten.
- Verwenden Sie AWS-KMS-Schlüssel, um Job-Lesezeichen und die von Crawlern und ETL-Jobs generierten Protokolle zu verschlüsseln.

Epen

Starten Sie die Vorlage CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Laden Sie die `aws-custom-guardrail-event-driven.yaml` Vorlage aus dem GitHub Repository herunter und stellen Sie sie dann bereit. Der `CREATE_COMPLETE` Status gibt an, dass Ihre Vorlage erfolgreich bereitgestellt wurde. Hinweis: Für die Vorlage sind keine Eingabeparameter erforderlich.	Cloud-Architekt

Überprüfen Sie die Verschlüsselungseinstellungen in AWS Glue

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-KMS-Schlüsselkonfigurationen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Glue-Konsole.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Katalogeinstellungen aus. 3. Vergewissern Sie sich, dass die Einstellungen Metadatenverschlüsselung und Verbindungskennwörter verschlüsseln gekennzeichnet und für die Verwendung konfiguriert sind. `KMSKeyGlue`	

Testen Sie die Durchsetzung der Verschlüsselung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Verschlüsselungseinstellung in CloudFormation.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 2. Wählen Sie im Navigationsbereich Stacks und dann Ihren Stack aus. 3. Wählen Sie die Registerkarte Resources (Ressourcen) aus. 4. Suchen Sie in der Tabelle Ressourcen nach der Verschlüsselungseinstellung nach der logischen ID.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Versetzen Sie die bereitgestellte Infrastruktur in einen Zustand, in dem sie nicht konform ist.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Katalogeinstellungen aus. 3. Deaktivieren Sie das Kontrollkästchen Metadatenverschlüsselung. 4. Deaktivieren Sie das Kontrollkästchen Verbindungskennwörter verschlüsseln. 5. Wählen Sie Speichern. 6. Aktualisieren Sie die AWS Glue Glue-Konsole. Die Guardrail erkennt den Status „Nicht konform“ in AWS Glue, nachdem Sie die Kontrollkästchen deaktiviert haben, und erzwingt dann die Einhaltung der Vorschriften, indem sie die Fehlkonfiguration der Verschlüsselung automatisch behebt. Daher sollten die Kontrollkästchen für die Verschlüsselung nach dem Aktualisieren der Seite erneut aktiviert werden.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudWatch Amazon-Dokumentation)
- Verschlüsselung in AWS Glue einrichten (AWS Glue Glue-Dokumentation)

Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden

Erstellt von Rohan Jamadagni (AWS) und Arunabha Datta (AWS)

Umgebung: Produktion	Technologien: Analytik; Datenseen; Speicherung und Sicherung	AWS-Services: Amazon Redshift; Amazon S3; AWS Glue; AWS Lambda

Übersicht

Dieses Muster enthält Anleitungen zur Konfiguration von Amazon Simple Storage Service (Amazon S3) für eine optimale Data-Lake-Leistung und zum anschließenden Laden inkrementeller Datenänderungen von Amazon S3 in Amazon Redshift mithilfe von AWS Glue, wobei Extraktions-, Transformations- und Ladevorgänge (ETL) ausgeführt werden.

Die Quelldateien in Amazon S3 können verschiedene Formate haben, darunter kommagetrennte Werte (CSV), XML- und JSON-Dateien. Dieses Muster beschreibt, wie Sie AWS Glue verwenden können, um die Quelldateien in ein kosten- und leistungsoptimiertes Format wie Apache Parquet zu konvertieren. Sie können Parquet-Dateien direkt von Amazon Athena und Amazon Redshift Spectrum aus abfragen. Sie können Parquet-Dateien auch in Amazon Redshift laden, sie aggregieren und die aggregierten Daten mit Verbrauchern teilen oder die Daten mithilfe von Amazon visualisieren. QuickSight

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Quell-Bucket mit den richtigen Rechten, der CSV-, XML- oder JSON-Dateien enthält.

Annahmen

- Die CSV-, XML- oder JSON-Quelldateien wurden bereits in Amazon S3 geladen und sind von dem Konto aus zugänglich, in dem AWS Glue und Amazon Redshift konfiguriert sind.

- Bewährte Methoden für das Laden der Dateien, das Teilen der Dateien, die Komprimierung und die Verwendung eines Manifests werden befolgt, wie in der Amazon Redshift Redshift-Dokumentation beschrieben.
- Die Struktur der Quelldatei ist unverändert.
- Das Quellsystem kann Daten in Amazon S3 aufnehmen, indem es der in Amazon S3 definierten Ordnerstruktur folgt.
- Der Amazon Redshift Redshift-Cluster erstreckt sich über eine einzige Availability Zone. (Diese Architektur ist angemessen, da AWS Lambda, AWS Glue und Amazon Athena serverlos sind.) Um eine hohe Verfügbarkeit zu gewährleisten, werden Cluster-Snapshots in regelmäßigen Abständen erstellt.

Einschränkungen

- Die Dateiformate sind auf diejenigen beschränkt, die derzeit von AWS Glue unterstützt werden.
- Downstream-Berichte in Echtzeit werden nicht unterstützt.

Architektur

Quelltechnologie-Stack

- S3-Bucket mit CSV-, XML- oder JSON-Dateien

Zieltechnologie-Stack

- S3-Datensee (mit partitioniertem Parquet-Dateispeicher)
- Amazon-Redshift

Zielarchitektur

Datenfluss

Tools

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice. Amazon S3 kann für eine Vielzahl von Speicherlösungen verwendet werden, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- AWS Lambda — Mit AWS Lambda können Sie Code ausführen, ohne Server bereitzustellen oder zu verwalten. AWS Lambda ist ein ereignisgesteuerter Service. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS-Services initiiert wird.
- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich. Mit Amazon Redshift können Sie Petabyte an strukturierten und halbstrukturierten Daten in Ihrem Data Warehouse und Ihrem Data Lake mithilfe von Standard-SQL abfragen.
- AWS Glue — AWS Glue ist ein vollständig verwalteter ETL-Service, der das Aufbereiten und Laden von Daten für Analysen erleichtert. AWS Glue erkennt Ihre Daten und speichert die zugehörigen Metadaten (z. B. Tabellendefinitionen und Schema) im AWS Glue Glue-Datenkatalog. Ihre katalogisierten Daten sind sofort durchsuchbar, können abgefragt werden und sind für ETL verfügbar.
- AWS Secrets Manager — AWS Secrets Manager erleichtert den Schutz und die zentrale Verwaltung von Geheimnissen, die für den Anwendungs- oder Servicezugriff benötigt werden. Der Service speichert Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse und macht es überflüssig, vertrauliche Informationen im Klartextformat fest zu codieren. Secrets Manager bietet auch eine Schlüsselrotation, um Sicherheits- und Compliance-Anforderungen zu erfüllen. Es verfügt über eine integrierte Integration für Amazon Redshift, Amazon Relational Database Service (Amazon RDS) und Amazon DocumentDB. Sie können Secrets mithilfe der Secrets Manager-Konsole, der Befehlszeilenschnittstelle (CLI) oder der Secrets Manager Manager-API und -SDKs speichern und zentral verwalten.
- Amazon Athena — Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von in Amazon S3 gespeicherten Daten vereinfacht. Athena ist serverlos und in AWS Glue integriert, sodass es die mit AWS Glue katalogisierten Daten direkt abfragen kann. Athena ist elastisch skaliert, um interaktive Abfrageleistung zu bieten.

Epen

Erstellen Sie die S3-Buckets und die Ordnerstruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Quellsysteme auf Datenstruktur und Attribute .	Führen Sie diese Aufgabe für jede Datenquelle aus, die zum Amazon S3 S3-Data Lake beiträgt.	Dateningenieur
Definieren Sie die Partitions- und Zugriffsstrategie.	Diese Strategie sollte auf der Häufigkeit der Datenerfassung, der Delta-Verarbeitung und den Nutzungsanforderungen basieren. Stellen Sie sicher, dass S3-Buckets nicht öffentlich zugänglich sind und dass der Zugriff nur durch spezifische, auf Servicerollen basierende Richtlinien gesteuert wird. Weitere Informationen finden Sie in der Amazon S3-Dokumentation.	Dateningenieur
Erstellen Sie separate S3-Buckets für jeden Datenquellentyp und einen separaten S3-Bucket pro Quelle für die verarbeiteten (Parquet-) Daten.	Erstellen Sie für jede Quelle einen separaten Bucket und anschließend eine Ordnerstruktur, die auf der Datenaufnahmefrequenz des Quellsystems basiert, z. B. `s3://source-system-name/date/hour` Erstellen Sie für die verarbeiteten (in das Parquet-Format konvertierten) Dateien eine ähnliche Struktur, z. B. `s3://source-proces`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sed-bucket/date/hour` Weitere Informationen zum Erstellen von S3-Buckets finden Sie in der Amazon S3 S3-Dokumentation.	

Erstellen Sie ein Data Warehouse in Amazon Redshift

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Amazon Redshift Redshift-Cluster mit den entsprechenden Parametergruppen und der Wartungs- und Sicherungsstrategie.	Verwenden Sie das Secrets Manager Manager-Datenbankgeheimnis für Administratoranmeldedaten, während Sie den Amazon Redshift Redshift-Cluster erstellen. Informationen zur Erstellung und Dimensionierung eines Amazon Redshift Redshift-Clusters finden Sie in der Amazon Redshift Redshift-Dokumentation und im Whitepaper Sizing Cloud Data Warehouses.	Dateningenieur
Erstellen Sie die IAM-Servicerolle und fügen Sie sie dem Amazon Redshift Redshift-Cluster hinzu.	Die Servicerolle AWS Identity and Access Management (IAM) gewährleistet den Zugriff auf Secrets Manager und die S3-Quell-Buckets. Weitere Informationen finden Sie in der AWS-Dokumentation zur Autorisierung und zum Hinzufügen einer Rolle.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Datenbank schema.	Folgen Sie den Best Practices von Amazon Redshift für das Tabellendesign. Wählen Sie je nach Anwendungsfall die geeigneten Sortier- und Verteilungsschlüssel sowie die bestmögliche Komprimie rungskodierung aus. Bewährte Methoden finden Sie in der AWS-Dokumentation.	Dateningenieur
Konfigurieren Sie das Workload-Management.	Konfigurieren Sie je nach Ihren Anforderungen Warteschlangen für Workload Management (WLM), Short Query Acceleration (SQA) oder Parallelitätsskalierung. Weitere Informationen finden Sie unter Implementieren des Workload-Managements in der Amazon Redshift Redshift-Dokumentation.	Dateningenieur

Erstellen Sie ein Geheimnis in Secrets Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein neues Geheimnis, um die Amazon Redshift Redshift-Anmeldein formationen in Secrets Manager zu speichern.	In diesem Secret werden die Anmeldeinformationen für den Admin-Benutzer sowie für einzelne Benutzer des Datenbankdienstes gespeiche rt. Anweisungen finden Sie in der Secrets Manager	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Manager-Dokumentation. Wählen Sie Amazon Redshift Cluster als geheimen Typ. Aktivieren Sie außerdem auf der Seite Secret Rotation die Rotation. Dadurch wird der entsprechende Benutzer im Amazon Redshift Redshift-Cluster erstellt und die Schlüsselgeheimnisse werden in definierten Intervallen rotiert.	
Erstellen Sie eine IAM-Richtlinie, um den Zugriff auf Secrets Manager einzuschränken.	Beschränken Sie den Secrets Manager Manager-Zugriff nur auf Amazon Redshift Redshift-Administratoren und AWS Glue.	Dateningenieur

AWS Glue konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie im AWS Glue Glue-Datenkatalog eine Verbindung für Amazon Redshift hinzu.	Anweisungen finden Sie in der AWS Glue Glue-Dokumentation.	Dateningenieur
Erstellen Sie eine IAM-Servicerolle für AWS Glue und fügen Sie sie hinzu, um auf Secrets Manager-, Amazon Redshift- und S3-Buckets zuzugreifen.	Weitere Informationen finden Sie in der AWS Glue Glue-Dokumentation.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den AWS Glue Glue-Datenkatalog für die Quelle.	Dieser Schritt beinhaltet die Erstellung einer Datenbank und der erforderlichen Tabellen im AWS Glue Glue-Datenkatalog. Sie können entweder einen Crawler verwenden, um die Tabellen in der AWS Glue Glue-Datenbank zu katalogisieren, oder sie als externe Amazon Athena Athena-Tabellen definieren. Sie können auch über den AWS Glue Glue-Datenkatalog auf die in Athena definierten externen Tabellen zugreifen. Weitere Informationen zur Definition des Datenkatalogs und zur Erstellung einer externen Tabelle in Athena finden Sie in der AWS-Dokumentation.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS Glue Glue-Job zur Verarbeitung von Quelldaten.	Bei dem AWS Glue Glue-Job kann es sich um eine Python-Shell handeln oder PySpark um die Quelldatendateien zu standardisieren, zu deduplizieren und zu bereinigen. Um die Leistung zu optimieren und zu vermeiden, dass der gesamte S3-Quell-Bucket abgefragt werden muss, partitionieren Sie den S3-Bucket nach Datum, aufgeschlüsselt nach Jahr, Monat, Tag und Stunde als Pushdown-Prädikat für den AWS Glue Glue-Job. Weitere Informationen finden Sie in der AWS Glue Glue-Dokumentation. Laden Sie die verarbeiteten und transformierten Daten im Parquet-Format in die verarbeiteten S3-Bucket-Partitionen. Sie können die Parquet-Dateien von Athena abfragen.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS Glue Glue-Job, um Daten in Amazon Redshift zu laden.	Der AWS Glue Glue-Job kann eine Python-Shell sein oder PySpark die Daten laden, indem die Daten aktualisiert werden, gefolgt von einer vollständigen Aktualisierung. Einzelheiten finden Sie in der AWS Glue Glue-Dokumentation und im Abschnitt Zusätzliche Informationen.	Dateningenieur
(Optional) Planen AWS Glue Glue-Jobs, indem Sie bei Bedarf Trigger verwenden.	Die inkrementelle Datenlast wird hauptsächlich durch ein Amazon S3 S3-Ereignis ausgelöst, das eine AWS Lambda Lambda-Funktion veranlasst, den AWS Glue Glue-Job aufzurufen. Verwenden Sie die triggerbasierte Planung von AWS Glue für alle Datenladungen, die eine zeitbasierte statt einer ereignisbasierten Planung erfordern.	Dateningenieur

Erstellen einer Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine mit dem IAM-Service verknüpfte Rolle für AWS Lambda, um auf S3-Buckets und den AWS Glue	Erstellen Sie eine mit dem IAM-Service verknüpfte Rolle für AWS Lambda mit einer Richtlinie zum Lesen von Amazon S3 S3-Objekten und	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Glue-Job zuzugreifen, und fügen Sie sie hinzu.	-Buckets und einer Richtlini e für den Zugriff auf die AWS Glue Glue-API, um einen AWS Glue Glue-Job zu starten. Weitere Informationen finden Sie im Knowledge Center.	
Erstellen Sie eine Lambda-Funktion, um den AWS Glue Glue-Job auf der Grundlage des definierten Amazon S3 S3-Ereignisses auszuführen.	Die Lambda-Funktion sollte durch die Erstellung der Amazon S3-Manifestdatei initiiert werden. Die Lambda-Funktion sollte den Speichero rt des Amazon S3 S3-Ordner s (z. B. source_bucket/ year/month/date/hour) als Parameter an den AWS Glue Glue-Job übergeben . Der AWS Glue Glue-Job verwendet diesen Parameter als Pushdown-Prädikat, um den Dateizugriff und die Auftragsverarbeitungsleistu ng zu optimieren. Weitere Informationen finden Sie in der AWS Glue Glue-Doku mentation.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon S3 S3-PUT-Objektereignis, um die Objekterstellung zu erkennen, und rufen Sie die entsprechende Lambda-Funktion auf.	Das Amazon S3 S3-PUT-Objektereignis sollte nur durch die Erstellung der Manifestdatei ausgelöst werden. Die Manifestdatei steuert die Lambda-Funktion und die Parallelität des AWS Glue Glue-Jobs und verarbeitet den Ladevorgang als Batch, anstatt einzelne Dateien zu verarbeiten, die in einer bestimmten Partition des S3-Quell-Buckets ankommen. Weitere Informationen finden Sie in der Lambda-Dokumentation.	Dateningenieur

Zugehörige Ressourcen

- Amazon S3 S3-Dokumentation
- AWS Glue Glue-Dokumentation
- Amazon Redshift Redshift-Dokumentation
- AWS Lambda
- Amazon Athena
- AWS Secrets Manager

Zusätzliche Informationen

Detaillierter Ansatz für Upsert und Complete Refresh

Upsert: Dies ist für Datensätze vorgesehen, die je nach geschäftlichem Anwendungsfall eine historische Aggregation erfordern. Folgen Sie je nach Ihren Geschäftsanforderungen einem der unter

Aktualisieren und Einfügen neuer Daten (Amazon Redshift Redshift-Dokumentation) beschriebenen Methoden.

Vollständige Aktualisierung: Dies ist für kleine Datensätze vorgesehen, für die keine historischen Aggregationen erforderlich sind. Folgen Sie einem der folgenden Ansätze:

1. Kürzen Sie die Amazon Redshift Redshift-Tabelle.
2. Lädt die aktuelle Partition aus dem Staging-Bereich

oder:

1. Erstellen Sie eine temporäre Tabelle mit aktuellen Partitionsdaten.
2. Löschen Sie die Amazon Redshift Redshift-Zieltabelle.
3. Benennen Sie die temporäre Tabelle in die Zieltabelle um.

Berechnen des Risikowerts (VaR) mithilfe von AWS-Services

Erstellt von Sumon Samanta (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik; Serverless	AWS-Services: Amazon Kinesis Data Streams; AWS Lambda ;Amazon SQS; Amazon ElastiCache

Übersicht

Dieses Muster beschreibt, wie Sie ein Value-at- Risk (VaR)-Berechnungssystem mithilfe von AWS-Services implementieren. In einer On-Premises-Umgebung verwenden die meisten VaR-Systeme eine große, dedizierte Infrastruktur und interne oder kommerzielle Rasterplanungssoftware, um Batchprozesse auszuführen. Dieses Muster bietet eine einfache, zuverlässige und skalierbare Architektur zur Verarbeitung der VaR-Verarbeitung in der AWS Cloud. Es erstellt eine Serverless-Architektur, die Amazon Kinesis Data Streams als Streaming-Service, Amazon Simple Queue Service (Amazon SQS) als verwalteten Warteschlangenservice, Amazon ElastiCache als Caching-Service und AWS Lambda verwendet, um Bestellungen zu verarbeiten und Risiken zu berechnen.

VaR ist ein statistisches Maß, mit dem Unternehmen und Risikomanager potenzielle Verluste in ihrem Portfolio über ein bestimmtes Zuverlässigkeitsniveau hinaus schätzen können. Die meisten VaR-Systeme umfassen die Ausführung einer großen Anzahl mathematischer und statistischer Berechnungen und die Speicherung der Ergebnisse. Diese Berechnungen erfordern erhebliche Rechenressourcen, sodass VaR-Batchprozesse in kleinere Gruppen von Rechenaufgaben aufgeteilt werden müssen. Die Aufteilung eines großen Batches in kleinere Aufgaben ist möglich, da diese Aufgaben größtenteils unabhängig sind (d. h. Berechnungen für eine Aufgabe hängen nicht von anderen Aufgaben ab).

Eine weitere wichtige Voraussetzung für eine VaR-Architektur ist die Skalierbarkeit der Datenverarbeitung. Dieses Muster verwendet eine Serverless-Architektur, die basierend auf der Rechenlast automatisch ab- oder abskaliert wird. Da der Batch- oder Online-Computing-Bedarf schwer vorherzusagen ist, ist eine dynamische Skalierung erforderlich, um den Prozess innerhalb der durch ein Service Level Agreement (SLA) auferlegten Frist abzuschließen. Außerdem sollte eine kostenoptimierte Architektur in der Lage sein, jede Rechenressource herunterzuskalieren, sobald die Aufgaben für diese Ressource abgeschlossen sind.

AWS-Services eignen sich gut für VaR-Berechnungen, da sie skalierbare Rechen- und Speicherkapazität, kostenoptimierte Analyseservices für die Verarbeitung und verschiedene Arten von Schedulern zur Ausführung Ihrer Risikomanagement-Workflows bieten. Außerdem zahlen Sie nur für die Rechen- und Speicherressourcen, die Sie in AWS nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eingabedateien, die von Ihren Geschäftsanforderungen abhängen. Ein typischer Anwendungsfall umfasst die folgenden Eingabedateien:
  - Marktdatendatei (Eingabe in die VaR-Berechnungs-Engine)
  - Handelsdatendatei (es sei denn, die Handelsdaten gelangen durch einen Stream).
  - Konfigurationsdatendatei (Modell- und andere statische Konfigurationsdaten)
  - Modelldateien der Berechnungs-Engine (quantitative Bibliotheken)
  - Zeitreihendatendatei (für historische Daten wie den Aktienkurs der letzten fünf Jahre)
- Wenn die Marktdaten oder andere Eingaben über einen Stream eingehen, richten Sie Amazon Kinesis Data Streams ein und Amazon Identity and Access Management (IAM)-Berechtigungen, die für das Schreiben in den Stream konfiguriert sind.

Dieses Muster erstellt eine Architektur, in der Handelsdaten aus einem Handelssystem in einen Kinesis-Datenstrom geschrieben werden. Anstatt einen Streaming-Service zu verwenden, können Sie Ihre Handelsdaten in kleinen Batchdateien speichern, sie in einem Amazon Simple Storage Service (Amazon S3)-Bucket speichern und ein Ereignis aufrufen, um mit der Verarbeitung der Daten zu beginnen.

Einschränkungen

- Die Kinesis-Datenstromsequenzierung ist für jeden Shard garantiert, sodass nicht garantiert wird, dass Handelsaufträge, die in mehrere Shards geschrieben werden, in derselben Reihenfolge wie Schreibvorgänge zugestellt werden.
- Das AWS Lambda-Laufzeitlimit beträgt derzeit 15 Minuten. (Weitere Informationen finden Sie unter Häufig gestellte Fragen zu Lambda.)

Architektur

Zielarchitektur

Das folgende Architekturdiagramm zeigt die AWS-Services und -Workflows für das Risikobewertungssystem.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Handelsstreams werden aus dem Bestellverwaltungssystem gestreamt.
2. Die Lambda-Funktion für das Vernetzen der Ticketposition verarbeitet die Bestellungen und schreibt konsolidierte Nachrichten für jeden Ticker in eine Risikowarteschlange in Amazon SQS .
3. Die Lambda-Funktion der Risikoberechnungs-Engine verarbeitet die Nachrichten von Amazon SQS , führt Risikoberechnungen durch und aktualisiert die VaR-Informationen zum Gewinn und Verlust (PnL) im Risiko-Cache in Amazon ElastiCache.
4. Die Lambda-Funktion für ElastiCache Lesedaten ruft die Risikoergebnisse von ab ElastiCache und speichert sie in einer Datenbank und einem S3-Bucket.

Weitere Informationen zu diesen Diensten und Schritten finden Sie im Abschnitt Telefonie.

Automatisierung und Skalierung

Sie können die gesamte Architektur mithilfe des AWS Cloud Development Kit (AWS CDK) oder AWS-CloudFormation Vorlagen bereitstellen. Die Architektur kann sowohl die Batchverarbeitung als auch die Intraday-Verarbeitung (Echtzeit) unterstützen.

Die Skalierung ist in die -Architektur integriert. Wenn mehr Handelstransaktionen in den Kinesis-Datenstrom geschrieben werden und auf die Verarbeitung warten, können zusätzliche Lambda-Funktionen aufgerufen werden, um diese Handelstransaktionen zu verarbeiten, und können dann nach Abschluss der Verarbeitung herunterskaliert werden. Die Verarbeitung über mehrere Amazon SQS-Quellschlangen zur Risikoberechnung ist ebenfalls eine Option. Wenn eine strikte Sortierung oder Konsolidierung über Warteschlangen hinweg erforderlich ist, kann die Verarbeitung nicht parallelisiert werden. Für einen - end-of-the-day Batch oder einen Mini-Intraday-Batch können die Lambda-Funktionen jedoch parallel verarbeiten und die Endergebnisse in speichern ElastiCache.

Tools

AWS-Services

- Amazon Aurora MySQL -Compatible Edition ist eine vollständig verwaltete, MySQL -kompatible relationale Datenbank-Engine, mit der Sie MySQL-Bereitstellungen einrichten, betreiben und skalieren können. Dieses Muster verwendet MySQL als Beispiel, aber Sie können jedes RDBMS-System zum Speichern von Daten verwenden.
- Amazon ElastiCache unterstützt Sie bei der Einrichtung, Verwaltung und Skalierung verteilter In-Memory-Cache-Umgebungen in der AWS Cloud.
- Amazon Kinesis Data Streams hilft Ihnen, große Streams von Datensätzen in Echtzeit zu sammeln und zu verarbeiten.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Dieses Muster bietet eine Beispielarchitektur für ein VaR-System in der AWS Cloud und beschreibt, wie Sie Lambda-Funktionen für VaR-Berechnungen verwenden können. Informationen zum Erstellen Ihrer Lambda-Funktionen finden Sie in den Codebeispielen in der Lambda-Dokumentation. Wenden Sie sich an AWS Professional Services, um Unterstützung zu erhalten.

Bewährte Methoden

- Halten Sie jede VaR-Datenverarbeitungsaufgabe so klein und leicht wie möglich. Experimentieren Sie mit unterschiedlichen Handelszahlen in jeder Rechenaufgabe, um zu sehen, welche am besten für Rechenzeit und Kosten optimiert ist.
- Speichern Sie wiederverwendbare Objekte in Amazon ElastiCache. Verwenden Sie ein Framework wie Apache Arrow, um Serialisierung und Deserialisierung zu reduzieren.

- Berücksichtigen Sie die Zeitbeschränkung von Lambda. Wenn Sie glauben, dass Ihre Datenverarbeitungsaufgaben 15 Minuten überschreiten könnten, versuchen Sie, sie in kleinere Aufgaben aufzuteilen, um das Lambda-Timeout zu vermeiden. Wenn dies nicht möglich ist, können Sie eine Container-Orchestrierungslösung mit AWS Fargate, Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Kubernetes Service (Amazon EKS) in Betracht ziehen.

Polen

Handelsfluss zum Risikosystem

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beginnen Sie mit dem Schreiben von Handelstr ansaktionen.	Neue, geküpfte oder teilweise gewährte Transaktionen werden aus dem Bestellve rwaltungssystem in einen Risikostrom geschrieben. Dieses Muster verwendet Amazon Kinesis als verwaltet en Streaming-Service. Der Hash des Tickers für Handelsaufträge wird verwendet, um Handelsau fträge über mehrere Shards hinweg zu platzieren.	Amazon Kinesis

Ausführen von Lambda-Funktionen für die Auftragsverarbeitung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Risikover arbeitung mit Lambda.	Führen Sie eine AWS Lambda-Funktion für die neuen Bestellungen aus. Basierend auf der Anzahl der ausstehenden Handelsau fträge wird Lambda automatis	Amazon Kinesis , AWS Lambda , Amazon ElastiCac he

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ch skaliert. Jede Lambda-In stance hat eine oder mehrere Bestellungen und ruft die neueste Position für jeden Ticker von Amazon ab ElastiCache. (Sie können eine CUSIP-ID, einen Kurvennam en oder einen Indexname n für andere Finanzprodukt als Schlüssel zum Speichern und Abrufen von Daten aus verwenden ElasticCache.) In werden ElastiCachedie Gesamtposition (Quantität) und das Schlüssel-Wert-Paar <ticker , Netzposition >, wobei die Netzposition der Skalierun gsfaktor ist, für jeden Ticker einmal aktualisiert.	

Schreiben von Nachrichten für jeden Ticker in die Warteschlange

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie konsolidierte Nachrichten in die Risikowar teschlange.	Schreiben Sie die Nachricht in eine Warteschlange. Dieses Muster verwendet Amazon SQS als verwalteten Warteschlangenservice. Eine einzelne Lambda-Instance kann zu einem bestimmte n Zeitpunkt einen Mini-Batc h von Handelsaufträgen erhalten, schreibt jedoch nur	Amazon SQS , AWS Lambda

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine einzige Nachricht für jeden Ticker in Amazon SQS . Es wird ein Skalierungsfaktor berechnet: (alte Netzposit ion + aktuelle Position)/alte Netzposition .	

Aufrufen einer Risiko-Engine

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Risikober echnungen.	Die Lambda-Funktion für die Risiko-Engine Lambda wird aufgerufen. Jede Position wird von einer einzelnen Lambda-Funktion verarbeit et. Zu Optimierungszwecken kann jede Lambda-Funktion jedoch mehrere Nachrichten von Amazon SQS verarbeiten.	Amazon SQS , AWS Lambda

Abrufen von Risikoergebnissen aus dem Cache

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie den Risiko-Cache ab und aktualisieren Sie ihn.	Lambda ruft die aktuelle Netzposition für jeden Ticker von ab ElastiCache. Es ruft auch ein VaR-Array für Gewinn und Verlust (PnL) für jeden Ticker aus ab ElastiCac he.	Amazon SQS , AWS Lambda , Amazon ElastiCache

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn das PnL-Array bereits vorhanden ist, aktualisiert die Lambda-Funktion das Array und VaR mit einer Skala, die aus der Amazon SQS-Nachr icht stammt, die von der Netz-Lambda-Funktion geschrieb en wurde. Wenn sich das PnL-Array nicht in befindet ElasticCache, werden eine neue PnL und VaR anhand simulierter Ticker-Preisreihen daten berechnet.	

Aktualisieren von Daten in Elastic Cache und Speichern in der Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die Risikoerg ebnisse.	Nachdem die VaR- und PnL-Nummern in aktualisiert wurden ElastiCache, wird alle fünf Minuten eine neue Lambda-Funktion aufgerufe n. Diese Funktion liest alle gespeicherten Daten aus ElastiCache und speichert sie in einer mit Aurora MySQL kompatiblen Datenbank und in einem S3-Bucket.	AWS Lambda, Amazon ElastiCache

Zugehörige Ressourcen

- Grundlegendes VaR-Framework

Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL

Quelle: Teradata Data Warehouse	Ziel: Amazon Redshift	R-Typ: Re-Architect
Umgebung: Produktion	Technologien: Analytik; Datenbanken; Migration	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon Redshift		

Übersicht

NORMALIZE ist eine Teradata-Erweiterung des ANSI SQL-Standards. Wenn eine SQL-Tabelle eine Spalte mit dem Datentyp PERIOD enthält, kombiniert NORMALIZE Werte, die sich in dieser Spalte treffen oder sich überschneiden, zu einer einzigen Periode, die mehrere einzelne Periodenwerte konsolidiert. Um NORMALIZE verwenden zu können, muss mindestens eine Spalte in der SQL SELECT-Liste den temporalen PERID-Datentyp von Teradata haben. Weitere Informationen zu NORMALIZE finden Sie in der Teradata-Dokumentation.

Amazon Redshift unterstützt NORMALIZE nicht, aber Sie können diese Funktionalität mithilfe der systemeigenen SQL-Syntax und der LAG-Fensterfunktion in Amazon Redshift implementieren. Dieses Muster konzentriert sich auf die Verwendung der Teradata NORMALIZE-Erweiterung mit der Bedingung ON MEETS OR OVERLAPS, dem beliebtesten Format. Es erklärt, wie diese Funktion in Teradata funktioniert und wie sie in die native SQL-Syntax von Amazon Redshift konvertiert werden kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse und Erfahrung mit Teradata SQL
- Wissen und Erfahrung mit Amazon Redshift

Architektur

Quelltechnologie-Stack

- Teradata-Datawarehouse

Zieltechnologie-Stack

- Amazon-Redshift

Zielarchitektur

Eine allgemeine Architektur für die Migration einer Teradata-Datenbank zu Amazon Redshift finden Sie im Muster Migrieren einer Teradata-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten. Die Migration konvertiert die Teradata NORMALIZE-Phrase nicht automatisch in Amazon Redshift SQL. Sie können diese Teradata-Erweiterung konvertieren, indem Sie die Richtlinien in diesem Muster befolgen.

Tools

Code

Sehen Sie sich die folgende Tabellendefinition in Teradata an, um das Konzept und die Funktionalität von NORMALIZE zu veranschaulichen:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          duration      PERIOD(DATE)
     );
```

Führen Sie den folgenden SQL-Code aus, um Beispieldaten in die Tabelle einzufügen:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  PERIOD(DATE '2010-01-10',
 DATE '2010-03-20') );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  PERIOD(DATE '2010-03-20',
 DATE '2010-07-15') );
```

```
INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  PERIOD(DATE
 '2010-06-15', DATE '2010-08-18') );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  PERIOD(DATE '2010-03-10',
 DATE '2010-07-20') );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  PERIOD(DATE
 '2020-05-10', DATE '2020-09-20') );

END TRANSACTION;
```

Ergebnisse:

```
select * from systest.project order by 1,2,3;

 *** Query completed. 4 rows found. 4 columns returned.
 *** Total elapsed time was 1 second.

     emp_id  project_name              dept_id  duration
-----------  --------------------  -----------  ------------------------
         10  First Phase                  1000  ('10/01/10', '10/03/20')
         10  First Phase                  2000  ('10/03/20', '10/07/15')
         10  Second Phase                 2000  ('10/06/15', '10/08/18')
         20  First Phase                  2000  ('10/03/10', '10/07/20')
         20  Second Phase                 1000  ('20/05/10', '20/09/20')
```

Anwendungsfall Teradata NORMALIZE

Fügen Sie nun die Teradata NORMALIZE SQL-Klausel zur SELECT-Anweisung hinzu:

```
SELECT NORMALIZE ON MEETS OR OVERLAPS emp_id, duration
FROM systest.project
ORDER BY 1,2;
```

Diese NORMALIZE-Operation wird für eine einzelne Spalte (emp_id) ausgeführt. Für emp_id=10 verschmelzen die drei sich überschneidenden Periodenwerte in der Angabe Dauer wie folgt zu einem einzigen Periodenwert:

```
     emp_id  duration
-----------  ------------------------
         10  ('10/01/10', '10/08/18')
         20  ('10/03/10', '10/07/20')
```

```
         20  ('20/05/10', '20/09/20')
```

Die folgende SELECT-Anweisung führt eine NORMALIZE-Operation für project_name und dept_id aus. Beachten Sie, dass die SELECT-Liste nur eine PERIOD-Spalte, nämlich die Dauer, enthält.

```
SELECT NORMALIZE project_name, dept_id, duration
FROM systest.project;
```

Ausgabe:

```
project_name              dept_id  duration
--------------------  -----------  ------------------------
First Phase                  1000  ('10/01/10', '10/03/20')
Second Phase                 1000  ('20/05/10', '20/09/20')
First Phase                  2000  ('10/03/10', '10/07/20')
Second Phase                 2000  ('10/06/15', '10/08/18')
```

Amazon Redshift Redshift-äquivalentes SQL

Amazon Redshift unterstützt derzeit den PERIOD-Datentyp in einer Tabelle nicht. Stattdessen müssen Sie ein Teradata PERIOD-Datenfeld wie folgt in zwei Teile unterteilen: start_date, end_date:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          start_date  DATE,
          end_date    DATE
     );
```

Fügen Sie Beispieldaten in die Tabelle ein:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  DATE '2010-01-10', DATE
 '2010-03-20' );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  DATE '2010-03-20', DATE
 '2010-07-15');

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  DATE '2010-06-15', DATE
 '2010-08-18' );
```

```
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  DATE '2010-03-10', DATE
 '2010-07-20' );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  DATE '2020-05-10', DATE
 '2020-09-20' );

END TRANSACTION;
```

Ausgabe:

```
 emp_id | project_name | dept_id | start_date |  end_date
--------+--------------+---------+------------+------------
     10 | First Phase  |    1000 | 2010-01-10 | 2010-03-20
     10 | First Phase  |    2000 | 2010-03-20 | 2010-07-15
     10 | Second Phase |    2000 | 2010-06-15 | 2010-08-18
     20 | First Phase  |    2000 | 2010-03-10 | 2010-07-20
     20 | Second Phase |    1000 | 2020-05-10 | 2020-09-20
(5 rows)
```

Um die NORMALIZE-Klausel von Teradata neu zu schreiben, können Sie die LAG-Fensterfunktion in Amazon Redshift verwenden. Diese Funktion gibt die Werte für eine Zeile mit einem bestimmten Offset über (vor) der aktuellen Zeile in der Partition zurück.

Sie können die LAG-Funktion verwenden, um jede Zeile zu identifizieren, mit der eine neue Periode beginnt, indem Sie ermitteln, ob eine Periode mit der vorherigen Periode übereinstimmt oder sich mit ihr überschneidet (0, wenn ja und 1, wenn nein). Wenn dieses Flag kumulativ zusammengefasst wird, stellt es eine Gruppen-ID bereit, die in der äußeren Group By-Klausel verwendet werden kann, um das gewünschte Ergebnis in Amazon Redshift zu erzielen.

Hier ist ein Beispiel für eine Amazon Redshift SQL-Anweisung, die LAG () verwendet:

```
SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project
ORDER BY 1,2;
```

Ausgabe:

```
 emp_id | start_date |  end_date  | groupstartflag
--------+------------+------------+----------------
```

```
     10 | 2010-01-10 | 2010-03-20 |              1
     10 | 2010-03-20 | 2010-07-15 |              0
     10 | 2010-06-15 | 2010-08-18 |              0
     20 | 2010-03-10 | 2010-07-20 |              1
     20 | 2020-05-10 | 2020-09-20 |              1
(5 rows)
```

Die folgende Amazon Redshift SQL-Anweisung normalisiert nur die Spalte emp_id:

```
SELECT T2.emp_id, MIN(T2.start_date) as new_start_date, MAX(T2.end_date) as
 new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY emp_id ORDER BY start_date ROWS
 UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.emp_id, T2.GroupID
ORDER BY 1,2;
```

Ausgabe:

```
 emp_id | new_start_date | new_end_date
--------+----------------+-------------------------------------
     10 | 2010-01-10     | 2010-08-18
     20 | 2010-03-10     | 2010-07-20
     20 | 2020-05-10     | 2020-09-20
(3 rows)
```

Die folgende Amazon Redshift SQL-Anweisung normalisiert die Spalten project_name und dept_id:

```
SELECT T2.project_name, T2.dept_id, MIN(T2.start_date) as new_start_date,
 MAX(T2.end_date) as new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY project_name, dept_id ORDER BY
 start_date ROWS UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT project_name, dept_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY project_name,
 dept_id ORDER BY start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
```

```
FROM systest.project ) T1
) T2
GROUP BY T2.project_name, T2.dept_id, T2.GroupID
ORDER BY 1,2,3;
```

Ausgabe:

```
 project_name | dept_id | new_start_date | new_end_date
--------------+---------+----------------+--------------
 First Phase  |    1000 | 2010-01-10     | 2010-03-20
 First Phase  |    2000 | 2010-03-10     | 2010-07-20
 Second Phase |    1000 | 2020-05-10     | 2020-09-20
 Second Phase |    2000 | 2010-06-15     | 2010-08-18
(4 rows)
```

Epen

NORMALIZE nach Amazon Redshift SQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihren Teradata-SQL-Code.	Verwenden Sie die NORMALIZE-Phrase entsprechend Ihren Bedürfnissen.	SQL Developer
Konvertieren Sie den Code in Amazon Redshift SQL.	Folgen Sie den Richtlinien im Abschnitt „Tools“ dieses Musters, um Ihren Code zu konvertieren.	SQL Developer
Führen Sie den Code in Amazon Redshift aus.	Erstellen Sie Ihre Tabelle, laden Sie Daten in die Tabelle und führen Sie Ihren Code in Amazon Redshift aus.	SQL Developer

Zugehörige Ressourcen

Referenzen

- Temporale Funktion „Teradata NORMALIZE“ (Teradata-Dokumentation)
- LAG-Fensterfunktion (Amazon Redshift Redshift-Dokumentation)
- Migrieren Sie zu Amazon Redshift (AWS-Website)
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift (AWS Prescriptive Guidance)
- Konvertieren Sie die Teradata RESET WHEN-Funktion auf Amazon Redshift SQL (AWS Prescriptive Guidance)

Tools

- AWS-Schemakonvertierungstool (AWS SCT)

Partner

- AWS-Kompetenzpartner für Migration

Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL

Quelle: Teradata Data Warehouse	Ziel: Amazon Redshift	R-Typ: Re-Architect
Umgebung: Produktion	Technologien: Analytik; Datenbanken; Migration	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon Redshift		

Übersicht

RESET WHEN ist eine Teradata-Funktion, die in analytischen Fensterfunktionen von SQL verwendet wird. Es ist eine Erweiterung des ANSI SQL-Standards. RESET WHEN bestimmt die Partition, über die eine SQL-Fensterfunktion ausgeführt wird, basierend auf einer bestimmten Bedingung. Wenn die Bedingung TRUE ergibt, wird eine neue, dynamische Unterpartition innerhalb der vorhandenen Fensterpartition erstellt. Weitere Informationen zu RESET WHEN finden Sie in der Teradata-Dokumentation.

Amazon Redshift unterstützt RESET WHEN in SQL-Fensterfunktionen nicht. Um diese Funktionalität zu implementieren, müssen Sie RESET WHEN in die native SQL-Syntax in Amazon Redshift konvertieren und mehrere verschachtelte Funktionen verwenden. Dieses Muster zeigt, wie Sie die Teradata RESET WHEN-Funktion verwenden und sie in die Amazon Redshift SQL-Syntax konvertieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse des Teradata Data Warehouse und seiner SQL-Syntax
- Gutes Verständnis von Amazon Redshift und seiner SQL-Syntax

Architektur

Quelltechnologie-Stack

- Teradata-Datawarehouse

Zieltechnologie-Stack

- Amazon-Redshift

Architektur

Eine allgemeine Architektur für die Migration einer Teradata-Datenbank zu Amazon Redshift finden Sie im Muster Migrieren einer Teradata-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten. Die Migration konvertiert die Teradata RESET WHEN-Phrase nicht automatisch in Amazon Redshift SQL. Sie können diese Teradata-Erweiterung konvertieren, indem Sie die Richtlinien im nächsten Abschnitt befolgen.

Tools

Code

Sehen Sie sich die folgende Tabellendefinition in Teradata an, um das Konzept von RESET WHEN zu veranschaulichen:

```
create table systest.f_account_balance
( account_id integer NOT NULL,
  month_id integer,
  balance integer )
unique primary index (account_id, month_id);
```

Führen Sie den folgenden SQL-Code aus, um Beispieldaten in die Tabelle einzufügen:

```
BEGIN TRANSACTION;
Insert Into systest.f_account_balance values (1,1,60);
Insert Into systest.f_account_balance values (1,2,99);
Insert Into systest.f_account_balance values (1,3,94);
Insert Into systest.f_account_balance values (1,4,90);
Insert Into systest.f_account_balance values (1,5,80);
Insert Into systest.f_account_balance values (1,6,88);
```

```
Insert Into systest.f_account_balance values (1,7,90);
Insert Into systest.f_account_balance values (1,8,92);
Insert Into systest.f_account_balance values (1,9,10);
Insert Into systest.f_account_balance values (1,10,60);
Insert Into systest.f_account_balance values (1,11,80);
Insert Into systest.f_account_balance values (1,12,10);
END TRANSACTION;
```

Die Beispieltabelle enthält die folgenden Daten:

account_id	month_id	Saldo
1	1	60
1	2	99
1	3	94
1	4	90
1	5	80
1	6	88
1	7	90
1	8	92
1	9	10
1	10	60
1	11	80
1	12	10

Nehmen wir an, Sie möchten für jedes Konto die Reihenfolge der aufeinanderfolgenden monatlichen Saldoerhöhungen analysieren. Wenn der Saldo eines Monats kleiner oder gleich dem Saldo des Vormonats ist, müssen Sie den Zähler auf Null zurücksetzen und neu starten.

Anwendungsfall Teradata RESET WHEN

Um diese Daten zu analysieren, verwendet Teradata SQL eine Fensterfunktion mit einem verschachtelten Aggregat und einer RESET WHEN-Phrase wie folgt:

```
SELECT account_id, month_id, balance,
 ( ROW_NUMBER() OVER (PARTITION BY account_id ORDER BY month_id
RESET WHEN balance <= SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS
 BETWEEN 1 PRECEDING AND 1 PRECEDING) ) -1 ) as balance_increase
FROM systest.f_account_balance
ORDER BY 1,2;
```

Ausgabe:

account_id	month_id	Saldo	gleichgewicht_erhöhen
1	1	60	0
1	2	99	1
1	3	94	0
1	4	90	0
1	5	80	0
1	6	88	1
1	7	90	2
1	8	92	3
1	9	10	0
1	10	60	1
1	11	80	2
1	12	10	0

Die Abfrage wird in Teradata wie folgt verarbeitet:

1. Die Aggregatfunktion SUM (Saldo) berechnet die Summe aller Salden für ein bestimmtes Konto in einem bestimmten Monat.
2. Wir prüfen, ob ein Saldo in einem bestimmten Monat (für ein bestimmtes Konto) höher ist als der Saldo des Vormonats.
3. Wenn der Saldo gestiegen ist, erfassen wir einen kumulierten Zählwert. Wenn die Bedingung RESET WHEN als falsch ausgewertet wird, was bedeutet, dass der Saldo in aufeinanderfolgenden Monaten gestiegen ist, erhöhen wir die Anzahl weiter.
4. Die geordnete analytische Funktion ROW_NUMBER () berechnet den Zählwert. Wenn wir einen Monat erreichen, dessen Saldo kleiner oder gleich dem Saldo des Vormonats ist, wird die RESET WHEN-Bedingung als wahr ausgewertet. Falls ja, starten wir eine neue Partition und ROW_NUMBER () setzt die Zählung bei 1 neu an. Wir verwenden ROWS BETWEEN 1 PREVIODING UND 1 PREVIODING, um auf den Wert der vorherigen Zeile zuzugreifen.
5. Wir subtrahieren 1, um sicherzustellen, dass der Zählwert mit 0 beginnt.

SQL entspricht Amazon Redshift

Amazon Redshift unterstützt die RESET WHEN-Phrase in einer SQL-Analysefensterfunktion nicht. Um dasselbe Ergebnis zu erzielen, müssen Sie Teradata SQL mithilfe der nativen SQL-Syntax von Amazon Redshift und verschachtelten Unterabfragen wie folgt neu schreiben:

```
SELECT account_id, month_id, balance,
   (ROW_NUMBER() OVER(PARTITION BY account_id, new_dynamic_part ORDER BY month_id) -1)
 as balance_increase
FROM
( SELECT account_id, month_id, balance, prev_balance,
SUM(dynamic_part) OVER (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN
 UNBOUNDED PRECEDING AND CURRENT ROW) As new_dynamic_part
FROM ( SELECT account_id, month_id, balance,
SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN 1 PRECEDING
 AND 1 PRECEDING) as prev_balance,
(CASE When balance <= prev_balance Then 1 Else 0 END) as dynamic_part
FROM systest.f_account_balance ) A
) B
ORDER BY 1,2;
```

Da Amazon Redshift keine Funktionen für verschachtelte Fenster in der SELECT-Klausel einer einzelnen SQL-Anweisung unterstützt, müssen Sie zwei verschachtelte Unterabfragen verwenden.

- In der inneren Unterabfrage (Alias A) wird ein dynamischer Partitionsindikator (dynamic_part) erstellt und gefüllt. dynamic_part wird auf 1 gesetzt, wenn der Saldo eines Monats kleiner oder gleich dem Saldo des Vormonats ist. Andernfalls wird er auf 0 gesetzt.
- In der nächsten Ebene (Alias B) wird ein new_dynamic_part-Attribut als Ergebnis einer SUM-Fensterfunktion generiert.
- Schließlich fügen Sie new_dynamic_part als neues Partitionsattribut (dynamische Partition) zum vorhandenen Partitionsattribut (account_id) hinzu und wenden dieselbe Fensterfunktion ROW_NUMBER () wie in Teradata an (und minus eins).

Nach diesen Änderungen generiert Amazon Redshift SQL dieselbe Ausgabe wie Teradata.

Epen

RESET WHEN nach Amazon Redshift SQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihre Teradata-Fensterfunktion.	Verwenden Sie je nach Bedarf verschachtelte Aggregate und die RESET WHEN-Phrase.	SQL Developer
Konvertieren Sie den Code in Amazon Redshift SQL.	Folgen Sie den Richtlinien im Abschnitt „Tools“ dieses Musters, um Ihren Code zu konvertieren.	SQL Developer
Führen Sie den Code in Amazon Redshift aus.	Erstellen Sie Ihre Tabelle, laden Sie Daten in die Tabelle und führen Sie Ihren Code in Amazon Redshift aus.	SQL Developer

Zugehörige Ressourcen

Referenzen

- RESET WHEN-Phrase (Teradata-Dokumentation)
- Erklärung RESET WHEN (Stack Overflow)

- Zu Amazon Redshift migrieren (AWS-Website)
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift (AWS Prescriptive Guidance)
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL (AWS Prescriptive Guidance)

Tools

- AWS-Schemakonvertierungstool (AWS SCT)

Partner

- AWS-Kompetenzpartner für Migration

Tagging von Amazon-EMR-Clustern beim Start erzwingen

Erstellt von Priyanka Chaudhary (AWS)

Umgebung: Produktion	Technologien: Analytik; Sicherheit, Identität, Compliance	AWS-Services: Amazon EMR; AWS Lambda; Amazon CloudWatch Events

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die sicherstellt, dass Amazon-EMR-Cluster beim Erstellen markiert werden.

Amazon EMR ist ein Amazon Web Services (AWS)-Service zur Verarbeitung und Analyse riesiger Datenmengen. Amazon EMR bietet einen erweiterbaren Service mit geringer Konfiguration als einfachere Alternative zur Ausführung von internem Cluster-Computing. Sie können das Tagging verwenden, um AWS-Ressourcen auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung . Sie können Ihre Amazon-EMR-Cluster beispielsweise markieren, indem Sie jedem Cluster benutzerdefinierte Metadaten zuweisen. Ein Tag besteht aus einem Schlüssel und einem Wert, den Sie definieren. Wir empfehlen Ihnen, einheitliche Tags zu erstellen, um die Anforderungen Ihrer Organisation zu erfüllen. Wenn Sie einem Amazon-EMR-Cluster ein Tag hinzufügen, wird das Tag auch an jede aktive Amazon Elastic Compute Cloud (Amazon EC2)-Instance weitergegeben, die dem Cluster zugeordnet ist. Wenn Sie ein Tag aus einem Amazon-EMR-Cluster entfernen, wird dieses Tag ebenfalls aus jeder zugehörigen, aktiven EC2-Instance entfernt.

Die detektivische Kontrolle überwacht API-Aufrufe und initiiert ein Amazon CloudWatch Events-Ereignis für die APIs RunJobFlow, AddTagsRemoveTags, und CreateTags APIs. Das Ereignis ruft AWS Lambda auf, das ein Python-Skript ausführt. Die Python-Funktion ruft die Amazon-EMR-Cluster-ID aus der JSON-Eingabe aus dem Ereignis ab und führt die folgenden Prüfungen durch:

- Überprüfen Sie, ob der Amazon-EMR-Cluster mit von Ihnen angegebenen Tag-Namen konfiguriert ist.
- Wenn nicht, senden Sie eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung mit den relevanten Informationen an den Benutzer: Amazon EMR-Clustername, Details zu Verstößen, AWS-Region, AWS-Konto und Amazon-Ressourcenname (ARN) für Lambda, aus denen diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket zum Hochladen des bereitgestellten Lambda-Codes. Oder Sie können zu diesem Zweck einen S3-Bucket erstellen, wie im Abschnitt „Pics“ beschrieben.
- Eine aktive E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- Eine Liste obligatorischer Tags, nach denen Sie suchen möchten.

Einschränkungen

- Diese Sicherheitskontrolle ist regional. Sie müssen sie in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Produktversionen

- Amazon-EMR-Version 4.8.0 und höher.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre

Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.

- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.
- Amazon EMR – Amazon EMR ist ein Webservice, der die Ausführung von Big-Data-Frameworks und die effiziente Verarbeitung riesiger Datenmengen vereinfacht.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `EMRTagValidation.zip` – Der Lambda-Code für die Sicherheitskontrolle.
- `EMRTagValidation.yml` – Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Polen

Einrichten des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket zum Hosten	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der ZIP-Datei des Lambda-Codes. Dieser S3-Bucket muss sich in derselben AWS-Region befinden wie der Amazon EMR-Cluster, den Sie überwachen möchten. Der Name eines Amazon S3-Buckets ist global eindeutig , und der Namespace wird von allen AWS-Konten verwendet. Der Name des S3-Buckets darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie die im Abschnitt Anhänge bereitgestellte ZIP-Datei mit dem Lambda-Code in den S3-Bucket hoch.	Cloud-Architekt

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die AWS-CloudFormation Vorlage.	Öffnen Sie die AWS-CloudFormation Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die Vorlage bereit. Weitere Informationen zum Bereitstellen von AWS- CloudFormation Vorlagen finden Sie unter Erstellen eines Stacks in der AWS- CloudFormation	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole in der - CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Parameter in der Vorlage ab.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im ersten Epi erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (ZIP-Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. Dateiname .zip oder Steuerelemente/Dateiname .zip). Schließen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, an die Sie Amazon SNS-Benac hrichtigungen erhalten möchten. • Markieren von Schlüssel namen: Geben Sie die Tags, nach denen Sie suchen möchten, in einer durch Komma getrennten Liste an (z. B. `Applicati onID` , `Environment` ,	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`0wner`). Das Ereignis CloudWatch Ereignisse überwacht den Cluster auf diese Tags und sendet eine Benachrichtigung, wenn sie nicht gefunden werden. • Lambda-Protokollierungsebene : Geben Sie die Protokollierungsebene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen zum Fortschritt, Fehler bei Fehlerereignissen, die eine Fortsetzung der Bereitstellung ermöglichen würden, und Warnung bei potenziell schädlichen Situationen zu protokollieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätige	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n, um Benachrichtigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- AWS Lambda-Entwicklerhandbuch
- Markieren von Clustern in Amazon EMR

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Serverlos; Analytik	Arbeitslast: Open Source
AWS-Dienste: Amazon EMR; Amazon S3; Amazon SNS; Amazon CloudWatch		

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die die Protokollierungskonfiguration für Amazon EMR-Cluster überwacht, die auf Amazon Web Services (AWS) ausgeführt werden.

Amazon EMR ist ein AWS-Tool für die Verarbeitung und Analyse großer Datenmengen. Amazon EMR bietet den erweiterbaren Service mit niedriger Konfiguration als Alternative zum Betrieb interner Cluster-Datenverarbeitung. Amazon EMR bietet zwei Arten von EMR-Clustern.

- Transiente Amazon EMR-Cluster: Transiente Amazon EMR-Cluster werden automatisch heruntergefahren und es fallen keine Kosten mehr an, wenn die Verarbeitung abgeschlossen ist.
- Persistente Amazon EMR-Cluster: Persistente Amazon EMR-Cluster werden weiterhin ausgeführt, nachdem der Datenverarbeitungsauftrag abgeschlossen ist.

Sowohl Amazon EMR als auch Hadoop erstellen Protokolldateien, die Aufschluss über den jeweiligen Status des Clusters geben. Standardmäßig werden diese auf den Master-Knoten im Verzeichnis /mnt/var/log/ geschrieben. Je nachdem, wie Sie den Cluster beim Start konfigurieren, können Sie diese Protokolle auch in Amazon Simple Storage Service (Amazon S3) speichern und sie über das grafische Debugging-Tool anzeigen. Beachten Sie, dass die Amazon S3 S3-Protokollierung nur angegeben werden kann, wenn der Cluster gestartet wird. Bei dieser Konfiguration werden alle 5 Minuten Protokolle vom primären Knoten an den Amazon S3 S3-Standort gesendet. Für transiente Cluster ist die Amazon S3 S3-Protokollierung wichtig, da die Cluster nach Abschluss der Verarbeitung verschwinden und diese Protokolldateien zum Debuggen fehlgeschlagener Jobs verwendet werden können.

Das Muster verwendet eine CloudFormation AWS-Vorlage, um eine Sicherheitskontrolle bereitzustellen, die API-Aufrufe überwacht und Amazon CloudWatch Events auf „RunJobFlow“ startet. Der Trigger ruft AWS Lambda auf, das ein Python-Skript ausführt. Die Lambda-Funktion ruft die EMR-Cluster-ID aus der JSON-Eingabe des Ereignisses ab und sucht auch nach einer Amazon S3 S3-Protokoll-URI. Wenn kein Amazon S3 S3-URI gefunden wird, sendet die Lambda-Funktion eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung, in der der EMR-Clustername, die Verstoßdetails, die AWS-Region, das AWS-Konto und der Lambda Amazon Resource Name (ARN), von dem die Benachrichtigung stammt, detailliert beschrieben werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket für die Lambda-Code-.zip-Datei
- Eine E-Mail-Adresse, an die Sie die Benachrichtigung über den Verstoß erhalten möchten

Einschränkungen

- Diese Detective Control ist regional und muss in den AWS-Regionen eingesetzt werden, die Sie überwachen möchten.

Produktversionen

- Amazon EMR Version 4.8.0 und höher

Architektur

Zieltechnologie-Stack

- Veranstaltung Amazon CloudWatch Events
- Amazon EMR
- Lambda-Funktion
- S3-Bucket
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS verwenden, CloudFormation StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

Tools

- AWS CloudFormation — AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung von AWS-Ressourcen mithilfe von Infrastructure as Code.
- AWS Cloudwatch Events — AWS CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- Amazon EMR — Amazon EMR ist eine verwaltete Cluster-Plattform, die den Betrieb von Big-Data-Frameworks vereinfacht.
- AWS Lambda — AWS Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon S3 ist eine Webservice-Schnittstelle, mit der Sie beliebige Datenmengen von überall im Internet speichern und abrufen können.
- Amazon SNS — Amazon SNS ist ein Webservice, der die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen, koordiniert und verwaltet.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Um die Lambda-Code-ZIP-Datei zu hosten, wählen oder erstellen Sie einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben AWS-Region befinden wie der Amazon EMR-Cluster, der bewertet wird.	Cloud-Architekt

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt „Anlagen“ bereitgestellt wird, in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie der Amazon EMR-Cluster, der bewertet wird.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie auf der CloudFormation AWS-Konsole, in derselben Region wie Ihr S3-Bucket, die CloudFormation AWS-Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an. Weitere Informationen zur Bereitstellung von CloudFormation AWS-Vorlagen finden Sie im Abschnitt „Verwandte Ressourcen“.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie den Amazon S3 S3-Schlüssel ein.	<file-name>Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket ohne führende Schrägstriche an (z. B.<directory>/.zip).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SNS-Benachrichtigungen zu erhalten.	
Definieren Sie die Protokoll ierungsebene.	Definieren Sie die Protokoll ierungsebene und die Häufigkeit für Ihre Lambda-Funktion. „Info“ bezeichnet detaillierte Informationsmeldun gen über den Fortschritt der Anwendung. „Fehler“ bezeichnet Fehlerereignisse, die dazu führen könnten, dass die Anwendung weiterhin ausgeführt werden kann. „Warnung“ steht für potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachric htigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

AWS Lambda

Amazon EMR-Protokollierung

Bereitstellen von CloudFormation AWS-Vorlagen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python

Umgebung: Produktion	Technologien: Analytik; Cloud-nativ; Data Lakes; Softwareentwicklung und Testen; Serverlos; Große Datenmengen	AWS-Dienste: AWS Glue; Amazon S3

Übersicht

Dieses Muster zeigt Ihnen, wie Sie schnell und einfach Millionen von Beispieldateien gleichzeitig generieren können, indem Sie einen in Python geschriebenen AWS Glue Glue-Job erstellen. Die Beispieldateien werden in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert. Die Fähigkeit, schnell eine große Anzahl von Beispieldateien zu generieren, ist wichtig für das Testen oder Evaluieren von Services in der AWS-Cloud. Sie können beispielsweise die Leistung von AWS Glue Studio- oder AWS Glue DataBrew Glue-Jobs testen, indem Sie Datenanalysen für Millionen kleiner Dateien in einem Amazon S3 S3-Präfix durchführen.

Sie können zwar andere AWS-Services verwenden, um Beispieldatensätze zu generieren, wir empfehlen Ihnen jedoch, AWS Glue zu verwenden. Sie müssen keine Infrastruktur verwalten, da AWS Glue ein serverloser Datenverarbeitungsservice ist. Sie können einfach Ihren Code mitbringen und ihn in einem AWS Glue Glue-Cluster ausführen. Darüber hinaus stellt AWS Glue die Ressourcen bereit, konfiguriert und skaliert sie, die für die Ausführung Ihrer Jobs erforderlich sind. Sie zahlen nur für die Ressourcen, die Ihre Jobs während der Ausführung verbrauchen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI), für die Verwendung mit dem AWS-Konto installiert und konfiguriert

Produktversionen

- Python 3.9
- AWS-CLI Version 2

Einschränkungen

Die maximale Anzahl von AWS Glue Glue-Jobs pro Trigger beträgt 50. Weitere Informationen finden Sie unter AWS Glue Glue-Endpunkte und Kontingente.

Architektur

Das folgende Diagramm zeigt eine Beispielarchitektur, in deren Mittelpunkt ein AWS Glue Glue-Job steht, der seine Ausgabe (d. h. Beispieldateien) in einen S3-Bucket schreibt.

Das Diagramm umfasst den folgenden Arbeitsablauf:

1. Sie verwenden die AWS-CLI, die AWS-Managementkonsole oder eine API, um den AWS Glue-Job zu initiieren. Mit der AWS-CLI oder API können Sie die Parallelisierung des aufgerufenen Jobs automatisieren und die Laufzeit für die Generierung von Beispieldateien reduzieren.
2. Der AWS Glue Glue-Job generiert Dateiinhalte nach dem Zufallsprinzip, konvertiert den Inhalt in das CSV-Format und speichert den Inhalt dann als Amazon S3 S3-Objekt unter einem gemeinsamen Präfix. Jede Datei ist kleiner als ein Kilobyte. Der AWS Glue Glue-Job akzeptiert zwei benutzerdefinierte Auftragsparameter: `START_RANGE` und`END_RANGE`. Sie können diese Parameter verwenden, um Dateinamen und die Anzahl der Dateien festzulegen, die in Amazon S3 bei jeder Auftragsausführung generiert werden. Sie können mehrere Instanzen dieses Jobs parallel ausführen (z. B. 100 Instanzen).

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Bewährte Methoden

Beachten Sie bei der Implementierung dieses Musters die folgenden bewährten Methoden für AWS Glue:

- Verwenden Sie den richtigen AWS Glue Glue-Worker-Typ, um die Kosten zu senken. Wir empfehlen Ihnen, sich mit den verschiedenen Eigenschaften von Workertypen vertraut zu machen und dann anhand der CPU- und Speicheranforderungen den richtigen Worker-Typ für Ihre Arbeitslast auszuwählen. Für dieses Muster empfehlen wir, einen Python-Shell-Job als Jobtyp zu verwenden, um die DPU zu minimieren und die Kosten zu senken. Weitere Informationen finden Sie unter Hinzufügen von Aufträgen in AWS Glue im AWS Glue Developer Guide.
- Verwenden Sie das richtige Parallelitätslimit, um Ihren Job zu skalieren. Wir empfehlen Ihnen, die maximale Parallelität Ihres AWS Glue Glue-Auftrags auf Ihrem Zeitbedarf und der erforderlichen Anzahl von Dateien festzulegen.
- Beginnen Sie zunächst mit der Generierung einer kleinen Anzahl von Dateien. Um Kosten und Zeit beim Erstellen Ihrer AWS Glue Glue-Jobs zu sparen, beginnen Sie mit einer kleinen Anzahl von Dateien (z. B. 1.000). Dies kann die Fehlerbehebung erleichtern. Wenn das Generieren einer kleinen Anzahl von Dateien erfolgreich ist, können Sie auf eine größere Anzahl von Dateien skalieren.
- Führen Sie es zuerst lokal aus. Um Kosten und Zeit bei der Erstellung Ihrer AWS Glue Glue-Jobs zu sparen, starten Sie die Entwicklung lokal und testen Sie Ihren Code. Anweisungen zur Einrichtung eines Docker-Containers, der Ihnen helfen kann, AWS Glue Glue-ETL-Jobs (Extrahieren, Transformieren und Laden) sowohl in einer Shell als auch in einer integrierten Entwicklungsumgebung (IDE) zu schreiben, finden Sie im Beitrag Entwickeln von AWS Glue Glue-ETL-Jobs lokal mithilfe eines Containers im AWS Big Data-Blog.

Weitere bewährte Methoden für AWS Glue finden Sie unter Bewährte Methoden in der AWS Glue Glue-Dokumentation.

Epen

Erstellen Sie einen S3-Ziel-Bucket und eine IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket zum Speichern der Dateien.	Erstellen Sie einen S3-Bucket und ein darin enthaltenes Präfix. Hinweis: In diesem Muster wird der `s3://{your-s3-bucket-name}/small-files/` Standort zu Demonstrationszwecken verwendet.	App-Developer
Erstellen und konfigurieren Sie eine IAM-Rolle.	Sie müssen eine IAM-Rolle erstellen, die Ihr AWS Glue Glue-Job verwenden kann, um in Ihren S3-Bucket zu schreiben. 1. Erstellen Sie eine IAM-Rolle (z. B. genannt `"AWSGlueServiceRole-smallfiles"`). 2. Wählen Sie AWS Glue als vertrauenswürdige Entität der Richtlinie. 3. Fügen Sie der Rolle eine von AWS verwaltete Richtlinie `"AWSGlueServiceRole"` hinzu, die aufgerufen wird. 4. Erstellen Sie eine Inline-Richtlinie oder eine vom	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kunden verwaltete Richtlinie, die auf der `"s3-small-file-access"` Grundlage der folgenden Konfiguration aufgerufen wird. `"{bucket}"` Ersetzen Sie es durch Ihren Bucket-Namen. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:PutObject" ], "Resource": [ "arn:aws:s3:::{bucket}/small-files/input/*" ] } ] }` 5. Hängen Sie die `"s3-small-file-access"` Richtlinie an Ihre Rolle an.	

Erstellen und konfigurieren Sie einen AWS Glue Glue-Job zur Verarbeitung gleichzeitiger Läufe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS Glue Glue-Job.	Sie müssen einen AWS Glue Glue-Job erstellen, der Ihre Inhalte generiert und in einem S3-Bucket speichert. Erstellen Sie einen AWS Glue Glue-Job und konfigurieren Sie dann Ihren Job, indem Sie die folgenden Schritte ausführen: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenintegration und ETL die Option Jobs aus. 3. Wählen Sie im Abschnitt Job erstellen die Option Python-Shell-Skripteditor aus. 4. Wählen Sie im Abschnitt Optionen die Option Neues Skript mit Standardcode erstellen und wählen Sie dann Erstellen aus. 5. Wählen Sie Jobdetails. 6. Geben Sie als Namen create_small_files ein.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie für IAM-Rolle die IAM-Rolle aus, die Sie zuvor erstellt haben. 8. Wählen Sie im Abschnitt Dieser Job wird ausgeführt die Option Ein neues Skript, das von Ihnen erstellt werden soll aus. 9. Erweitern Sie Erweiterte Eigenschaften. 10. Geben Sie zu Demonstrationszwecken für Maximale Parallelität den Wert 100 ein. Hinweis: Die maximale Parallelität definiert, wie viele Instanzen des Jobs Sie parallel ausführen können. 11. Wählen Sie Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie den Jobcode.	1. Öffnen Sie die AWS Glue Glue-Konsole.
	2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
	3. Wählen Sie im Bereich Ihre Jobs den Job aus, den Sie zuvor erstellt haben.
	4. Wählen Sie die Registerkarte Skript und aktualisieren Sie dann das Skript auf der Grundlage des folgenden Codes. Aktualisieren Sie die `text_str` Variablen `BUCKET_NAME PREFIX`, und mit Ihren Werten.
	`from awsglue.utils import getResolvedOptions`
	`import sys`
	`import boto3`
	`from random import randrange`
	
	`# Two arguments`
	`args = getResolvedOptions(sys.argv, ['START_RANGE', 'END_RANGE'])`
	
	`START_RANGE = int(args['START_RANGE'])`
	`END_RANGE = int(args['END_RANGE'])`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>BUCKET_NAME = '{BUCKET_NAME}'
	PREFIX = 'small-files/input/'
	s3 = boto3.resource('s3')
	for x in range(START_RANGE, END_RANGE):
	    # generate file name
	    file_name = f"input_{x}.txt"
	    # generate text
	    text_str = str(randrange(100000))+","+str(randrange(100000))+", " + str(randrange(10000000)) + "," + str(randrange(10000))
	    # write in s3
	s3.Object(BUCKET_NAME, PREFIX + file_name).put(Body=text_str)</pre> 5. Wählen Sie Speichern.	

Führen Sie den AWS Glue Glue-Job über die Befehlszeile oder Konsole aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue Glue-Job von der Befehlszeile aus.	Um Ihren AWS Glue Glue-Job über die AWS-CLI auszuführen, führen Sie den folgenden Befehl mit Ihren Werten aus:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"0","--END_RANGE":"1000000"}'`
	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"1000000","--END_RANGE":"2000000"}'`
	
	Hinweis: Anweisungen zur Ausführung des AWS Glue Glue-Jobs von der AWS-Managementkonsole aus finden Sie in der Geschichte Ausführen des AWS Glue-Jobs in der AWS-Managementkonsole in diesem Muster.
	
	Tipp: Wir empfehlen, die AWS-CLI zum Ausführen von AWS Glue-Jobs zu verwenden, wenn Sie mehrere Ausführungen gleichzeitig mit unterschiedlichen Parametern ausführen möchten, wie im obigen Beispiel gezeigt.
	
	Um alle AWS-CLI-Befehle zu generieren, die zum Generieren einer definierten Anzahl von Dateien unter Verwendung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	eines bestimmten Paralleli sierungsfaktors erforderl ich sind, führen Sie den folgenden Bash-Code aus (unter Verwendung Ihrer Werte):
	
	`# define parameters NUMBER_OF_FILES= 10000000; PARALLELIZATION=50;`
	
	`# initialize _SB=0;`
	
	`# generate commands for i in $(seq 1 $PARALLELIZATION); do echo aws glue start-job-run -- job-name create_sm all_files --argumen ts "'"'{"--START_RANG E":"'$(((NUMBER_OF _FILES/PARALLELIZA TION) * (i-1) + _SB))'","--END_RAN GE":"'$(((NUMBER_O F_FILES/PARALLELIZ ATION) * (i)))'"}'"'"; _SB=1; done`
	
	Wenn Sie das obige Skript verwenden, sollten Sie Folgendes beachten:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Das Skript vereinfacht das Aufrufen und Generieren kleiner Dateien in großem Maßstab. • Aktualisiere `NUMBER_OF_FILES` und `PARALLELIZATION` mit deinen Werten. • Das obige Skript druckt eine Liste von Befehlen, die Sie ausführen müssen. Kopieren Sie diese Ausgabebefehle und führen Sie sie dann in Ihrem Terminal aus. • Wenn Sie die Befehle direkt aus dem Skript heraus ausführen möchten, entfernen Sie die `echo` Anweisung in Zeile 11. Hinweis: Ein Beispiel für die Ausgabe des obigen Skripts finden Sie unter Shell-Skriptausgabe im Abschnitt Zusätzliche Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue Glue-Job in der AWS-Manag ementkonsole aus.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Glue-Konsole. 2. Wählen Sie im Navigatio nsbereich unter Dateninte gration und ETL die Option Jobs aus. 3. Wählen Sie im Bereich „Ihre Jobs“ Ihren Job aus. 4. Aktualisieren Sie im Abschnitt Parameter (optional) Ihre Parameter. 5. Wählen Sie Aktion und dann Job ausführen aus. 6. Wiederholen Sie die Schritte 3 bis 5 so oft Sie möchten. Um beispiels weise 10 Millionen Dateien zu erstellen, wiederhol en Sie diesen Vorgang zehnmal.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status Ihres AWS Glue Glue-Auftrags.	1. Öffnen Sie die AWS Glue Glue-Konsole. 2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus. 3. Wählen Sie im Bereich „Ihre Jobs“ den Job aus, den Sie zuvor erstellt haben (d. h. `create_small_files`). 4. Einen Einblick in den Fortschritt und die Generierung Ihrer Dateien finden Sie in den Spalten Lauf-ID, Ausführungsstatus und anderen.	App-Developer

Zugehörige Ressourcen

Referenzen

- Register für offene Daten auf AWS
- Datensätze für Analysen
- Daten auf AWS öffnen
- Hinzufügen von Aufträgen in AWS Glue
- Erste Schritte mit AWS Glue

Anleitungen und Muster

- Bewährte Methoden für AWS Glue
- Anwendungen zum Testen auslasten

Zusätzliche Informationen

Benchmarking-Test

Dieses Muster wurde verwendet, um im Rahmen eines Benchmark-Tests 10 Millionen Dateien mit unterschiedlichen Parallelisierungsparametern zu generieren. Die folgende Tabelle zeigt die Ergebnisse des Tests:

Parallelisierung	Anzahl der Dateien, die durch einen Joblauf generiert wurden	Dauer des Job	Geschwindigkeit
10	1 000 000	6 Stunden, 40 Minuten	Sehr langsam
50	200 000	80 Minuten	Mittel
100	100 000	40 Minuten	Schnell

Wenn Sie den Prozess beschleunigen möchten, können Sie in Ihrer Jobkonfiguration mehr gleichzeitige Läufe konfigurieren. Sie können die Auftragskonfiguration ganz einfach an Ihre Anforderungen anpassen. Beachten Sie jedoch, dass es ein Kontingent für den AWS Glue Glue-Service gibt. Weitere Informationen finden Sie unter AWS Glue Glue-Endpunkte und Kontingente.

Shell-Skriptausgabe

Das folgende Beispiel zeigt die Ausgabe des Shell-Skripts aus dem Job Run the AWS Glue von der Befehlszeile aus in diesem Muster.

```
user@MUC-1234567890 MINGW64 ~
  $ # define parameters
  NUMBER_OF_FILES=10000000;
  PARALLELIZATION=50;
  # initialize
  _SB=0;

  # generate commands
  for i in $(seq 1 $PARALLELIZATION);
   do
```

```
        echo aws glue start-job-run --job-name create_small_files --arguments
 "'"'{"--START_RANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i-1) + SB))'","--
ENDRANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i)))'"}'"'";
        _SB=1;
   done

  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"0","--END_RANGE":"200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"200001","--END_RANGE":"400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"400001","--END_RANGE":"600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"600001","--END_RANGE":"800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"800001","--END_RANGE":"1000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1000001","--END_RANGE":"1200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1200001","--END_RANGE":"1400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1400001","--END_RANGE":"1600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1600001","--END_RANGE":"1800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1800001","--END_RANGE":"2000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2000001","--END_RANGE":"2200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2200001","--END_RANGE":"2400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2400001","--END_RANGE":"2600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2600001","--END_RANGE":"2800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2800001","--END_RANGE":"3000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3000001","--END_RANGE":"3200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3200001","--END_RANGE":"3400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3400001","--END_RANGE":"3600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3600001","--END_RANGE":"3800000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3800001","--END_RANGE":"4000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4000001","--END_RANGE":"4200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4200001","--END_RANGE":"4400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4400001","--END_RANGE":"4600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4600001","--END_RANGE":"4800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4800001","--END_RANGE":"5000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5000001","--END_RANGE":"5200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5200001","--END_RANGE":"5400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5400001","--END_RANGE":"5600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5600001","--END_RANGE":"5800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5800001","--END_RANGE":"6000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6000001","--END_RANGE":"6200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6200001","--END_RANGE":"6400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6400001","--END_RANGE":"6600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6600001","--END_RANGE":"6800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6800001","--END_RANGE":"7000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7000001","--END_RANGE":"7200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7200001","--END_RANGE":"7400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7400001","--END_RANGE":"7600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7600001","--END_RANGE":"7800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7800001","--END_RANGE":"8000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8000001","--END_RANGE":"8200000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8200001","--END_RANGE":"8400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8400001","--END_RANGE":"8600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8600001","--END_RANGE":"8800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8800001","--END_RANGE":"9000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9000001","--END_RANGE":"9200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9200001","--END_RANGE":"9400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9400001","--END_RANGE":"9600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9600001","--END_RANGE":"9800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9800001","--END_RANGE":"10000000"}'

  user@MUC-1234567890 MINGW64 ~
```

HÄUFIG GESTELLTE FRAGEN

Wie viele gleichzeitige Läufe oder parallel Jobs sollte ich verwenden?

Die Anzahl der gleichzeitigen Läufe und parallel Jobs hängt von Ihrem Zeitbedarf und der gewünschten Anzahl von Testdateien ab. Wir empfehlen Ihnen, die Größe der Dateien, die Sie erstellen, zu überprüfen. Prüfen Sie zunächst, wie viel Zeit ein AWS Glue Glue-Job benötigt, um die gewünschte Anzahl von Dateien zu generieren. Verwenden Sie dann die richtige Anzahl gleichzeitiger Läufe, um Ihre Ziele zu erreichen. Wenn Sie beispielsweise davon ausgehen, dass 100.000 Dateien 40 Minuten benötigen, um den Lauf abzuschließen, Ihre Zielzeit jedoch 30 Minuten beträgt, müssen Sie die Parallelitätseinstellung für Ihren AWS Glue Glue-Job erhöhen.

Welche Art von Inhalt kann ich mit diesem Muster erstellen?

Sie können jede Art von Inhalt erstellen, z. B. Textdateien mit unterschiedlichen Trennzeichen (z. B. PIPE, JSON oder CSV). Dieses Muster verwendet Boto3, um in eine Datei zu schreiben, und speichert die Datei dann in einem S3-Bucket.

Welche IAM-Berechtigungen benötige ich für den S3-Bucket?

Sie benötigen eine identitätsbasierte Richtlinie, die den `Write` Zugriff auf Objekte in Ihrem S3-Bucket ermöglicht. Weitere Informationen finden Sie unter Amazon S3: Erlaubt Lese- und Schreibzugriff auf Objekte in einem S3-Bucket in der Amazon S3 S3-Dokumentation.

Starten eines Spark-Auftrags in einem vorübergehenden EMR-Cluster mithilfe einer Lambda-Funktion

Erstellt von Dhr Boljioti Mukherjee (AWS)

Umgebung: Produktion	Technologien: Analytik	Workload: Open-Source
AWS-Services: Amazon EMR; AWS Identity and Access Management ;AWS Lambda; Amazon VPC		

Übersicht

Dieses Muster verwendet die Amazon-EMR RunJobFlow -API-Aktion, um einen vorübergehenden Cluster zu starten, um einen Spark-Auftrag von einer Lambda-Funktion aus auszuführen.
Ein vorübergehender EMR-Cluster ist so konzipiert, dass er beendet wird, sobald der Auftrag abgeschlossen ist oder ein Fehler auftritt. Ein vorübergehender Cluster bietet Kosteneinsparungen, da er nur während der Berechnungszeit ausgeführt wird und Skalierbarkeit und Flexibilität in einer Cloud-Umgebung bietet.

Der vorübergehende EMR-Cluster wird mit der Boto3-API und der Python-Programmiersprache in einer Lambda-Funktion gestartet. Die in Python geschriebene Lambda-Funktion bietet die zusätzliche Flexibilität, den Cluster bei Bedarf zu initiieren.

Um eine Beispiel-Batch-Berechnung und -Ausgabe zu demonstrieren, startet dieses Muster einen Spark-Auftrag in einem EMR-Cluster von einer Lambda-Funktion aus und führt eine Batch-Berechnung für die Beispiel-Vertriebsdaten eines fiktiven Unternehmens durch. Die Ausgabe des Spark-Auftrags ist eine CSV-Datei (durch Kommas getrennte Werte) in Amazon Simple Storage Service (Amazon S3). Die Eingabedatendatei, die Spark .jar-Datei, ein Codeausschnitt und eine AWS- CloudFormation Vorlage für eine Virtual Private Cloud (VPC)- und AWS Identity and Access Management (IAM)-Rolle zum Ausführen der Berechnung werden als Anhang bereitgestellt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

Einschränkungen

- Es kann jeweils nur ein Spark-Auftrag aus dem Code initiiert werden.

Produktversionen

- Getestet auf Amazon EMR 6.0.0

Architektur

Zieltechnologie-Stack

- Amazon EMR
- AWS Lambda
- Amazon S3
- Apache Spark

Zielarchitektur

Automatisierung und Skalierung

Um die Spark-EMR-Stapelberechnung zu automatisieren, können Sie eine der folgenden Optionen verwenden.

- Implementieren Sie eine Amazon- EventBridge Regel, die die Lambda-Funktion in einem Cron-Zeitplan initiieren kann. Weitere Informationen finden Sie unter Tutorial: Planen von AWS Lambda-Funktionen mit EventBridge.
- Konfigurieren Sie Amazon S3-Ereignisbenachrichtigungen, um die Lambda-Funktion bei Dateiankunft zu initiieren.
- Übergeben Sie die Eingabeparameter an die AWS Lambda-Funktion über den Ereignistext und die Lambda-Umgebungsvariablen.

Tools

AWS-Services

- Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks in AWS vereinfacht, um große Datenmengen zu verarbeiten und zu analysieren.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Apache Spark ist eine mehrsprachige Analyse-Engine für die umfangreiche Datenverarbeitung.

Polen

Erstellen der Amazon-EMR- und Lambda-IAM-Rollen und der VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rollen und die VPC.	Wenn Sie bereits über die IAM-Rollen AWS Lambda und Amazon EMR und eine VPC verfügen, können Sie diesen Schritt überspringen. Um den Code auszuführen, benötigen sowohl der EMR-Cluster als auch die Lambda-Funktion IAM-Rollen. Der EMR-Clust er benötigt auch eine VPC mit einem öffentlichen Subnetz oder ein privates Subnetz mit einem NAT-Gateway. Um automatisch alle IAM-Rolle	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n und eine VPC zu erstellen , stellen Sie die angehängt e AWS- CloudFormation Vorlage unverändert bereit. Sie können die Rollen und die VPC auch manuell erstellen, wie im Abschnitt Zusätzliche Informationen angegeben.	
Notieren Sie sich die Ausgabeschlüssel der AWS-CloudFormation Vorlage.	Nachdem die CloudFormation Vorlage erfolgreich bereitgestellt wurde, navigieren Sie in der AWS- CloudFormation Konsole zur Registerkarte Outputs. Notieren Sie sich die fünf Ausgabeschlüssel: • `S3Bucket` • `LambdaExecutionRole` • `ServiceRole` • `JobFlowRole` • `Ec2SubnetId` Sie verwenden die Werte aus diesen Schlüsseln, wenn Sie die Lambda-Funktion erstellen .	Cloud-Architekt

Laden Sie die Spark-.jar-Datei hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Spark-.jar-Datei hoch.	Laden Sie die Spark .jar-Datei in den S3-Bucket hoch, den	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der AWS- CloudFormation Stack erstellt hat. Der Bucket-Name ist mit dem Ausgabesc hlüssel identisch`S3Bucket`.	

Erstellen der Lambda-Funktion zum Starten des EMR-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Fu nktion.	Erstellen Sie in der Lambda-Konsole eine Python 3.9+ Lambda-Funktion mit einer Ausführungsrolle. Die Richtlini e für die Ausführungsrolle muss Lambda erlauben, einen EMR-Cluster zu starten. (Siehe angehängte AWS-CloudFormation Vorlage.)	Dateningenieur, Cloud-Ing enieur
Kopieren Sie den Code und fügen Sie ihn ein.	Ersetzen Sie den Code in der `lambda_function.py` Datei durch den Code aus dem Abschnitt Zusätzliche Informationen dieses Musters.	Dateningenieur, Cloud-Ing enieur
Ändern Sie die Parameter im Code.	Folgen Sie den Kommentaren im Code, um die Parameter werte so zu ändern, dass sie Ihrem AWS-Konto entsprech en.	Dateningenieur, Cloud-Ing enieur
Starten Sie die -Funktion, um den Cluster zu initiieren.	Starten Sie die Funktion , um die Erstellung eines vorüberge henden EMR-Clusters mit der bereitgestellten Spark-.jar-	Dateningenieur, Cloud-Ing enieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei zu initiieren. Es führt den Spark-Auftrag aus und wird automatisch beendet, wenn der Auftrag abgeschlossen ist.	
Überprüfen Sie den Status des EMR-Clusters.	Nachdem der EMR-Cluster initiiert wurde, wird er in der Amazon-EMR-Konsole auf der Registerkarte Cluster angezeigt. Alle Fehler beim Starten des Clusters oder beim Ausführen des Auftrags können entsprechend überprüft werden.	Dateningenieur, Cloud-Ingenieur

Einrichten und Ausführen der Beispieldemo

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Spark-.jar-Datei hoch.	Laden Sie die Spark-.jar-Datei aus dem Abschnitt Anhänge herunter und laden Sie sie in den S3-Bucket hoch.	Dateningenieur, Cloud-Ingenieur
Laden Sie den Eingabedatensatz hoch.	Laden Sie die angehängte `fake_sales_data.csv` Datei in den S3-Bucket hoch.	Dateningenieur, Cloud-Ingenieur
Fügen Sie den Lambda-Code ein und ändern Sie die Parameter.	Kopieren Sie den Code aus dem Abschnitt Tools und fügen Sie den Code in eine Lambda-Funktion ein, indem Sie die `lambda_function.py` Codedatei ersetzen. Ändern Sie die	Dateningenieur, Cloud-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Parameterwerte so, dass sie Ihrem Konto entsprechen.	
Starten Sie die Funktion und überprüfen Sie die Ausgabe.	Nachdem die Lambda-Funktion den Cluster mit dem bereitgestellten Spark-Auftrag initiiert hat, generiert sie eine CSV-Datei im S3-Bucket.	Dateningenieur, Cloud-Ingenieur

Zugehörige Ressourcen

- Spark erstellen
- Apache Spark und Amazon EMR
- Boto3 Docs run_job_flow-Dokumentation
- Informationen und Dokumentation zu Apache Spark

Zusätzliche Informationen

Code

```
"""
Copy paste the following code in your Lambda function. Make sure to change the
 following key parameters for the API as per your account

-Name (Name of Spark cluster)
-LogUri (S3 bucket to store EMR logs)
-Ec2SubnetId (The subnet to launch the cluster into)
-JobFlowRole (Service role for EC2)
-ServiceRole (Service role for Amazon EMR)

The following parameters are additional parameters for the Spark job itself. Change the
 bucket name and prefix for the Spark job (located at the bottom).

-s3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar (Spark jar file)
-s3://your-bucket-name/prefix/fake_sales_data.csv (Input data file in S3)
-s3://your-bucket-name/prefix/outputs/report_1/ (Output location in S3)
"""
```

```
import boto3

client = boto3.client('emr')


def lambda_handler(event, context):
    response = client.run_job_flow(
        Name='spark_job_cluster',
        LogUri='s3://your-bucket-name/prefix/logs',
        ReleaseLabel='emr-6.0.0',
        Instances={
            'MasterInstanceType': 'm5.xlarge',
            'SlaveInstanceType': 'm5.large',
            'InstanceCount': 1,
            'KeepJobFlowAliveWhenNoSteps': False,
            'TerminationProtected': False,
            'Ec2SubnetId': 'subnet-XXXXXXXXXXXXX'
        },
        Applications=[{'Name': 'Spark'}],
        Configurations=[
            {'Classification': 'spark-hive-site',
             'Properties': {
                 'hive.metastore.client.factory.class':
 'com.amazonaws.glue.catalog.metastore.AWSGlueDataCatalogHiveClientFactory'}
             }
        ],
        VisibleToAllUsers=True,
        JobFlowRole='EMRLambda-EMREC2InstanceProfile-XXXXXXXXX',
        ServiceRole='EMRLambda-EMRRole-XXXXXXXXX',
        Steps=[
            {
                'Name': 'flow-log-analysis',
                'ActionOnFailure': 'TERMINATE_CLUSTER',
                'HadoopJarStep': {
                    'Jar': 'command-runner.jar',
                    'Args': [
                        'spark-submit',
                        '--deploy-mode', 'cluster',
                        '--executor-memory', '6G',
                        '--num-executors', '1',
                        '--executor-cores', '2',
                        '--class', 'com.aws.emr.ProfitCalc',
                        's3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar',
                        's3://your-bucket-name/prefix/fake_sales_data.csv',
```

```
                        's3://your-bucket-name/prefix/outputs/report_1/'
                    ]
                }
            }
        ]
    )
```

IAM-Rollen und VPC-Erstellung

Um den EMR-Cluster in einer Lambda-Funktion zu starten, werden eine VPC- und IAM-Rolle benötigt. Sie können die VPC- und IAM-Rollen mithilfe der AWS- CloudFormation Vorlage im Abschnitt Anhänge dieses Musters einrichten oder sie manuell mithilfe der folgenden Links erstellen.

Die folgenden IAM-Rollen sind erforderlich, um Lambda und Amazon EMR auszuführen.

Lambda-Ausführungsrolle

Die Ausführungsrolle einer Lambda-Funktion gewährt ihr die Berechtigung, auf AWS-Services und -Ressourcen zuzugreifen.

Servicerolle für Amazon EMR

Die Amazon-EMR-Rolle definiert die zulässigen Aktionen für Amazon EMR beim Bereitstellen von Ressourcen und Ausführen von Aufgaben auf Serviceebene, die nicht im Kontext einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance ausgeführt werden, die in einem Cluster ausgeführt wird. Die Servicerolle wird beispielsweise verwendet, um EC2-Instances bereitzustellen, wenn ein Cluster gestartet wird.

Servicerolle für EC2-Instances

Die Servicerolle für Cluster-EC2-Instances (auch als EC2-Instance-Profil für Amazon EMR bezeichnet) ist eine spezielle Art von Servicerolle, die jeder EC2-Instance in einem Amazon-EMR-Cluster zugewiesen wird, wenn die Instance gestartet wird. Anwendungsprozesse, die zusätzlich zu Apache Hadoop ausgeführt werden, übernehmen diese Rolle für Berechtigungen zur Interaktion mit anderen AWS-Services.

VPC- und Subnetzerstellung

Sie können eine VPC über die VPC-Konsole erstellen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren von Apache Cassandra-Workloads zu Amazon Keyspaces mithilfe von AWS Glue

Erstellt von Nikolai Kolesnikov (AWS), Karthiga Priya Chandran (AWS) und Samir Patel (AWS)

Umgebung: Produktion	Quelle: Cassandra	Ziel: Amazon Keyspaces
R-Typ: N/A	Workload: Open-Source; Alle anderen Workloads	Technologien: Analytik; Migration; Serverless; Big Data
AWS-Services: AWS Glue; Amazon Keyspaces; Amazon S3; AWS CloudShell		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Ihre vorhandenen Apache Cassandra-Workloads mithilfe von CQLReplicator auf AWS Glue zu Amazon Keyspaces (für Apache Cassandra) migrieren. Sie können CQLReplicator auf AWS Glue verwenden, um die Replikationsverzögerung bei der Migration Ihrer Workloads auf einige Minuten zu minimieren. Sie erfahren auch, wie Sie einen Amazon Simple Storage Service (Amazon S3)-Bucket verwenden, um die für die Migration erforderlichen Daten zu speichern, einschließlich Apache Parquet-Dateien, Konfigurationsdateien und Skripts. Bei diesem Muster wird davon ausgegangen, dass Ihre Cassandra-Workloads auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances in einer Virtual Private Cloud (VPC) gehostet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Cassandra-Cluster mit einer Quelltabelle
- Zieltabelle in Amazon Keyspaces zum Replizieren des Workloads
- S3-Bucket zum Speichern von Parquet-Zwischendateien, die inkrementelle Datenänderungen enthalten
- S3-Bucket zum Speichern von Auftragskonfigurationsdateien und Skripts

Einschränkungen

- CQLReplicator auf AWS Glue benötigt einige Zeit, um Data Processing Units (DPUs) für die Cassandra-Workloads bereitzustellen. Die Replikationsverzögerung zwischen dem Cassandra-Cluster und dem Ziel-Keyspace und der Tabelle in Amazon Keyspaces dauert wahrscheinlich nur wenige Minuten.

Architektur

Quelltechnologie-Stack

- Apache Cassandra
- DataStax Server
- ScyllaDB

Zieltechnologie-Stack

- Amazon Keyspaces

Migrationsarchitektur

Das folgende Diagramm zeigt eine Beispielarchitektur, bei der ein Cassandra-Cluster auf EC2-Instances gehostet und über drei Availability Zones verteilt wird. Die Cassandra-Knoten werden in privaten Subnetzen gehostet.

Das Diagramm zeigt den folgenden Workflow:

1. Eine benutzerdefinierte Servicerolle bietet Zugriff auf Amazon Keyspaces und den S3-Bucket.
2. Ein AWS Glue-Auftrag liest die Auftragskonfiguration und die Skripts im S3-Bucket.
3. Der AWS Glue-Auftrag stellt über Port 9042 eine Verbindung her, um Daten aus dem Cassandra-Cluster zu lesen.
4. Der AWS Glue-Auftrag stellt über Port 9142 eine Verbindung her, um Daten in Amazon Keyspaces zu schreiben.

Tools

AWS-Services und -Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudShell ist eine browserbasierte Shell, mit der Sie AWS-Services mithilfe der AWS Command Line Interface (AWS CLI) und einer Reihe vorinstallierter Entwicklungstools verwalten können.
- AWS Glue ist ein vollständig verwalteter ETL-Service, mit dem Sie Daten zuverlässig kategorisieren, bereinigen, anreichern und zwischen Datenspeichern und Datenströmen verschieben können.
- Amazon Keyspaces (für Apache Cassandra) ist ein verwalteter Datenbankservice, der Sie bei der Migration, Ausführung und Skalierung Ihrer Cassandra-Workloads in der AWS Cloud unterstützt.

Code

Der Code für dieses Muster ist im GitHub CQLReplicator-Repository verfügbar.

Bewährte Methoden

- Um die erforderlichen AWS Glue-Ressourcen für die Migration zu ermitteln, schätzen Sie die Anzahl der Zeilen in der Cassandra-Quelltabelle. Zum Beispiel 250 000 Zeilen pro 0,25 DPU (2 vCPUs, 4 GB Arbeitsspeicher) mit 84 GB Festplatte.
- Vorwärmen von Amazon Keyspaces-Tabellen vor dem Ausführen von CQLReplicator . Beispielsweise können acht CQLReplicator-Kacheln (AWS Glue-Aufträge) bis zu 22 K WCUs pro Sekunde schreiben, sodass das Ziel auf bis zu 25 bis 30 K WCUs pro Sekunde vorgewärmt werden sollte.
- Um die Kommunikation zwischen AWS Glue-Komponenten zu ermöglichen, verwenden Sie eine selbstreferenzierende eingehende Regel für alle TCP-Ports in Ihrer Sicherheitsgruppe.
- Verwenden Sie die Strategie für inkrementellen Datenverkehr, um den Migrations-Workload im Laufe der Zeit zu verteilen.

Polen

Bereitstellen von CQLReplicator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Ziel-Keyspace und eine Tabelle.	1. Erstellen Sie einen Keyspace und eine Tabelle in Amazon Keyspaces. Weitere Informationen zur Schreibkapazität finden Sie unter Berechnungen von Schreibeinheiten im Abschnitt Zusätzliche Informationen dieses Musters. Sie können einen Keyspace auch mithilfe der Cassandra Query Language (CQL) erstellen. Weitere Informationen finden Sie unter Erstellen eines Keyspace mithilfe von CQL im Abschnitt Zusätzliche Informationen dieses Musters. Hinweis: Nachdem Sie die Tabelle erstellt haben, sollten Sie die Tabelle in den On-Demand-Kapazitätsmodus versetzen, um unnötige Gebühren zu vermeiden. 2. Um auf den Durchsatzmodus zu aktualisieren,	App-Besitzer, AWS-Administrator, DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	führen Sie das folgende Skript aus: `ALTER TABLE target_keyspace.target_table WITH CUSTOM_PROPERTIES = { 'capacity_mode': { 'throughput_mode': 'PAY_PER_REQUEST'} }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Cassandra-Treiber für die Verbindung mit Cassandra.	Verwenden Sie das folgende Konfigurationsskript: `Datastax-java-driver { basic.request.consistency = “LOCAL_QUORUM” basic.contact-points = [“127.0.0.1:9042”] advanced.reconnect-on-init = true basic.load-balancing-policy { local-datacenter = “datacenter1” } advanced.auth-provider = { class = PlainTextAuthProvider username = “user-at-sample” password = “S@MPLE=PASSWORD=” } }` Hinweis: Das vorherige Skript verwendet den Spark-Cassandra-Konnektor. Weitere Informationen finden Sie in der Referenzkonfiguration für Cassandra .	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Cassandra-Treiber für die Verbindung mit Amazon Keyspaces.	Verwenden Sie das folgende Konfigurationsskript: `datastax-java-driver { basic { load-balancing-pol icy { local-datacenter = us-west-2 } contact-points = ["cassandr a.us-west-2.amazon aws.com:9142"] request { page-size = 2500 timeout = 360 seconds consistency = LOCAL_QUORUM } } advanced { control-connection { timeout = 360 seconds } session-leak.thres hold = 6 connection { connect-timeout = 360 seconds init-query-timeout = 360 seconds warn-on-init-error = false } auth-provider = { class = software. aws.mcs.auth.SigV4 AuthProvider`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> aws-region = us-
	west-2
	 }
	
	 ssl-engine-factory {
	  class = DefaultSs
	lEngineFactory
	  }
	  }
	}</pre>
	Hinweis: Das vorherige Skript verwendet den Spark-Cassandra-Konnektor. Weitere Informationen finden Sie in der Referenzkonfiguration für Cassandra .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den AWS Glue-Auftrag.	Erstellen Sie eine neue AWS-Servicerolle mit dem Namen `glue-cassandra-migration` mit AWS Glue als vertrauenswürdiger Entität. Hinweis: Die `glue-cassandra-migration` sollte Lese- und Schreibzugriff auf den S3-Bucket und die Amazon Keyspaces gewähren. Der S3-Bucket enthält die JAR-Dateien, Konfigurationsdateien für Amazon Keyspaces und Cassandra sowie die Parquet-Zwischendateien. Sie enthält beispielsweise die `AmazonKeyspacesFullAccess` `AWSGlueServiceRole` verwaltet en Richtlinien `AmazonS3FullAccess` , und .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie CQLReplicator in AWS herunter CloudShell.	Laden Sie das Projekt in Ihren Basisordner herunter, indem Sie den folgenden Befehl ausführen:
	`git clone https://github.com/aws-samples/cql-replicator .git`
	`cd cql-replicator/glue`
	`# Only for AWS CloudShell, the bc package includes bc and dc. Bc is an arbitrary precision numeric processing arithmetic language`
	`sudo yum install bc -y`	

Ändern Sie die Referenzkonfigurationsdateien.	Kopieren Sie `Cassandra Connector.conf` und in `KeyspacesConnector.conf` das `../glue/conf` Verzeichnis im Projektordner.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initiieren Sie den Migration sprozess.	Der folgende Befehl initialisiert die CQLReplicator-Umgebung. Die Initialisierung umfasst das Kopieren von JAR-Artefakten und das Erstellen eines AWS Glue-Konnektors, eines S3-Buckets, eines AWS Glue-Auftrags, des `migration` Keyspaces und der `ledger` Tabelle:
	`cd cql-replicator/glue/bin`
	`./cqlreplicator --state init --sg '"sg-1","sg-2"' \ --subnet "subnet-XXXXXXXXXXXX" \ --az us-west-2a --region us-west-2 \ --glue-iam-role glue-cassandra-migration \ --landing-zone s3://cql-replicator-1234567890-us-west-2`
	Das Skript enthält die folgenden Parameter:
	• `--sg` – Die Sicherheitsgruppen, die den Zugriff auf den Cassandra-Cluster von AWS Glue aus ermöglichen und die
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	selbstreferenzierende Regel für eingehenden Datenverkehr für den gesamten Datenverkehr enthalten • `--subnet` – Das Subnetz, zu dem der Cassandra-Cluster gehört • `--az` – Die Availability Zone des Subnetzes • `--region` – Die AWS-Region, in der der Cassandra-Cluster bereitgestellt wird • `--glue-iam-role` – Die IAM-Rollenberechtigungen, die AWS Glue annehmen kann, wenn Amazon Keyspaces und Amazon S3 in Ihrem Namen aufgerufen werden • `--landing zone` – Ein optionaler Parameter für die Wiederverwendung eines S3-Buckets (Wenn Sie keinen Wert für den `--landing zone` Parameter angeben, versucht der `init` Prozess, einen neuen Bucket zum Speichern der Konfigurationsdateien, .jar-Artefakte und Zwischendateien zu erstellen.)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	Nachdem Sie den vorherigen Befehl ausgeführt haben, sollte das AWS-Konto Folgendes enthalten: • Der CQLReplicator-AWS Glue-Auftrag und der AWS Glue-Konnektor in AWS Glue • Der S3-Bucket, in dem die Artefakte gespeichert sind • Der Ziel-Keyspace `migration` und die `ledger` Tabelle in Amazon Keyspaces	AWS DevOps

CQLReplicator ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Migrationsprozess.	Um CQLReplicator auf AWS Glue zu betreiben, müssen Sie den `--state run` Befehl verwenden, gefolgt von einer Reihe von Parametern. Die genaue Konfiguration dieser Parameter hängt hauptsächlich von Ihren individuellen Migrationsanforderungen ab. Diese Einstellungen können beispielsweise variieren, wenn Sie TTL-Werte (Time to Live) und Aktualisierungen replizieren oder Objekte, die größer	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als 1 MB sind, nach Amazon S3 auslagern. Führen Sie den folgenden Befehl aus, um den Workload aus dem Cassandra-Cluster in Amazon Keyspaces zu replizieren: `./cqlreplicator --state run --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace \ --src-table source_table \ --trg-keyspace taget_keyspace \ --writetime-column column_name \ --trg-table target_table --inc-traffic` Ihr Quell-Keyspace und Ihre Tabelle befinden sich `source_keyspace.source_table` im Cassandra-Cluster. Ihr Ziel-Keyspace und Ihre Tabelle befinden sich	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`target_keyspace.target_table` in Amazon Keyspaces. Der Parameter `--inc-traffic` hilft zu verhindern, dass inkrement eller Datenverkehr den Cassandra-Cluster und die Amazon Keyspaces mit einer hohen Anzahl von Anfragen überlastet. Um Updates `--writetime-column regular_column_name` zu replizieren, fügen Sie zu Ihrer Befehlsze ile hinzu. Die reguläre Spalte wird als Quelle des Schreibze itstempels verwendet.	

Überwachen des Migrationsprozesses

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie migrierte Cassandra-Zeilen während der historischen Migration sphase.	Führen Sie den folgenden Befehl aus, um die Anzahl der Zeilen zu erhalten, die während der Abgleichphase repliziert wurden: `./cqlreplicator --state stats \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--src-keyspace source_keyspace --src-table source_table --region us-west-2`	

Beenden des Migrationsprozesses

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie den `cqlreplicator` Befehl oder die AWS Glue-Konsole.	Führen Sie den folgenden Befehl aus, um den Migration sprozess ordnungsgemäß zu beenden: `./cqlreplicator --state request-stop --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace --src-table source_table` Um den Migrationsprozess sofort zu beenden, verwenden Sie die AWS Glue-Konsole.	AWS DevOps

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die bereitgestellten Ressourcen.	Mit dem folgenden Befehl werden der AWS Glue-Auftrag, der Konnektor, der S3-Bucket und die Keyspaces-Tabelle gelöscht`ledger`: `./cqlreplicator --state cleanup --landing-zone s3://cql-replicator-1234567890-us-west-2`	AWS DevOps

Fehlerbehebung

Problem	Lösung
AWS Glue-Aufträge sind fehlgeschlagen und haben einen Out of Memory (OOM)-Fehler zurückgegeben.	1. Ändern Sie den Worker-Typ (hochskalieren). Ändern Sie beispielsweise `G0.25X` in `G.1X` oder `G.1X` in `G.2X`. Alternativ können Sie die Anzahl der DPUs pro AWS Glue-Auftrag (hochskalieren) in CQLReplicator erhöhen. 2. Starten Sie den Migrationsprozess von dem Punkt aus, an dem er unterbrochen wurde. Um fehlgeschlagene CQLReplicator-Aufträge neu zu starten, führen Sie den `--state run` Befehl mit denselben Parametern erneut aus.

Zugehörige Ressourcen

- CQLReplicator mit AWS Glue README.MD

- AWS Glue-Dokumentation
- Dokumentation zu Amazon Keyspaces
- Apache Cassandra

Zusätzliche Informationen

Überlegungen zur Migration

Sie können AWS Glue verwenden, um Ihren Cassandra-Workload zu Amazon Keyspaces zu migrieren, während Ihre Cassandra-Quelldatenbanken während des Migrationsprozesses voll funktionsfähig bleiben. Nachdem die Replikation abgeschlossen ist, können Sie Ihre Anwendungen mit minimaler Replikationsverzögerung (weniger als Minuten) zwischen dem Cassandra-Cluster und Amazon Keyspaces auf Amazon Keyspaces umstellen. Um die Datenkonsistenz aufrechtzuerhalten, können Sie auch eine ähnliche Pipeline verwenden, um die Daten aus Amazon Keyspaces zurück in den Cassandra-Cluster zu replizieren.

Berechnungen von Schreibeinheiten

Betrachten Sie beispielsweise, dass Sie beabsichtigen, 500.000.000 mit der Zeilengröße 1 KiB während einer Stunde zu schreiben. Die Gesamtzahl der benötigten Amazon Keyspaces-Schreibeinheiten (WCUs) basiert auf dieser Berechnung:

```
(number of rows/60 mins 60s) 1 WCU per row = (500,000,000/(60*60s) * 1 WCU)
= 69,444 WCUs required
```

69 444 WCUs pro Sekunde entsprechen der Rate für 1 Stunde, Sie könnten jedoch etwas Aufwand verursachen. Beispielsweise `69,444 * 1.10 = 76,388 WCUs` hat einen Overhead von 10 Prozent.

Erstellen eines Keyspace mithilfe von CQL

Um einen Keyspace mithilfe von CQL zu erstellen, führen Sie die folgenden Befehle aus:

```
CREATE KEYSPACE target_keyspace WITH replication = {'class': 'SingleRegionStrategy'}
CREATE TABLE target_keyspace.target_table ( userid uuid, level text, gameid int,
 description text, nickname text, zip text, email text, updatetime text, PRIMARY KEY
 (userid, level, gameid) ) WITH default_time_to_live = 0 AND CUSTOM_PROPERTIES =
 {'capacity_mode':{ 'throughput_mode':'PROVISIONED', 'write_capacity_units':76388,
 'read_capacity_units':3612 }} AND CLUSTERING ORDER BY (level ASC, gameid ASC)
```

Migrieren Sie Oracle Business Intelligence 12c von On-Premises-Servern zur AWS Cloud

Erstellt von Bolre (Lan-Ray) showunmi (AWS) und Patrick Huang (AWS)

Umgebung: Produktion	Quelle: On-Premises	Ziel: Amazon EC2, Amazon RDS, Amazon ALB, Amazon EFS
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Analytik; Datenbanken
AWS-Services: Amazon EBS; Amazon EC2; Amazon EFS; AWS CloudFormation; Elastic Load Balancing (ELB); AWS Certificate Manager (ACM)		

Übersicht

Dieses Muster zeigt, wie Oracle Business Intelligence Enterprise Edition 12c mithilfe von AWS von On-Premises-Servern in die AWS Cloud migriert wird CloudFormation. Außerdem wird beschrieben, wie Sie andere AWS-Services verwenden können, um Oracle BI 12c-Komponenten zu implementieren, die Hochverfügbarkeit, Sicherheit, Flexibilität und die Möglichkeit zur dynamischen Skalierung bieten.

Eine Liste der bewährten Methoden für die Migration von Oracle BI 12c in die AWS Cloud finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

Hinweis: Es hat sich bewährt, mehrere Testmigrationen durchzuführen, bevor Sie Ihre vorhandenen Oracle BI 12c-Daten in die Cloud übertragen. Diese Tests helfen Ihnen dabei, Ihren Migrationsansatz zu optimieren, potenzielle Probleme zu identifizieren und zu beheben und die Ausfallzeiten genauer zu schätzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Sichere Netzwerkkonnektivität zwischen Ihren On-Premises-Servern und AWS über AWS Virtual Private Network (AWS VPN)-Services oder AWS Direct Connect
- Softwarelizenzen für Ihr Oracle-Betriebssystem, Oracle BI 12c, Oracle Database, Oracle WebLogic Server und Oracle HTTP Server

Einschränkungen

Informationen zu Speichergrößenbeschränkungen finden Sie in der Dokumentation zu Amazon Relational Database Service (Amazon RDS) für Oracle.

Produktversionen

- Oracle Business Intelligence Enterprise Edition 12c
- Oracle WebLogic Server 12c
- Oracle HTTP Server 12c
- Oracle Database 12c (oder neuer)
- Oracle Java SE 8

Architektur

Das folgende Diagramm zeigt eine Beispielarchitektur für die Ausführung von Oracle BI 12c-Komponenten in der AWS Cloud:

Dieses Diagramm zeigt die folgende Architektur:

1. Amazon Route 53 bietet eine DNS-Konfiguration (Domain Name Service).
2. Elastic Load Balancing (ELB) verteilt den Netzwerkverkehr, um die Skalierbarkeit und Verfügbarkeit der Oracle BI 12c-Komponenten auf mehrere Availability Zones zu verbessern.
3. Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling-Gruppen hosten die Oracle HTTP Servers-, Weblogical Admin- und verwalteten BI-Server über mehrere Availability Zones hinweg.
4. Amazon Relational Database Service (Amazon RDS) für Oracle Datenbankspeicher BI Server-Metadaten über mehrere Availability Zones hinweg.

5. Amazon Elastic File System (Amazon EFS) wird für den gemeinsam genutzten Dateispeicher auf jeder Oracle BI 12c-Komponente gemountet.

Technologie-Stack

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon RDS für Oracle
- AWS Certificate Manager (ACM)
- Elastic Load Balancing (ELB)
- Oracle BI 12c
- Oracle WebLogic Server 12c
- Oracle HTTP Server (S)

Tools

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Certificate Manager (ACM) hilft Ihnen, öffentliche und private SSL/TLS X.509-Zertifikate und -Schlüssel zu erstellen, zu speichern und zu erneuern, die Ihre AWS-Websites und -Anwendungen schützen.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und sie schnell nach oben oder unten skalieren.
- Amazon EC2 Auto Scaling unterstützt Sie bei der Aufrechterhaltung der Anwendungsverfügbarkeit und ermöglicht Ihnen das automatische Hinzufügen oder Entfernen von Amazon EC2-Instances gemäß den von Ihnen definierten Bedingungen.
- Amazon Elastic File System (Amazon EFS) hilft Ihnen beim Erstellen und Konfigurieren freigegebener Dateisysteme in der AWS Cloud.

- Elastic Load Balancing verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.
- Mit Oracle Data Pump können Sie Daten und Metadaten mit hohen Geschwindigkeiten von einer Datenbank in eine andere verschieben.
- Oracle Fusion Middleware ist eine Suite von Tools zur Anwendungsentwicklung und Integrationslösungen für Identitätsmanagement, Zusammenarbeit und Business Intelligence Reporting.
- Oracle GoldenGate unterstützt Sie beim Entwerfen, Ausführen, Orchestrieren und Überwachen Ihrer Datenreplikations- und Stream-Datenverarbeitungslösungen in der Oracle Cloud Infrastructure.
- Oracle WebLogic Scripting Tool (WLST) bietet eine Befehlszeilenschnittstelle, mit der Sie Ihre WebLogic Cluster horizontal skalieren können.

Polen

Bewerten der Quellumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen zum Softwarebestand.	Identifizieren Sie Versionen und Patch-Level für jede der Softwarekomponenten Ihres Quelltechnologie-Stacks, einschließlich der folgenden: • Oracle-Betriebssystem	Migration Architect, Solutions Architect, Application Owner, Oracle-BI-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Oracle Database • Oracle BI 12c • Oracle WebLogic Server • Oracle HTTP Server • Java	
Sammeln Sie Informationen zum Datenverarbeitungs- und Speicherbestand.	Überprüfen Sie in Ihrer Quellumgebung die aktuellen und historischen Auslastun gsmetriken für Folgendes: • CPU-Verwendung • Speicherauslastung • Speichernutzung Wichtig: Stellen Sie sicher, dass Sie historische Nutzungsspitzen berücksic htigen.	Migration Architect, Solutions Architect, Application Owner, Oracle BI Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen über die Architektur der Quellumgebung und ihre Anforderungen.	Informieren Sie sich über die Architektur Ihrer Quellumgebung und ihre Anforderungen, einschließlich der folgenden Kenntnisse: • Oracle WebLogic Server-Domänenkonfiguration • Clustering • Load Balancing • Konnektivität • Verfügbarkeit • Anforderungen an die Notfallwiederherstellung	Migration Architect, Solutions Architect, Application Owner, Oracle-BI-Administrator
Identifizieren Sie Java Database Connectivity (JDBC)-Datenquellen.	Sammeln Sie Informationen über die JDBC-Datenquellen und Treiber Ihrer Quellumgebung für jede verwendete Datenbank-Engine.	Migration Architect, Application Owner, Oracle BI Administrator, Database Engineer oder Administrator
Sammeln Sie Informationen zu umgebungsspezifischen Einstellungen.	Sammeln Sie Informationen zu Einstellungen und Konfigurationen, die für Ihre Quellumgebung spezifisch sind, einschließlich der folgenden: • Benutzerdefinierte Startup- und Shutdown-Skripts • Java und andere Umgebungsvariablen • Zertifikate	Migration Architect, Solutions Architect, Application Owner, Oracle-BI-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie alle Abhängigkeiten von anderen Anwendungen.	Sammeln Sie Informationen über Integrationen in Ihrer Quellumgebung, die Abhängigkeiten mit anderen Anwendungen erstellen. Wichtig: Stellen Sie sicher, dass Sie alle LDAP-Integrationen (Lightweight Directory Access Protocol) und andere Netzwerkanforderungen identifizieren.	Migration Architect, Solutions Architect, Application Owner, Oracle-BI-Administrator

Entwerfen Ihrer Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein allgemeines Entwurfsdokument.	Erstellen Sie ein Zielarchitektur-Designdokument. Stellen Sie sicher, dass Sie die Informationen verwenden, die Sie bei der Bewertung Ihrer Quellumgebung gesammelt haben, um das Entwurfsdokument zu informieren.	Lösungsarchitekt, Anwendungsarchitekt, Datenbankingenieur, Migrationsarchitekt
Holen Sie sich die Genehmigung für das Entwurfsdokument.	Überprüfen Sie das Entwurfsdokument mit den Stakeholdern und holen Sie die erforderlichen Genehmigungen ein.	Anwendungs- oder Serviceeigentümer, Lösungsarchitekt, Anwendungsarchitekt

Bereitstellen der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Infrastrukturcode in vor CloudFormation.	Erstellen Sie CloudFormation Vorlagen für die Bereitstellung Ihrer Oracle BI 12c-Infrastruktur in der AWS Cloud. Weitere Informationen finden Sie unter Arbeiten mit AWS-CloudFormation Vorlagen im AWS- CloudFormation Benutzerhandbuch. Hinweis: Es hat sich bewährt, modulare CloudFormation Vorlagen für jede Oracle BI 12c-Stufe zu erstellen, anstatt eine große Vorlage für alle Ihre Ressourcen. Weitere Informationen zu CloudFormation bewährten Methoden finden Sie unter 8 bewährte Methoden zur Automatisierung Ihrer Bereitstellungen mit AWS CloudFormation im AWS-Blog.	Cloud Infrastructure Achitect, Lösungsarchitekt, Anwendungsarchitekt
Laden Sie die erforderliche Software herunter.	DDownload die folgende Software zusammen mit den erforderlichen Versionen und Patches von der Oracle-Website herunter: • Java JDK8 • Oracle WebLogic Server 12c	Migration Architect, Datenbankingenieur, Anwendungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Oracle BI 12c	
Bereiten Sie die Installat ionsskripts vor.	Erstellen Sie Softwareinstallati onsskripts, die eine Installat ion im Hintergrund ausführen . Diese Skripts vereinfachen die Bereitstellungsautomatisier ung. Weitere Informationen finden Sie unter OBIEE 12c: How to Perform Silent Installat ion? auf der Oracle Support-Website. Sie benötigen ein Oracle Support-Konto, um die Dokumentation anzuzeigen.	Migration Architect, Datenbank ingenieur, Anwendung sarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EBS-gestütztes Linux-AMI für Ihre Web- und Anwendung sebenen.	1. Stellen Sie Amazon EC2-Instances für Ihre Web- und Anwendungsebenen bereit und konfigurieren Sie sie. Stellen Sie sicher, dass die Instances die Vorausset zungen für die Ausführung der folgenden Bedingungen erfüllen: • Einrichtung der Oracle-Be triebssystemumgebung • Einrichten des Benutzerk ontos des Oracle-Be triebssystems • Java-Softwareinstallation 2. Erstellen Sie Amazon Machine Images (AMIs) der Instances und speichern Sie Kopien für die zukünftig e Verwendung. Anweisung en finden Sie unter Erstellen eines Amazon-EBS-gestützten Linux-AMI im Amazon EC2-Benut zerhandbuch für Linux-Ins tances.	Migration Architect, Datenbank ingenieur, Anwendung sarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Ihre AWS-Infrastruktur mithilfe von CloudFormation.	Stellen Sie Ihre Web- und Anwendungsebenen von Oracle BI 12c mithilfe der von Ihnen erstellten CloudFormation Vorlagen in Modulen bereit. Anweisungen finden Sie unter Erste Schritte mit AWS CloudFormation im AWS-CloudFormation Benutzerhandbuch.	Cloud Infrastructure Architect, Solutions Architect, Application Architect

Migrieren von Oracle BI 12c zu AWS mithilfe einer neuen Installation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stufen Sie die erforderliche Software ein.	Stellen Sie die erforderliche Software an einem Speicherort bereit, auf den die Amazon EC2 zugreifen können. Sie können beispielsweise die Software in Amazon S3 oder einer anderen Amazon EC2-Instance bereitstellen, auf die Ihre Web- und Anwendungsserver zugreifen können.	Migration Architect, Oracle BI Architect, Cloud Infrastructure Achitect, Solutions Architect, Application Architect
Bereiten Sie Ihre Repository-Datenbank für die Installation von Oracle BI 12c vor.	Erstellen Sie Oracle BI 12c-Schemas, indem Sie das Oracle Repository Creation Utility (RCU) vor einer neuen Datenbank-Instance von	Cloud Infrastructure Achitect, Solutions Architect, Application Architect, Migration Architect, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon RDS für Oracle ausführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle Fusion Middleware 12c und Oracle BI 12c.	1. Beginnend mit einer Amazon EC2-Instance installieren Sie die Infrastruktur von Oracle Fusion Middleware 12c und OBIEE 12c. Weitere Informationen finden Sie in den folgenden Abschnitten des Oracle Fusion Middleware Enterprise Deployment Guide für Oracle Business Intelligence: • Starten des Infrastrukturinstallationsprogramms auf BIHOST1 • Installieren von Oracle Business Intelligence zur Vorbereitung auf eine Unternehmensbereitstellung Hinweis: Verwenden Sie Amazon EFS, um Verzeichnisse zu hosten, die von Oracle-BI-12c-Clusterknoten gemeinsam genutzt werden. 2. Wenden Sie alle erforderlichen Patches auf die Installation an. 3. Erstellen Sie AMIs der Instances und speichern Sie Kopien für die zukünftige Verwendung.	Migration Architect, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihre Oracle WebLogic Server-Domain für Oracle BI 12c.	Konfigurieren Sie Ihre Oracle BI 12c-Domain als nicht gruppierte Bereitstellung. Weitere Informationen finden Sie unter Konfigurieren der BI-Domain im Oracle Fusion Middleware Enterprise-Bereitstellungshandbuch für Oracle Business Intelligence.	Migration Architect, Oracle BI Architect
Führen Sie eine horizontale Skalierung aus Oracle BI 12c durch.	Skalieren Sie den einzelnen Knoten horizontal auf die gewünschte Anzahl von Knoten. Weitere Informationen finden Sie unter Aufskalieren von Oracle Business Intelligence im Oracle Fusion Middleware Enterprise-Bereitstellungshandbuch für Oracle Business Intelligence.	Migration Architect, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle HTTP Server 12c.	1. Installieren Sie Oracle HTTP Server 12c auf den Oracle-Web-Tier-Amazon EC2. Anweisungen finden Sie unter Installieren von Oracle HTTP Server 12c in Installieren und Konfiguri eren von Oracle HTTP Server für Oracle Access Management 12c. 2. Wenden Sie alle erforderl ichen Patches auf die Installation an. 3. Erstellen Sie AMIs der Instances und speichern Sie Kopien für die zukünftig e Verwendung.	Migration Architect, Oracle BI Architect
Konfigurieren Sie Load Balancer für SSL-Beendigung.	1. Erstellen oder importieren Sie SSL-Zertifikate in ACM . 2. Ordnen Sie die SSL-Zerti fikate ELB zu.	Cloud Infrastructure Architect, Migration Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Business Intelligence-Metadatenartefakte zu AWS.	1. Exportieren Sie Oracle Business Intelligence Application Archive (BAR)-Dateien aus der lokalen Oracle BI 12c-Installation. Um die BAR-Dateien zu exportieren, verwenden Sie das WebLogic Scripting Tool (WLST) ,um den exportServiceInstance Befehl auszuführen. 2. Importieren Sie die lokalen BAR-Dateien in die AWS Oracle BI 12c-Installation. Führen Sie den importServiceInstance WLST-Befehl aus, um die BAR-Dateien zu importieren.	Migration Architect, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Aufgaben nach der Migration aus.	Gehen Sie nach dem Importieren der BAR-Dateien wie folgt vor: • Konfigurieren Sie alle zusätzlichen JDBC-Datenquellen. • Installieren Sie Treiber für andere Datenquellen wie PostgreSQL oder Amazon Redshift. • Konfigurieren Sie Oracle LDAP , SSL , Single Sign-On (SSO) und WebLogic Sicherheitsspeicher . • Konfigurieren Sie AWS Identity and Access Management (IAM)-Richtlinien. • Aktivieren Sie die Nutzungsnachverfolgung. • Richten Sie Integrationen in andere Systeme ein. • Migrieren Sie alle benutzerdefinierten Skripts.	Migration Architect, Oracle BI Architect

Testen der neuen Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die neue Oracle BI 12c-Umgebung.	Führen Sie end-to-end Tests in der neuen Oracle BI 12c-Umgebung durch. Verwenden	Migration Architect, Solutions Architect, Application Owner, Oracle BI Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Automatisierung so weit wie möglich. Beispiele für Testaktivitäten sind die folgenden: • Validieren von Dashboards, Berichten und URLs • Benutzerakzeptanztests (UAT) • Operative Akzeptanztests (OAT) Hinweis: Führen Sie bei Bedarf zusätzliche Tests und Validierungen durch.	

Umstellung auf die neue Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Trennen Sie den Datenverkehr zur lokalen Oracle BI 12c-Umgebung.	Stoppen Sie im Fenster für den Cutover den gesamten Datenverkehr zur lokalen Oracle BI 12c-Umgebung.	Migration Architect, Solutions Architect, Application Owner, Oracle BI Administrator
Synchronisieren Sie die neue Oracle BI 12c-Repository-Datenbank erneut mit der Quelldatenbank.	Synchronisieren Sie die Amazon RDS Oracle BI 12c-Repository-Datenbank erneut mit der On-Premises-Datenbank. Um die Datenbanken zu synchronisieren, können Sie entweder eine Oracle Data	Oracle-BI-Administrator, Datenbankingenieur/Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pump-Aktualisierung oder eine AWS DMS Change Data Capture (CDC) verwenden.	
Wechseln Sie Ihre Oracle BI 12c-URLs so, dass sie auf die neue AWS-Umgebung verweisen.	Aktualisieren Sie die Oracle BI 12c-URLs auf Ihren internen DNS-Servern, sodass sie auf die neue AWS-Installation verweisen.	Migration Architect, Solutions Architect, Application Owner, Oracle-BI-Administrator
Überwachen Sie die neue Umgebung.	Überwachen Sie die neue Oracle BI 12c-Umgebung mit einem der folgenden Tools: • Amazon CloudWatch • Amazon RDS Performance Insights • Oracle Enterprise Manager	Oracle-BI-Administrator, Datenbankingenieur/Administrator, Anwendungsadministrator
Holen Sie sich die Abmeldung für das Projekt.	Überprüfen Sie die Testergebnisse mit den Stakeholdern und holen Sie die erforderlichen Genehmigungen ein, um die Migration abzuschließen.	Application Owner, Service Owner, Cloud Infrastructure Architect, Migration Architect, Oracle BI Architect

Zugehörige Ressourcen

- Verwenden des Oracle Repository Creation Utility auf RDS für Oracle (Amazon-RDS-Benutzerhandbuch)
- Oracle in Amazon RDS (Amazon-RDS-Benutzerhandbuch)
- Oracle WebLogic Server 12c in AWS (AWS-Whitepaper)
- Bereitstellen von Oracle Business Intelligence für hohe Verfügbarkeit (Oracle Help Center)
- Oracle Business Intelligence Application Archive (BAR)-Dateien (Oracle Help Center)
- So migrieren Sie OBI 12c zwischen Umgebungen (Oracle Support)

Zusätzliche Informationen

Im Folgenden finden Sie eine Liste bewährter Methoden im Zusammenhang mit der Migration von Oracle BI 12c in die AWS Cloud.

Repository-Datenbanken

Es hat sich bewährt, Oracle BI 12c-Datenbankschemata auf einer Amazon RDS for Oracle-Instance zu hosten. Dieser Instance-Typ bietet kostengünstige und anpassbare Kapazität und automatisiert gleichzeitig Verwaltungsaufgaben wie Hardwarebereitstellung, Datenbankeinrichtung, Patching und Backups.

Weitere Informationen finden Sie unter Verwenden des Oracle Repository Creation Utility auf RDS für Oracle im Amazon-RDS-Benutzerhandbuch.

Web- und Anwendungsebenen

Arbeitsspeicheroptimierte Amazon EC2-Instances eignen sich oft gut für Oracle-BI-12c-Server. Unabhängig davon, welchen Instance-Typ Sie wählen, stellen Sie sicher, dass die von Ihnen bereitgestellten Instances die Speichernutzungsanforderungen Ihres Systems erfüllen. Stellen Sie außerdem sicher, dass Sie eine ausreichende WebLogic Java Virtual Machine (JVM)-Heap-Größe basierend auf dem verfügbaren Speicher Ihrer Amazon-EC2-Instance konfigurieren. Amazon EC2

Lokaler Speicher

E/A spielt eine wichtige Rolle für die Gesamtleistung Ihrer Oracle BI 12c-Anwendung. Amazon Elastic Block Store (Amazon EBS) bietet verschiedene Speicherklassen, die für verschiedene Workload-Muster optimiert sind. Stellen Sie sicher, dass Sie einen Amazon-EBS-Volume-Typ auswählen, der zu Ihrem Anwendungsfall passt.

Weitere Informationen zu EBS-Volume-Typen finden Sie unter Amazon-EBS-Funktionen in der Amazon-EBS-Dokumentation.

Freigegebener Speicher

Eine geclusterte Oracle BI 12c-Domain erfordert gemeinsamen Speicher für die folgenden Ressourcen:

- Konfigurationsdateien
- Oracle BI 12c Singleton-Datenverzeichnis (SDD)

- Globaler Oracle-Cache
- Oracle-BI-Scheduler-Skripts
- Oracle WebLogic Server-Binärdateien

Sie können diese Anforderung an den gemeinsam genutzten Speicher erfüllen, indem Sie Amazon EFS verwenden, das ein skalierbares, vollständig verwaltetes Elastic Network File System (NFS)-Dateisystem bietet.

Feinabstimmung der Leistung des gemeinsam genutzten Speichers

Amazon EFS hat zwei Durchsatzmodi: Bereitgestellt und Bursting. Der Service hat auch zwei Leistungsmodi: Allzweck und Max. E/A.

Um die Leistung zu optimieren, testen Sie zunächst Ihre Workloads im Allzweck-Leistungsmodus und im Modus mit bereitgestelltem Durchsatz. Durch diese Tests können Sie feststellen, ob diese Basismodi ausreichen, um die gewünschten Servicelevels zu erreichen.

Weitere Informationen finden Sie unter Amazon-EFS-Leistung im Amazon-EFS-Benutzerhandbuch.

Verfügbarkeit und Notfallwiederherstellung

Es hat sich bewährt, Oracle BI 12c-Komponenten in mehreren Availability Zones bereitzustellen, um diese Ressourcen im Falle eines Ausfalls der Availability Zone zu schützen. Im Folgenden finden Sie eine Liste der bewährten Methoden für Verfügbarkeit und Notfallwiederherstellung für bestimmte Oracle BI 12c-Ressourcen, die in der AWS Cloud gehostet werden:

- Oracle-BI-12c-Repository-Datenbanken: Stellen Sie eine Multi-AZ-Amazon-RDS-Datenbank-Instance in Ihrer Oracle-BI-12-Repository-Datenbank bereit. Bei einer Multi-AZ-Bereitstellung stellt Amazon RDS automatisch ein synchrones Standby-Replikat in einer anderen AZ bereit und verwaltet es. Das Ausführen einer Oracle BI 12c-Repository-Datenbank-Instance über Availability Zones hinweg kann die Verfügbarkeit bei geplanten Systemwartungen verbessern und Ihre Datenbanken vor Instance- und Availability Zone-Ausfällen schützen.
- Oracle BI 12c Managed Servers: Um Fehlertoleranz zu erreichen, empfiehlt es sich, Oracle BI 12c-Systemkomponenten auf verwalteten Servern in einer Amazon EC2 Auto Scaling-Gruppe bereitzustellen, die für mehrere Availability Zones konfiguriert ist. Auto Scaling ersetzt fehlerhafte Instances basierend auf Amazon EC2-Zustandsprüfungen. Im Falle eines Ausfalls der Availability Zone leiten Oracle HTTP Server weiterhin Datenverkehr an verwaltete Server in der funktionierenden Availability Zone weiter. Anschließend startet Auto Scaling Instances,

um mit Ihren Anforderungen an die Hostanzahl Schritt zu halten. Es wird empfohlen, die HTTP-Sitzungsstatusreplikation zu aktivieren, um sicherzustellen, dass ein reibungsloses Failover der vorhandenen Sitzungen auf die funktionierenden Managed Server erfolgt.

- Oracle BI 12c Administration Servers: Um sicherzustellen, dass Ihr Administration Server über hohe Verfügbarkeit verfügt, hosten Sie ihn in einer Amazon EC2 Auto Scaling-Gruppe, die so konfiguriert ist, dass sie sich über mehrere Availability Zones erstreckt. Legen Sie dann die minimale und maximale Größe der Gruppe auf 1 fest. Wenn eine Availability Zone ausfällt, startet Amazon EC2 Auto Scaling einen Ersatz-Administratorserver in einer alternativen Availability Zone. Um ausgefallene zugrunde liegende Hosts innerhalb derselben Availability Zone wiederherzustellen, können Sie Amazon EC2 Auto Recovery aktivieren.
- Oracle Web Tier-Server: Es hat sich bewährt, Ihren Oracle HTTP Server mit Ihrer Oracle WebLogic Server-Domain zu verknüpfen. Stellen Sie für hohe Verfügbarkeit Ihren Oracle HTTP Server in einer Amazon EC2 Auto Scaling-Gruppe bereit, die so konfiguriert ist, dass mehrere Availability Zones zugewiesen werden. Platzieren Sie dann den Server hinter einem ELB Elastic Load Balancer. Um zusätzlichen Schutz vor Host-Ausfällen zu bieten, können Sie Amazon EC2 Auto Recovery aktivieren.

Skalierbarkeit

Die Elastizität der AWS Cloud hilft Ihnen dabei, Anwendungen entweder horizontal oder vertikal als Reaktion auf Workload-Anforderungen zu skalieren.

Vertikale Skalierung

Um Ihre Anwendung vertikal zu skalieren, können Sie die Größe und den Typ der Amazon EC2-Instances ändern, auf denen Ihre Oracle BI 12c-Komponenten ausgeführt werden. Sie müssen Instances zu Beginn Ihrer Bereitstellung nicht übermäßig bereitstellen und es fallen unnötige Kosten an.

Horizontale Skalierung

Amazon EC2 Auto Scaling unterstützt Sie bei der horizontalen Skalierung Ihrer Anwendung, indem verwaltete Server basierend auf den Workload-Anforderungen automatisch hinzugefügt oder entfernt werden.

Hinweis: Die horizontale Skalierung mit Amazon EC2 Auto Scaling erfordert Skriptierfähigkeiten und gründliche Tests zur Implementierung.

Backup und Wiederherstellung

Im Folgenden finden Sie eine Liste der bewährten Methoden für Backup und Wiederherstellung für bestimmte Oracle BI 12c-Ressourcen, die in der AWS Cloud gehostet werden:

- Metadaten-Repositorys von Oracle Business Intelligence: Amazon RDS erstellt und speichert automatisch Backups Ihrer Datenbank-Instances. Diese Backups werden für einen von Ihnen angegebenen Zeitraum aufbewahrt. Stellen Sie sicher, dass Sie Ihre Einstellungen für die Dauer und Aufbewahrung von Amazon-RDS-Sicherungen auf der Grundlage Ihrer Datenschutzanforderungen konfigurieren. Weitere Informationen finden Sie unter Amazon-RDS-Backup und -Wiederherstellung.
- Verwaltete Server, Administrationsserver und Web-Tier-Server: Stellen Sie sicher, dass Sie Amazon-EBS-Snapshots basierend auf Ihren Datenschutz- und Aufbewahrungsanforderungen konfigurieren.
- Freigegebener Speicher: Sie können Backup und Wiederherstellung für Dateien verwalten, die in Amazon EFS gespeichert sind, indem Sie AWS Backup verwenden. Der AWS Backup-Service kann auch bereitgestellt werden, um die Sicherung und Wiederherstellung anderer -Services, einschließlich Amazon EC2, Amazon EBS und Amazon RDS, zentral zu verwalten. Weitere Informationen finden Sie unter Was ist AWS Backup? Im AWS Backup-Entwicklerhandbuch .

Sicherheit und Compliance

Im Folgenden finden Sie eine Liste bewährter Sicherheitsmethoden und AWS-Services, die Ihnen beim Schutz Ihrer Oracle BI 12c-Anwendungen in der AWS Cloud helfen können:

- Verschlüsselung im Ruhezustand: Amazon RDS, Amazon EFS und Amazon EBS unterstützen alle branchenübliche Verschlüsselungsalgorithmen. Sie können AWS Key Management Service (AWS KMS) verwenden, um kryptografische Schlüssel zu erstellen und zu verwalten und deren Verwendung in AWS-Services und in Ihren Anwendungen zu steuern. Sie können Oracle Transparent Data Encryption (TDE) auch auf der Datenbank-Instance von Amazon RDS für Oracle konfigurieren, die Ihre Oracle-BI-12c-Repository-Datenbank hostet.
- Verschlüsselung während der Übertragung: Es hat sich bewährt, entweder SSL- oder TLS-Protokolle zu aktivieren, um Daten während der Übertragung zwischen den verschiedenen Ebenen Ihrer Oracle BI 12c-Installation zu schützen. Sie können AWS Certificate Manager (ACM) verwenden, um öffentliche und private SSL- und TLS-Zertifikate für Ihre Oracle BI 12c-Ressourcen bereitzustellen, zu verwalten und bereitzustellen.
- Netzwerksicherheit: Stellen Sie sicher, dass Sie Ihre Oracle BI 12c-Ressourcen in einer Amazon VPC bereitstellen, für die die entsprechenden Zugriffskontrollen für Ihren Anwendungsfall

konfiguriert sind. Konfigurieren Sie Ihre Sicherheitsgruppen, um ein- und ausgehenden Datenverkehr von den Amazon EC2-Instances zu filtern, auf denen Ihre Installation ausgeführt wird. Stellen Sie außerdem sicher, dass Sie Network Access Control Lists (NACLs) konfigurieren, die Datenverkehr basierend auf definierten Regeln zulassen oder verweigern.

- Überwachung und Protokollierung: Sie können AWS CloudTrail verwenden, um API-Aufrufe an Ihre AWS-Infrastruktur zu verfolgen, einschließlich Ihrer Oracle BI 12c-Ressourcen. Diese Funktionalität ist nützlich, wenn Änderungen an der Infrastruktur verfolgt werden oder wenn eine Sicherheitsanalyse durchgeführt wird. Sie können Amazon CloudWatch auch verwenden, um Betriebsdaten anzuzeigen, die Ihnen einen umsetzbaren Einblick in die Leistung und den Zustand Ihrer Oracle BI 12c-Anwendung bieten können. Sie können auch Alarme konfigurieren und automatisierte Aktionen basierend auf diesen Alarmen ausführen. Amazon RDS bietet zusätzliche Überwachungstools, darunter Enhanced Monitoring und Performance Insights.

Migrieren eines lokalen Apache-Kafka-Clusters zu Amazon MSK mithilfe von MirrorMaker

Erstellt von Zhang (AWS) und Tanner Prattt (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises- oder selbstverwalteter Apache-Kafka-Cluster	Ziel: Amazon Managed Streaming für Apache Kafka (Amazon MSK)
R-Typ: Plattformwechsel	Workload: Open-Source; Alle anderen Workloads	Technologien: Analytik; Big Data; Migration
AWS-Services: Amazon MSK		

Übersicht

Dieses Muster bietet Anleitungen für die Migration eines lokalen, selbstverwalteten oder gehosteten Apache-Kafka-Clusters zu Amazon Managed Streaming für Apache Kafka (Amazon MSK). Sie können dieses Muster auch verwenden, um von einem Amazon-MSK-Cluster zu einem anderen zu migrieren.

Apache Kafka enthält das MirrorMaker Feature , das Daten zwischen zwei Kafka- MirrorMaker Clustern repliziert.besteht aus einer Sammlung von Verbrauchern, die Teil einer Verbrauchergruppe sind. Die Verbraucher lesen Daten aus den Themen im Quell-Cluster und übergeben diese Daten dann an Produzenten, die die Daten in den Ziel-Cluster schreiben.

Die Amazon-MSK-Dokumentation enthält einen allgemeinen Überblick über den Prozess zur Verwendung von MirrorMaker Version 1.0 zur Migration von On-Premises-Kafka-Clustern zu Amazon MSK. Dieses Muster ergänzt diese Informationen durch umfassende step-by-step Anweisungen zur Verwendung von MirrorMaker Version 2.0.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Ein Kafka-Quell-Cluster, der einer der folgenden ist:
  - In einem On-Premises-Rechenzentrum
  - Selbstverwaltet in der Cloud
  - Wird über einen Partner gehostet

Einschränkungen

- Um MirrorMaker Version 2.0 verwenden zu können, muss der Quell-Cluster Apache Kafka Version 2.4.0 oder höher verwenden. Informationen zu früheren Versionen finden Sie in den Anweisungen in der Amazon-MSK-Dokumentation zur Verwendung von MirrorMaker Version 1.0.

Produktversionen

- MirrorMaker Version 2.0
- Apache Kafka Version 2.4.0 oder höher. Weitere Informationen zu den Versionen von Apache Kafka, die Amazon MSK unterstützt, finden Sie unter Unterstützte Apache-Kafka-Versionen.

Architektur

Quelltechnologie-Stack

- Lokaler oder selbstverwalteter Kafka-Cluster

Zieltechnologie-Stack

- Amazon-MSK-Cluster

Zielarchitektur

Das Diagramm zeigt den folgenden Prozess:

1. MirrorMaker liest die Daten aus den Themen und Verbrauchergruppen im Quell-Kafka-Cluster.
2. MirrorMaker repliziert die Daten und Verbraucherinformationen auf den Amazon-MSK-Ziel-Cluster.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Andere Tools

- Apache Kafka ist eine Open-Source-Event-Streaming-Plattform. In diesem Muster verwenden Sie das MirrorMaker Feature von Kafka, um die Cluster-übergreifende Migration durchzuführen.

Bewährte Methoden

Sie können MirrorMaker auf entweder in der Quell- oder in der Zielumgebung ausführen, es wird jedoch empfohlen, sie so nah wie möglich am Ziel-Cluster auszuführen. Weitere Informationen finden Sie unter Bewährte Methode: Aus der Ferne nutzen, In lokal produzieren in der Apache-Kafka-Dokumentation.

Polen

Erstellen der VPC und Ziel-Amazon-MSK-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	1. Erstellen Sie eine VPC im AWS-Zielkonto. Anweisungen finden Sie unter Erstellen einer VPC.	AWS-Systemadministrator, DevOps Techniker, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erstellen Sie drei private Subnetze in verschiedenen Availability Zones in der neuen VPC. Anweisungen finden Sie unter Erstellen eines Subnetzes. Die Verwendung verschiedener Availability Zones bietet hohe Verfügbarkeit und Fehlertoleranz. Hinweis: Wenn Sie eine öffentliche Internetv erbindung verwenden , um den Kafka-Cluster zu migrieren, erstellen Sie öffentliche Subnetze und aktivieren Sie den öffentlichen Zugriff auf den Amazon-MSK-Cluster.	
Erstellen Sie den Amazon-MSK-Cluster.	Erstellen Sie einen Amazon-MSK-Cluster. Anweisungen finden Sie unter Erstellen eines Clusters mit der AWS-Managementkonsole oder Erstellen eines Clusters mit der AWS CLI. Konfiguri eren Sie den Cluster für die Verwendung der VPC und der Subnetze, die Sie zuvor erstellt haben.	AWS-Systemadministrator, DevOps Techniker, Cloud-Administrator

Einrichten MirrorMaker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie MirrorMaker.	1. Starten Sie eine EC2-Instance. 2. Stellen Sie eine Verbindung zu Ihrer EC2-Instance her. 3. Laden Sie auf der EC2-Instance die neueste Kafka-Version herunter und extrahieren Sie sie. Anweisungen finden Sie unter Schnellstart (Kafka-Dokumentation). Hinweis: In diesem Muster installieren Sie MirrorMaker2.0 als dedizierten MirrorMaker Cluster auf einer Amazon EC2. Diese Option ist für Entwicklungsumgebungen akzeptabel und ist der Ansatz, der in diesem Muster verwendet wird. Weitere Informationen zu anderen Bereitstellungsoptionen für MirrorMaker2.0 finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	AWS-Systemadministrator, Cloud-Administrator, DevOps Engineer
Geben Sie Kafka-Cluster-Informationen an.	Erstellen Sie im `bin` Installationsordner des Kafka-Clients eine mm2.properties-Datei und konfigurieren Sie sie für Ihren Quell-Kafka-Cluster.	AWS-Systemadministrator, Cloud-Administrator, DevOps Engineer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie unter Ausführen eines dedizierten MirrorMaker Clusters (Kafka-Dokumentation).	
Starten Sie MirrorMaker.	Geben Sie den folgenden Befehl ein, um die Datei mm2.properties zu starten MirrorMaker und zu übergeben. `$ ./bin/connect-mirror-maker.sh mm2.properties`	AWS-Systemadministrator, Cloud-Administrator, DevOps Engineer
Überwachen Sie den Fortschritt.	Überprüfen Sie den Fortschritt, indem Sie die Verzögerung zwischen dem letzten Offset für jedes Thema und dem aktuellen Offset für das Thema überprüfen MirrorMaker . Anweisungen finden Sie unter Überwachung der Georeplikation in der Kafka-Dokumentation.	AWS-Systemadministrator, Cloud-Administrator, DevOps Engineer

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die Verbrauchseranwendungen an.	Halten Sie alle Konsumentenanwendungen an, die Daten aus dem Quell-Cluster verbrauchen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Konsumentenanwendungen.	Ändern Sie die Bootstrap-Konfiguration der Anwendungen so, dass sie auf den Ziel-Cluster verweist. Beginnen Sie dann mit der Nutzung auf dem Ziel-Cluster.	App-Developer
Halten Sie die Produzenten auf dem Quell-Cluster an.	Wenn die Konsumentenanwendungen erfolgreich auf dem Ziel-Cluster verbrauchen, halten Sie die Produzenten auf dem Quell-Cluster an.	App-Developer
Starten Sie die Produzenten auf dem Ziel-Cluster.	Ändern Sie die Bootstrap-Server des Produzenten und zeigen Sie auf den Ziel-Cluster. Warten Sie MirrorMaker , bis die Spiegelung aller Daten aus dem Quell-Cluster abgeschlossen hat, bevor Sie die Produzenten starten.	App-Developer
Stoppen Sie MirrorMaker.	Nachdem Produzenten in den Ziel-Cluster verschoben wurden, stoppen Sie MirrorMaker.	AWS-Systemadministrator, Cloud-Administrator, DevOps Engineer

Zugehörige Ressourcen

AWS-Ressourcen

- Migrieren von Clustern mit MirrorMaker (Amazon-MSK-Dokumentation)
- Amazon-MSK-Migrationsumgebungen (AWS-Workshop-Studio)

Sonstige Ressourcen

- MirrorMaker 2.0 (Verbesserungsvorschläge für Apache Kafka)
- Geo-Replikation: Clusterübergreifende Datenspiegelung (Apache-Kafka-Dokumentation)

Zusätzliche Informationen

Dieses Muster führt MirrorMaker 2.0 als dedizierter MirrorMaker Cluster auf Amazon EC2 aus. Diese Option ist für Entwicklungsumgebungen akzeptabel. Obwohl es in diesem Muster nicht behandelt wird, können Sie MirrorMaker 2.0 auch in einem Kafka-Connect-Cluster ausführen. Diese Bereitstellungsoption verwendet ein Framework im Kafka-Ökosystem, das Skalierung und Wartung verbessert. Sie stellen den Konnektor in einem Kafka-Connect-Cluster mit der zugehörigen Konfiguration bereit, um die Anwendung auszuführen. Der Konnektor kann im eigenständigen Modus für Entwicklung oder Tests oder im verteilten Modus für die Produktion ausgeführt werden. Weitere Informationen finden Sie unter In MirrorMaker einem Connect-Cluster ausführen (Apache-Kafka-Dokumentation). Weitere Informationen zu anderen MirrorMaker 2.0-Bereitstellungsoptionen finden Sie unter Walkthrough: Running MirrorMaker 2.0 (Kafka-Dokumentation).

Migrieren eines ELK-Stacks zu Elastic Cloud in AWS

Erstellt von Battulga Bolvragchaa (AWS), Uday Reddy und Antony Prasad Thevaraj (AWS)

Umgebung: Produktion	Quelle: Elasticsearch	Ziel: Elastic Cloud
R-Typ: Plattformwechsel	Workload: Alle anderen Workloads	Technologien: Analytik; Sicherheit, Identität, Compliance
AWS-Services: Amazon EC2; Amazon EC2 Auto Scaling; Elastic Load Balancing (ELB); Amazon S3; Amazon Route 53		

Übersicht

Elastic stellt seit vielen Jahren Services bereit, wobei ihre Benutzer und Kunden Elastic selbst in der Regel On-Premises verwalten. Elastic Cloud, der verwaltete Elasticsearch-Service , bietet eine Möglichkeit, den Elastic Stack (ELK Stack) und Lösungen für die Unternehmenssuche , Beobachtbarkeit und Sicherheit zu nutzen. Sie können auf Elastic-Lösungen mit Apps wie Protokollen, Metriken, APM (Überwachung der Anwendungsleistung) und SIEM (Sicherheitsinformationen und Ereignismanagement) zugreifen. Sie können integrierte Funktionen wie Machine Learning, Index-Lebenszyklusmanagement, Kibana Lens (für Drag-and-Drop-Visualisierungen) verwenden.

Wenn Sie von selbstverwaltetem Elasticsearch zu Elastic Cloud wechseln, kümmert sich der Elasticsearch-Service um Folgendes:

- Bereitstellung und Verwaltung der zugrunde liegenden Infrastruktur
- Erstellen und Verwalten von Elasticsearch-Clustern
- Skalieren von Clustern nach oben und unten
- Upgrades, Patches und Erstellen von Snapshots

Dadurch haben Sie mehr Zeit, sich auf die Lösung anderer Herausforderungen zu konzentrieren.

Dieses Muster definiert, wie Sie lokale Elasticsearch 7.13 zu Elasticsearch in Elastic Cloud auf Amazon Web Services (AWS) migrieren. Andere Versionen erfordern möglicherweise geringfügige Änderungen an den Prozessen, die in diesem Muster beschrieben sind. Weitere Informationen erhalten Sie von Ihrem Elastic-Mitarbeiter.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit Zugriff auf Amazon Simple Storage Service (Amazon S3) für Snapshots
- Ein sicherer privater Link mit ausreichend hoher Bandbreite zum Kopieren von Snapshot-Datendateien nach Amazon S3
- Amazon S3 Transfer Acceleration
- Elastic-Snapshot-Richtlinien zur regelmäßigen Archivierung der Datenaufnahme, entweder in einem ausreichend großen lokalen Datenspeicher oder in einem Remote-Speicher (Amazon S3)

Sie müssen verstehen, wie groß Ihre Snapshots und die Lebenszyklusrichtlinien für dazugehörige Indizes vor Ort sind, bevor Sie Ihre Migration einleiten. Weitere Informationen erhalten Sie von Elastic .

Rollen und Fähigkeiten

Der Migrationsprozess erfordert auch die in der folgenden Tabelle beschriebenen Rollen und das Fachwissen.

Rolle	Bol	Verantwortlichkeiten
App-Unterstützung	Vertrautheit mit Elastic Cloud und Elastic On-Premises	Alle Elastic-bezogenen Aufgaben
Systemadministrator oder DBA	Fundierte Kenntnisse der lokalen Elastic-Umgebung und ihrer Konfiguration	Die Möglichkeit, Speicher bereitzustellen, die AWS Command Line Interface (AWS CLI) zu installieren und zu verwenden und alle Datenquellen zu identifizieren, die Elastic On-Premises speist

Netzwerkadministrator	Kenntnisse über On-Premises-Netzwerkkonnektivität, Sicherheit und Leistung von AWS	Einrichtung von Netzwerkverbindungen von On-Premises zu Amazon S3 mit einem Verständnis der Konnektivitätsbandbreite

Einschränkungen

- Elasticsearch in Elastic Cloud ist nur in unterstützten AWS-Regionen (September 2021) verfügbar.

Produktversionen

- Elasticsearch 7.13

Architektur

Quelltechnologie-Stack

Lokale Elasticsearch 7.13 oder höher:

- Cluster-Snapshots
- Index-Snapshots
- Beats-Konfiguration

Quelltechnologiearchitektur

Das folgende Diagramm zeigt eine typische On-Premises-Architektur mit unterschiedlichen Erfassungsmethoden, Knotentypen und Kibana. Die verschiedenen Knotentypen spiegeln die Elasticsearch-Cluster-, Authentifizierungs- und Visualisierungsrollen wider.

1. Aufnahme von Beats in Logstash
2. Aufnahme von Beats in die Apache-Kafka-Messaging-Warteschlange
3. Aufnahme von Filebeat in Logstash
4. Aufnahme aus der Apache-Kafka-Messaging-Warteschlange in Logstash

5. Aufnahme von Logstash in einen Elasticsearch-Cluster
6. Elasticsearch-Cluster
7. Authentifizierungs- und Benachrichtigungsknoten
8. Kibana- und Blob-Knoten

Zieltechnologie-Stack

Elastic Cloud wird für Ihr Software as a Service (SaaS)-Konto in mehreren AWS-Regionen mit Cluster-übergreifender Replikation bereitgestellt.

- Cluster-Snapshots
- Index-Snapshots
- Beats-Konfigurationen
- Elastic Cloud
- Network Load Balancer
- Amazon Route 53
- Amazon S3

Zielarchitektur

Die verwaltete Elastic Cloud-Infrastruktur ist:

- Hochverfügbar, in mehreren Availability Zones und mehreren AWS-Regionen vorhanden.
- Regionsfehlertolerant, da Daten (Indizes und Snapshots) mit der clusterübergreifenden Elastic Cloudcross-Replikation (CCR) repliziert werden
- Archivierung, da Snapshots in Amazon S3 archiviert werden
- Netzwerkpartition tolerant durch eine Kombination aus Network Load Balancern und Route 53
- Datenerfassung von (aber nicht beschränkt auf) Elastic APM , Beats , Logstash

Schritte zur Migration auf hoher Ebene

Elastic hat eine eigene präskriptive Methode für die Migration von lokalen Elastic Clustern zu Elastic Cloud entwickelt. Die Elastic-Methode ist direkt abgestimmt und ergänzt die AWS-

Migrationsrichtlinien und bewährten Methoden, einschließlich Well-Architected Framework und AWS Migration Acceleration Program (MAP). In der Regel sind die drei AWS-Migrationsphasen die folgenden:

- Bewerten
- Mobilisieren
- Migrieren und modernisieren

Elastic folgt ähnlichen Migrationsphasen mit ergänzender Terminologie:

- Initiieren
- Plan
- Implementieren von
- Bereitstellen
- Schließen

Elastic verwendet die Elastic Implementation Methodology, um die Bereitstellung von Projektergebnissen zu erleichtern. Dies ist beabsichtigt, um sicherzustellen, dass die Elastic-, Beratungs- und Kundenteams klar zusammenarbeiten, um gemeinsam die angestrebten Ergebnisse zu erzielen.

Die Elastic-Methode kombiniert herkömmliche Wasserfallphasen mit Scrum innerhalb der Implementierungsphase. Konfigurationen technischer Anforderungen werden iterativ und kollaborativ bereitgestellt und gleichzeitig das Risiko minimiert.

Tools

AWS-Services

- Amazon Route 53 – Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS)-Webservice. Sie können Route 53 zum Durchführen von drei wesentlichen Aufgaben in beliebiger Kombination verwenden: Domänenregistrierung, DNS-Routing und Zustandsprüfung.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet

speichern und aufrufen. Dieses Muster verwendet einen S3-Bucket und Amazon S3 Transfer Acceleration .

- Elastic Load Balancing – Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, z. B. EC2-Instances, Container und IP-Adressen, in einer oder mehreren Availability Zones.

Andere Tools

- Beats – Beats liefern Daten aus Logstash oder Elasticsearch
- Elastic Cloud – Elastic Cloud ist ein verwalteter Service zum Hosten von Elasticsearch.
- Elasticsearch – Elasticsearch ist eine Such- und Analyse-Engine, die den Elastic Stack verwendet, um Ihre Daten für Suchen und Analysen, die skaliert werden, zentral zu speichern. Dieses Muster verwendet auch die Snapshot-Erstellung und die Cluster-übergreifende Replikation.
- Logstash – Logstash ist eine serverseitige Datenverarbeitungspipeline, die Daten aus mehreren Quellen aufnimmt, transformiert und dann an Ihren Datenspeicher sendet.

Polen

Vorbereiten der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Server, auf denen die lokale Elastic-L ösung ausgeführt wird.	Vergewissern Sie sich, dass die Elastic-Migration unterstüt zt wird.	App-Besitzer
Machen Sie sich mit der On-Premises-Serverkonfiguration vertraut.	Um die Serverkonfiguration zu verstehen, die erforderlich ist, um Workloads erfolgrei ch On-Premises zu steuern, ermitteln Sie den Hardwareb edarf des Servers, die Netzwerkkonfiguration und die Speichermerkmale, die derzeit verwendet werden	-App-Unterstützung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie Benutzer- und App-Kontoinformationen.	Identifizieren Sie die Benutzernamen und App-Namen, die von der lokalen Elastic-Umgebung verwendet werden.	Systemadministrator, -App-Unterstützung
Document Beats und Daten-Sender-Konfiguration.	Um die Konfigurationen zu dokumentieren, schauen Sie sich vorhandene Datenquel len und Senken an. Weitere Informationen finden Sie in der Elastic-Dokumentation.	App-Unterstützung
Bestimmen Sie die Geschwind igkeit und das Datenvolumen.	Richten Sie eine Grundlage dafür ein, wie viele Daten der Cluster verarbeitet.	Systemadministrator, -App-Unterstützung
Dokumentieren Sie RPO- und RTO-Szenarien.	Szenarien für Document Recovery Point Objective (RPO) und Recovery Time Objective (RTO) in Bezug auf Ausfälle und Service Level Agreements (SLAs).	App-Besitzer, Systemadm inistrator, App-Unterstützung
Bestimmen Sie die optimalen Einstellungen für den Snapshot-Lebenszyklus.	Definieren Sie, wie oft Daten gesichert werden müssen, indem Sie während und nach der Migration Elastic Snapshots verwenden.	App-Besitzer, Systemadm inistrator, App-Unterstützung
Definieren Sie die Erwartung en an die Leistung nach der Migration.	Generieren Sie Metriken zur aktuellen und erwartete n Bildschirmaktualisierung, Abfragelaufzeiten und zum Verhalten der Benutzero berfläche.	Systemadministrator, -App-Unterstützung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie die Anforderungen an den Transport, die Bandbreite und die Verfügbarkeit des Internetzugangs.	Stellen Sie Geschwindigkeit, Latenz und Ausfallsicherheit von Internetverbindungen zum Kopieren von Snapshots nach Amazon S3 sicher.	Netzwerkadministrator
Dokumentieren Sie die aktuellen Kosten der On-Premises-Laufzeit für Elastic.	Stellen Sie sicher, dass die Größe der AWS-Zielumgebung sowohl leistungsfähig als auch kostengünstig ist.	DBA, Systemadministrator, App-Unterstützung
Identifizieren Sie die Authentifizierungs- und Autorisierungsanforderungen.	Die Elastic-Stack-Sicherheitsfunktionen bieten integrierte Bereiche wie Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML) und OpenID Connect (OIDC).	DBA, Systemadministrator, App-Unterstützung
Machen Sie sich mit den spezifischen regulatorischen Anforderungen auf der Grundlage des geografischen Standorts vertraut.	Stellen Sie sicher, dass Daten gemäß Ihren Anforderungen und allen relevanten nationalen Anforderungen exportiert und verschlüsselt werden.	DBA, Systemadministrator, App-Unterstützung

Implementieren der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Staging-Bereich auf Amazon S3 vor.	Um Snapshots auf Amazon S3 zu erhalten, erstellen Sie einen S3-Bucket und eine temporäre AWS Identity and Access Management (IAM)-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Rolle mit vollem Zugriff auf Ihren neu erstellten Bucket. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer. Verwenden Sie den AWS Security Token Service, um temporäre Sicherheitsanmeldeinformationen anzufordern. Schützen Sie die Zugriffsschlüssel-ID, den geheimen Zugriffsschlüssel und das Sitzungstoken. Aktivieren Sie Amazon S3 Transfer Acceleration für den Bucket.	
Installieren Sie AWS CLI und das Amazon S3-Plugin On-Premises.	Führen Sie auf jedem Elasticsearch-Knoten den folgenden Befehl aus. `sudo bin/elasticsearch-plugin install repository-s3` Starten Sie dann den Knoten neu.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Amazon S3-Clientzugriff.	Fügen Sie die zuvor erstellten Schlüssel hinzu, indem Sie die folgenden Befehle ausführen.
	`elasticsearch-keystore add s3.client.default.access_key`
	`elasticsearch-keystore add s3.client.default.secret_key`
	`elasticsearch-keystore add s3.client.default.session_token`
		AWS-Administrator

Registrieren eines Snapshot-Repositorys für Elastic-Daten	Verwenden Sie die Kibana-Entwicklungstools, um dem lokalen On-Premises-Cluster mitzuteilen, in welchen Remote-S3-Bucket geschrieben werden soll.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Snapshot-Richtlinie.	Um die Snapshot-Lebenszyklusverwaltung zu konfigurieren, wählen Sie auf der Registerkarte Kibana-Richtlinien die Option SLM-Richtlinie aus und legen Sie fest, welche Zeiten, Datenströme oder Indizes enthalten sein sollen und welche Namen verwendet werden sollen. Konfigurieren Sie eine Richtlinie, die häufig Snapshots erstellt. Snapshots sind inkrementell und nutzen effizient Speicher. Stimmen Sie mit Ihrer Entscheidung zur Bereitschaftsbewertung überein. Eine Richtlinie kann auch eine Aufbewahrungsrichtlinie angeben und Snapshots automatisch löschen, wenn sie nicht mehr benötigt werden.	App-Unterstützung
Stellen Sie sicher, dass Snapshots funktionieren.	Führen Sie in den Kibana-Entwicklungstools den folgenden Befehl aus. `GET _snapshot/<your_repo_name>/_all`	AWS-Administrator, App-Unterstützung,

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen neuen Cluster in Elastic Cloud bereit.	Melden Sie sich bei Elastic an und wählen Sie einen Cluster für „Beobachtbarkeit, Suche oder Sicherheit“, der aus Ihren Geschäftsergebnissen in der Bereitschaftsbewertung abgeleitet wird.	AWS-Administrator, App-Unterstützung
Richten Sie den Zugriff auf den Cluster-Schlüsselspeicher ein.	Der neue Cluster benötigt Zugriff auf den S3-Bucket, der die Snapshots speichert. Wählen Sie in der Elasticsearch-Servicekonsole Sicherheit und geben Sie die Zugriffs- und geheimen IAM-Schlüssel ein, die Sie zuvor erstellt haben.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den von Elastic Cloud gehosteten Cluster für den Zugriff auf Amazon S3.	Richten Sie einen neuen Clusterzugriff auf das zuvor erstellte Snapshot-Repository in Amazon S3 ein. Gehen Sie mit Kibana wie folgt vor: 1. Wählen Sie Stack-Verwaltung, Snapshot-Einstellungen, RegisterRepo. 2. Geben Sie im Feld Alias den Namen des Repositorys ein. 3. Wählen Sie für S3-Clientname die Option sekundäres aus. 4. Fügen Sie den S3-Bucket, den Sie zuvor erstellt haben, dem Repository hinzu. 5. Wählen Sie Snapshot komprimieren aus. 6. Behalten Sie für die Verschlüsselungseinstellungen die Standardwerte bei.	AWS-Administrator, App-Unterstützung
Überprüfen Sie das neue Amazon S3-Repository.	Stellen Sie sicher, dass Sie auf Ihr neues Repository zugreifen können, das im Elastic Cloud-Cluster gehostet wird.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initiieren Sie den Elasticsearch-Service-Cluster.	Initialisieren Sie in der Elasticsearch-Servicekonsole den Elasticsearch-Service-Cluster aus dem S3-Snapshot.
	
	Führen Sie die folgenden Befehle als POST aus.
	
	`*/_close?expand_wildcards=all`
	
	`/_snapshot/<your-repo-name>/  <your-snapshot-name>/_restore`
	
	`*/_open?expand_wildcards=all`
		-App-Unterstützung

Schließen Sie die Migration ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob die Snapshot-Wiederherstellung erfolgreich war.	Führen Sie mit den Kibana-Entwicklertools den folgenden Befehl aus. `GET _cat/indices`	App-Unterstützung
Stellen Sie Aufnahmeservices erneut bereit.	Verbinden Sie die Endpunkte für Beats und Logstash mit dem neuen Elasticsearch-Service-Endpunkt.	App-Unterstützung

Testen der Cluster-Umgebung und Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Cluster-Umgebung.	Nachdem die lokale Elastic Cluster-Umgebung zu AWS migriert wurde, können Sie eine Verbindung zu ihr herstellen und Ihre eigenen Tools für Benutzerakzeptanztests (UAT) verwenden, um die neue Umgebung zu validieren.	App-Unterstützung
Bereinigen Sie die Ressourcen.	Nachdem Sie überprüft haben, ob der Cluster erfolgreich migriert wurde, entfernen Sie den S3-Bucket und die für die Migration verwendete IAM-Rolle.	AWS-Administrator

Zugehörige Ressourcen

Elastische Referenzen

- Elastic Cloud
- Verwaltete Elasticsearch und Kibana in AWS
- Elastic-Enterprise-Suche
- Elastische Integrationen
- Elastische Beobachtbarkeit
- Elastische Sicherheit
- Beats
- Elastic APM
- Migrieren zum Index-Lebenszyklusmanagement
- Elastic-Abonnements
- Elastic kontaktieren

Elastic-Blogbeiträge

- So migrieren Sie von selbstverwaltetem Elasticsearch zu Elastic Cloud in AWS (Blogbeitrag)
- Migrieren zu Elastic Cloud (Blogbeitrag)

Elastic-Dokumentation

- Tutorial: Automatisieren von Backups mit SLM
- ILM: Verwalten des Indexlebenszyklus
- Logstash
- Clusterübergreifende Replikation (CCR)
- Pipelines aufnehmen
- Elasticsearch-API-Anforderungen ausführen
- Snapshot-Aufbewahrung

Elastic Video und Webinar

- Elastic Cloud-Migration
- Elastic Cloud: Warum migrieren Kunden (webinar)

AWS-Referenzen

- Elastic Cloud auf AWS Marketplace
- AWS-Befehlszeilenschnittstelle
- AWS Direct Connect
- AWS Migration Acceleration Program
- Network Load Balancers
- Regionen und Availability Zones
- Amazon Route 53
- Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration
- VPN-Verbindungen
- Well-Architected Framework

Zusätzliche Informationen

Wenn Sie komplexe Workloads migrieren möchten, wenden Sie sich an Elastic Elastic Elastic Services . Wenn Sie grundlegende Fragen zu Konfigurationen und Services haben, wenden Sie sich an das Elastic Support-Team.

Migrieren von Daten in die AWS Cloud mithilfe von Starburst

Erstellt von Antony Prasad Thevaraj (AWS), Shaun Van Staden (Starburst) undsh Veer Boli (AWS)

Umgebung: Produktion	Technologien: Analytik; Data Lakes; Datenbanken	Workload: Alle anderen Workloads
AWS-Services: Amazon EKS		

Übersicht

Starburst trägt dazu bei, Ihre Datenmigration zu Amazon Web Services (AWS) zu beschleunigen, indem es eine Enterprise-Abfrage-Engine bereitstellt, die vorhandene Datenquellen in einem einzigen Zugriffspunkt zusammenfasst. Sie können Analysen für mehrere Datenquellen ausführen, um wertvolle Erkenntnisse zu erhalten, bevor Sie Migrationspläne abschließen. Ohne die business-as-usual Analyse zu unterbrechen, können Sie die Daten mithilfe der Starburst-Engine oder einer dedizierten ETL-Anwendung (Extract, Transform, Load) migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Virtual Private Cloud (VPC)
- Ein Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster
- Eine Auto Scaling-Gruppe von Amazon Elastic Compute Cloud (Amazon EC2)
- Eine Liste der aktuellen System-Workloads, die migriert werden müssen
- Netzwerkkonnektivität von AWS zu Ihrer On-Premises-Umgebung

Architektur

Referenzarchitektur

Das folgende allgemeine Architekturdiagramm zeigt die typische Bereitstellung von Starburst Enterprise in der AWS Cloud:

1. Der Starburst Enterprise-Cluster wird in Ihrem AWS-Konto ausgeführt.
2. Ein Benutzer authentifiziert sich mithilfe des Lightweight Directory Access Protocol (LDAP) oder der Open Authorization (OAuth) und interagiert direkt mit dem Starburst-Cluster.
3. Starburst kann eine Verbindung zu mehreren AWS-Datenquellen herstellen, z. B. AWS Glue, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS) und Amazon Redshift. Starburst bietet Verbundabfragefunktionen für alle Datenquellen in der AWS Cloud, On-Premises oder in anderen Cloud-Umgebungen.
4. Sie starten Starburst Enterprise in einem Amazon-EKS-Cluster mithilfe von Helm-Diagrammen.
5. Starburst Enterprise verwendet Amazon EC2-Auto Scaling-Gruppen und Amazon EC2-Spot-Instances zur Optimierung der Infrastruktur.
6. Starburst Enterprise stellt eine direkte Verbindung zu Ihren vorhandenen On-Premises-Datenquellen her, um Daten in Echtzeit zu lesen. Wenn Sie über eine vorhandene Starburst Enterprise-Bereitstellung in dieser Umgebung verfügen, können Sie Ihren neuen Starburst-Cluster in der AWS Cloud direkt mit diesem vorhandenen Cluster verbinden.

Beachten Sie bitte Folgendes:

- Starburst ist keine Datenvirtualisierungsplattform. Es ist eine SQL-basierte Abfrage-Engine für massiv parallele Verarbeitung (Massively Parallel Processing, MPP), die die Grundlage für eine allgemeine Datengitterstrategie für Analysen bildet.
- Wenn Starburst im Rahmen einer Migration bereitgestellt wird, verfügt es über direkte Konnektivität zur vorhandenen On-Premises-Infrastruktur.
- Starburst bietet mehrere integrierte Unternehmens- und Open-Source-Konnektoren, die die Konnektivität zu einer Vielzahl von Legacy-Systemen erleichtern. Eine vollständige Liste der Connectors und ihrer Funktionen finden Sie unter Connectors im Starburst Enterprise-Benutzerhandbuch.
- Starburst kann Daten in Echtzeit aus On-Premises-Datenquellen abfragen. Dadurch werden Unterbrechungen des regulären Geschäftsbetriebs während der Migration von Daten verhindert.
- Wenn Sie von einer vorhandenen On-Premises-Starburst-Enterprise-Bereitstellung migrieren, können Sie einen speziellen Konnektor, Starburst Stargate, verwenden, um Ihren Starburst-Enterprise-Cluster in AWS direkt mit Ihrem On-Premises-Cluster zu verbinden. Dies bietet zusätzliche Leistungsvorteile, wenn Geschäftsbenutzer und Datenanalysten Abfragen von der AWS Cloud in Ihre On-Premises-Umgebung verbinden.

Übersicht über den Prozess auf hoher Ebene

Sie können Datenmigrationsprojekte beschleunigen, indem Sie Starburst verwenden, da Starburst vor der Migration Einblicke in alle Ihre Daten ermöglicht. Die folgende Abbildung zeigt den typischen Prozess für die Migration von Daten mithilfe von Starburst.

Rollen

Die folgenden Rollen sind in der Regel erforderlich, um eine Migration mit Starburst abzuschließen:

- Cloud-Administrator – Verantwortlich für die Bereitstellung von Cloud-Ressourcen für die Ausführung der Starburst-Enterprise-Anwendung
- Starburst-Administrator – verantwortlich für die Installation, Konfiguration, Verwaltung und Unterstützung der Starburst-Anwendung
- Dateningenieur – verantwortlich für:
  - Migrieren der Legacy-Daten in die Cloud
  - Erstellen von semantischen Ansichten zur Unterstützung von Analysen
- Lösungs- oder Systemeigentümer – verantwortlich für die Implementierung der Gesamtlösung

Tools

AWS-Services

- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud.
- Amazon EKS – Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service für die Ausführung von Kubernetes in AWS, ohne dass Sie Ihre eigene Kubernetes-Steuerebene einrichten oder warten müssen. Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Anwendungen in Containern.

Andere Tools

- Helm – Helm ist ein Paketmanager für Kubernetes, mit dem Sie Anwendungen auf Ihrem Kubernetes-Cluster installieren und verwalten können.

- Starburst Enterprise – Starburst Enterprise ist eine SQL-basierte Abfrage-Engine für massiv parallele Verarbeitung (Massively Parallel Processing, MPP), die die Grundlage für eine allgemeine Datengitterstrategie für Analysen bildet.
- Starburst Stargate – Starburst Stargate verknüpft Kataloge und Datenquellen in einer Starburst Enterprise-Umgebung, z. B. einen Cluster in einem On-Premises-Rechenzentrum, mit den Katalogen und Datenquellen in einer anderen Starburst Enterprise-Umgebung, z. B. einem Cluster in der AWS Cloud.

Polen

Bewerten der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren und priorisieren Sie Ihre Daten.	Identifizieren Sie die Daten, die Sie verschieben möchten. Große, On-Premises-System können Kerndaten enthalten, die Sie zusammen mit Daten migrieren möchten, die Sie nicht verschieben möchten oder die aus Compliance-Gründen nicht verschobe n werden können. Wenn Sie mit einem Datenbest and beginnen, können Sie priorisieren, auf welche Daten Sie zuerst abzielen sollten. Weitere Informationen finden Sie unter Erste Schritte mit der automatisierten Portfolio erkennung.	Dateningenieur, DBA
Erkunden, inventarisieren und sichern Sie Ihre Daten.	Überprüfen Sie die Qualität, Menge und Relevanz der Daten für Ihren Anwendung sfall. Sichern oder erstellen	Dateningenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie nach Bedarf einen Snapshot der Daten und schließen Sie die Zielumgeb ung für die Daten ab.	

Einrichten der Starburst Enterprise-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Starburst Enterprise in der AWS Cloud.	Richten Sie Starburst Enterprise in einem verwaltet en Amazon-EKS-Cluster ein, während Daten katalogisiert werden. Weitere Informationen finden Sie unter Bereitste llen mit Kubernetes in der Starburst-Enterprise-Refere nzdokumentation. Dies ermöglicht business-as-usual Analysen, während die Datenmigration läuft.	AWS-Administrator, App-Entwi ckler
Verbinden Sie Starburst mit den Datenquellen.	Nachdem Sie die Daten identifiziert und Starburst Enterprise eingerichtet haben, verbinden Sie Starburst mit den Datenquellen. Starburst liest Daten direkt aus der Datenquelle als SQL-Abfrage. Weitere Informationen finden Sie in der Starburst Enterpris e-Referenzdokumentation.	AWS-Administrator, App-Entwi ckler

Migrieren der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und führen Sie die ETL-Pipelines aus.	Starten Sie den Datenmigr ationsprozess. Diese Aktivität kann gleichzeitig mit Analysen erfolgen business-as-usual . Für die Migration können Sie ein Drittanbieterprodukt oder Starburst verwenden . Starburst ist in der Lage, sowohl Lese- als auch Schreibdaten über verschied ene Quellen hinweg zu lesen. Weitere Informationen finden Sie in der Starburst Enterpris e-Referenzdokumentation.	Dateningenieur
Validieren Sie die Daten.	Nachdem die Daten migriert wurden, validieren Sie die Daten, um sicherzustellen, dass alle erforderlichen Daten verschoben wurden und intakt sind.	Dateningenieur, DevOps Techniker

Cutover und Rollout

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überschneiden Sie die Daten.	Nachdem die Datenmigration und -validierung abgeschlo ssen sind, können Sie die Daten abschneiden. Dazu müssen Sie die Datenverb indungslinks in Starburst	Dateningenieur, Cutover-V erantwortlicher

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ändern. Anstatt auf die On-Premises-Quellen zu verweisen, zeigen Sie auf die neuen Cloud-Quellen und aktualisieren die semantisc hen Ansichten. Weitere Informationen finden Sie unter Connectors in der Starburst Enterprise-Referenzdokument ation.	
Führen Sie ein Rollout für Benutzer durch.	Datenkonsumenten beginnen mit der Arbeit an den migrierte n Datenquellen. Dieser Prozess ist für die Analyse-E ndbenutzer unsichtbar.	Cutover-Verantwortlicher, Dateningenieur

Zugehörige Ressourcen

AWS Marketplace

- Starburst-Galaxy
- Starburst Enterprise
- Starburst-Daten JumpStart
- Starburst Enterprise mit Graviton

Starburst-Dokumentation

- Starburst-Enterprise-Benutzerhandbuch
- Referenzdokumentation zu Starburst Enterprise

Andere AWS-Dokumentation

- Erste Schritte mit der automatisierten Portfolioerkennung (AWS Prescriptive Guidance)

- Optimierung von Kosten und Leistung der Cloud-Infrastruktur mit Starburst in AWS (Blogbeitrag)

Optimieren Sie die ETL-Erfassung der Eingabedateigröße auf AWS

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik; Datenseen	Arbeitslast: Open Source
AWS-Dienste: AWS Glue; Amazon S3		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie den Aufnahmeschritt des ETL-Prozesses (Extrahieren, Transformieren und Laden) für Big Data- und Apache Spark-Workloads auf AWS Glue optimieren können, indem Sie die Dateigröße vor der Verarbeitung Ihrer Daten optimieren. Verwenden Sie dieses Muster, um das Problem mit kleinen Dateien zu verhindern oder zu lösen. Dies ist der Fall, wenn eine große Anzahl kleiner Dateien die Datenverarbeitung aufgrund der Gesamtgröße der Dateien verlangsamt. Beispielsweise können Hunderte von Dateien, die jeweils nur einige hundert Kilobyte groß sind, die Datenverarbeitungsgeschwindigkeit für Ihre AWS Glue Glue-Jobs erheblich verlangsamen. Dies liegt daran, dass AWS Glue interne Listenfunktionen auf Amazon Simple Storage Service (Amazon S3) ausführen muss und YARN (Yet Another Resource Negotiator) eine große Menge an Metadaten speichern muss. Um die Datenverarbeitungsgeschwindigkeit zu verbessern, können Sie mithilfe von Gruppierung Ihre ETL-Aufgaben in die Lage versetzen, eine Gruppe von Eingabedateien in eine einzige In-Memory-Partition zu lesen. Die Partition gruppiert automatisch kleinere Dateien zusammen. Alternativ können Sie benutzerdefinierten Code verwenden, um Ihren vorhandenen Dateien Batch-Logik hinzuzufügen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein oder mehrere AWS-Klebejobs
- Eine oder mehrere Big-Data- oder Apache Spark-Workloads
- Einen S3-Bucket

Architektur

Das folgende Muster zeigt, wie Daten in verschiedenen Formaten von einem AWS Glue Glue-Job verarbeitet und dann in einem S3-Bucket gespeichert werden, um einen Überblick über die Leistung zu erhalten.

Das Diagramm zeigt den folgenden Workflow:

1. Ein AWS Glue Glue-Job konvertiert kleine Dateien im CSV-, JSON- und Parquet-Format in dynamische Frames. Hinweis: Die Größe der Eingabedatei hat den größten Einfluss auf die Leistung des AWS Glue Glue-Jobs.
2. Der AWS Glue Glue-Job führt interne Listenfunktionen in einem S3-Bucket aus.

Tools

- AWS Glue ist ein vollständig verwalteter ETL-Service. Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Epen

Verwenden Sie Gruppierung, um die ETL-Aufnahme beim Lesen zu optimieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Gruppengröße an.	Wenn Sie mehr als 50.000 Dateien haben, erfolgt die Gruppierung standardm äßig. Sie können die Gruppierung jedoch auch für weniger als 50.000 Dateien verwenden, indem Sie die Gruppengröße im `connectio`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`n0ptions` Parameter angeben. Der `connectio n0ptions` Parameter ist in der `create_dynamic_fra me.from_options` Methode enthalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie den Gruppierungscode.	Verwenden Sie die `create_dynamic_frame` Methode, um einen dynamischen Frame zu erstellen. Beispielsweise: `S3bucket_node1 = glueContext.create_dynamic_frame.from_options(format_options={"multiline": False}, connection_type="s3", format="json", connection_options={ "paths": ["s3://bucket/prefix/file.json"], "recurse": True, "groupFiles": 'inPartition', "groupSize": 1048576 }, transformation_ctx="S3bucket_node1",)`  Hinweis: Wird verwendet `groupFiles` , um Dateien in einer Amazon S3 S3-Partitionsgruppe zu gruppieren. Wird verwendet`groupSize` , um die Zielgröße der Gruppe festzulegen, die im Speicher	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gelesen werden soll. Geben Sie `groupSize` in Byte an (1048576 = 1 MB).	
Fügen Sie den Code zum Workflow hinzu.	Fügen Sie den Gruppierungscode zu Ihrem Job-Workflow in AWS Glue hinzu.	Dateningenieur

Verwenden Sie benutzerdefinierte Logik, um die ETL-Erfassung zu optimieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Sprache und die Verarbeitungsplattform.	Wählen Sie die Skriptsprache und die Verarbeitungsplattform, die auf Ihren Anwendungsfall zugeschnitten sind.	Cloud-Architekt
Schreiben Sie den Code.	Schreiben Sie die benutzerdefinierte Logik, um Ihre Dateien zu stapeln.	Cloud-Architekt
Fügen Sie den Code zum Workflow hinzu.	Fügen Sie den Code zu Ihrem Job-Workflow in AWS Glue hinzu. Dadurch kann Ihre benutzerdefinierte Logik bei jeder Ausführung des Jobs angewendet werden.	Dateningenieur

Neupartitionierung beim Schreiben von Daten nach der Transformation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Konsummuster.	Finden Sie heraus, wie nachgelagerte Anwendungen die von Ihnen geschriebenen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Daten verwenden werden. Wenn sie beispielsweise täglich Daten abfragen und Sie nur Daten pro Region partitionieren oder sehr kleine Ausgabedateien haben, z. B. 2,5 KB pro Datei, ist dies nicht optimal für die Nutzung.	
Daten vor dem Schreiben neu partitionieren.	Neupartitionierung auf der Grundlage von Verknüpfungen oder Abfragen während der Verarbeitung (basierend auf der Verarbeitungslogik) und nach der Verarbeitung (basierend auf dem Verbrauch). Zum Beispiel eine Neupartitionierung auf der Grundlage der Bytegröße, wie `.repartition(100000)` , oder eine Neupartitionierung auf der Grundlage von Spalten, wie. `.repartition("column_name")`	Dateningenieur

Zugehörige Ressourcen

- Eingabedateien in größeren Gruppen lesen
- Überwachung von AWS Glue
- Überwachung von AWS Glue mithilfe von CloudWatch Amazon-Metriken
- Auftragsüberwachung und Debugging
- Erste Schritte mit serverlosem ETL auf AWS Glue

Zusätzliche Informationen

Ermitteln der Dateigröße

Es gibt keine einfache Methode, um festzustellen, ob eine Datei zu groß oder zu klein ist. Die Auswirkung der Dateigröße auf die Verarbeitungsleistung hängt von der Konfiguration Ihres Clusters ab. In Core Hadoop empfehlen wir, Dateien mit einer Größe von 128 MB oder 256 MB zu verwenden, um die Blockgröße optimal zu nutzen.

Für die meisten Textdatei-Workloads auf AWS Glue empfehlen wir eine Dateigröße zwischen 100 MB und 1 GB für einen 5-10 DPU-Cluster. Um die beste Größe der Eingabedateien zu ermitteln, überwachen Sie den Vorverarbeitungsbereich Ihres AWS Glue Glue-Auftrags und überprüfen Sie dann die CPU-Auslastung und die Speicherauslastung des Auftrags.

Zusätzliche Überlegungen

Wenn die Leistung in den frühen ETL-Phasen einen Engpass darstellt, sollten Sie die Datendateien vor der Verarbeitung gruppieren oder zusammenführen. Wenn Sie die vollständige Kontrolle über den Dateigenerierungsprozess haben, kann es noch effizienter sein, Datenpunkte auf dem Quellsystem selbst zu aggregieren, bevor die Rohdaten an AWS gesendet werden.

Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions

Erstellt von Sandip Gangapadhyay (AWS)

aws-step-functions-etlQuell code-Repository: -pipeline-pattern	Umgebung: Produktion	Technologien: Analytik; Große Datenmengen; Datenseen DevOps; Serverlos
AWS-Services: Amazon Athena; AWS Glue; AWS Lambda; AWS Step Functions		

Übersicht

Dieses Muster beschreibt, wie Sie eine serverlose ETL-Pipeline (Extrahieren, Transformieren und Laden) erstellen, um einen großen CSV-Datensatz zur Leistungs- und Kostenoptimierung zu validieren, zu transformieren, zu komprimieren und zu partitionieren. Die Pipeline wird von AWS Step Functions orchestriert und umfasst Funktionen zur Fehlerbehandlung, zur automatischen Wiederholung und zur Benutzerbenachrichtigung.

Wenn eine CSV-Datei in einen Bucket-Quellordner von Amazon Simple Storage Service (Amazon S3) hochgeladen wird, beginnt die ETL-Pipeline zu laufen. Die Pipeline validiert den Inhalt und das Schema der CSV-Quelldatei, wandelt die CSV-Datei in ein komprimiertes Apache Parquet-Format um, partitioniert den Datensatz nach Jahr, Monat und Tag und speichert ihn in einem separaten Ordner, damit Analysetools ihn verarbeiten können.

Der Code, der dieses Muster automatisiert GitHub, ist im Repository ETL-Pipeline mit AWS Step Functions verfügbar.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde mit Ihrem AWS-Konto installiert und konfiguriert, sodass Sie AWS-Ressourcen erstellen können, indem Sie einen CloudFormation AWS-Stack bereitstellen. AWS CLI Version 2 wird empfohlen. Installationsanweisungen finden Sie unter Installation, Aktualisierung und Deinstallation von AWS CLI Version 2 in der AWS-CLI-Dokumentation. Anweisungen zur AWS-CLI-Konfiguration finden Sie unter Einstellungen für Konfiguration und Anmeldeinformationsdatei in der AWS-CLI-Dokumentation.
- Ein Amazon-S3-Bucket
- Ein CSV-Datensatz mit dem richtigen Schema. (Das in diesem Muster enthaltene Code-Repository enthält eine CSV-Beispieldatei mit dem richtigen Schema und Datentyp, die Sie verwenden können.)
- Ein Webbrowser, der für die Verwendung mit der AWS-Managementkonsole unterstützt wird. (Sehen Sie sich die Liste der unterstützten Browser an.)
- Zugriff auf die AWS Glue Glue-Konsole.
- Zugriff auf die AWS Step Functions Functions-Konsole.

Einschränkungen

- In AWS Step Functions beträgt die Höchstgrenze für die Aufbewahrung von Verlaufsprotokollen 90 Tage. Weitere Informationen finden Sie unter Kontingente und Kontingente für Standard-Workflows in der AWS Step Functions Functions-Dokumentation.

Produktversionen

- Python 3.11 für AWS Lambda
- AWS Glue, Version 2.0

Architektur

Der in der Abbildung dargestellte Arbeitsablauf besteht aus diesen grundlegenden Schritten:

1. Der Benutzer lädt eine CSV-Datei in den Quellordner in Amazon S3 hoch.
2. Ein Amazon S3 S3-Benachrichtigungsereignis initiiert eine AWS Lambda Lambda-Funktion, die die Step Functions Functions-Zustandsmaschine startet.

3. Die Lambda-Funktion validiert das Schema und den Datentyp der CSV-Rohdatei.
4. Abhängig von den Validierungsergebnissen:
    a. Wenn die Überprüfung der Quelldatei erfolgreich ist, wird die Datei zur weiteren Verarbeitung in den Stage-Ordner verschoben.
    b. Schlägt die Überprüfung fehl, wird die Datei in den Fehlerordner verschoben und eine Fehlerbenachrichtigung wird über Amazon Simple Notification Service (Amazon SNS) gesendet.
5. Ein AWS Glue Glue-Crawler erstellt das Schema der Rohdatei aus dem Stage-Ordner in Amazon S3.
6. Ein AWS Glue Glue-Job transformiert, komprimiert und partitioniert die Rohdatei in das Parquet-Format.
7. Der AWS Glue Glue-Job verschiebt die Datei auch in den Transformationsordner in Amazon S3.
8. Der AWS Glue Glue-Crawler erstellt das Schema aus der transformierten Datei. Das resultierende Schema kann von jedem Analysejob verwendet werden. Sie können Amazon Athena auch verwenden, um Ad-hoc-Abfragen auszuführen.
9. Wenn die Pipeline ohne Fehler abgeschlossen wird, wird die Schemadatei in den Archivordner verschoben. Wenn Fehler auftreten, wird die Datei stattdessen in den Fehlerordner verschoben.
10. Amazon SNS sendet eine Benachrichtigung, die auf Erfolg oder Misserfolg basierend auf dem Status der Pipeline-Fertigstellung hinweist.

Alle in diesem Muster verwendeten AWS-Ressourcen sind serverlos. Es müssen keine Server verwaltet werden.

Tools

AWS-Services

- AWS Glue — AWS Glue ist ein vollständig verwalteter ETL-Service, der es Kunden leicht macht, ihre Daten für Analysen vorzubereiten und zu laden.
- AWS Step Functions — AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. In der grafischen Konsole von AWS Step Functions sehen Sie den Workflow Ihrer Anwendung als eine Reihe von ereignisgesteuerten Schritten.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein hochverfügbarer, langlebiger, sicherer und vollständig verwalteter Pub/Sub-Messaging-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln können.
- AWS Lambda — AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.

Code

Der Code für dieses Muster ist im Repository ETL-Pipeline mit AWS Step Functions verfügbar. GitHub Das Code-Repository enthält die folgenden Dateien und Ordner:

- `template.yml`— CloudFormation AWS-Vorlage für die Erstellung der ETL-Pipeline mit AWS Step Functions.
- `parameter.json`— Enthält alle Parameter und Parameterwerte. Sie aktualisieren diese Datei, um Parameterwerte zu ändern, wie im Abschnitt Epics beschrieben.
- `myLayer/python`Ordner — Enthält Python-Pakete, die zur Erstellung der erforderlichen AWS-Lambda-Schicht für dieses Projekt benötigt werden.
- `lambda`Ordner — Enthält die folgenden Lambda-Funktionen:
  - `move_file.py`— Verschiebt den Quelldatensatz in den Archiv-, Transformations- oder Fehlerordner.
  - `check_crawler.py`— Überprüft den Status des AWS Glue Glue-Crawlers so oft, wie von der `RETRYLIMIT` Umgebungsvariablen konfiguriert, bevor er eine Fehlermeldung sendet.
  - `start_crawler.py`— Startet den AWS Glue Glue-Crawler.
  - `start_step_function.py`— Startet AWS Step Functions.
  - `start_codebuild.py`— Startet das CodeBuild AWS-Projekt.
  - `validation.py`— Validiert den Eingabe-Rohdatensatz.
  - `s3object.py`— Erzeugt die erforderliche Verzeichnisstruktur innerhalb des S3-Buckets.
  - `notification.py`— Sendet Erfolgs- oder Fehlerbenachrichtigungen am Ende der Pipeline.

Um den Beispielcode zu verwenden, folgen Sie den Anweisungen im Abschnitt Epics.

Epen

Bereiten Sie die Quelldateien vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispielcode-Repository.	1. Öffnen Sie die ETL-Pipeline mit dem AWS Step Functions Functions-Repository. 2. Wählen Sie auf der Haupt-Repository-Seite über der Dateiliste die Option Code aus und kopieren Sie die unter Clone with HTTPS aufgeführte URL. 3. Ändern Sie Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten. 4. Geben Sie in einem Terminal oder an einer Befehlszeile den folgenden Befehl ein: `git clone <repoURL>` wo `<repoURL>` bezieht sich auf die URL, die Sie in Schritt 2 kopiert haben.	Developer
Aktualisieren Sie die Parameterwerte.	Bearbeiten Sie in Ihrer lokalen Kopie des Repositorys die `parameter.json` Datei und aktualisieren Sie die	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardparameterwerte wie folgt: • `pS3BucketName` – Der Name des S3-Buckets zum Speichern der Datensätze. Die Vorlage erstellt diesen Bucket für Sie. Der Bucket-Name muss global eindeutig sein. • `pSourceFolder` – Der Name des Ordners im S3-Bucket, der zum Hochladen der CSV-Quell datei verwendet wird. • `pStageFolder` – Der Name des Ordners im S3-Bucket, der während des Vorgangs als Staging-B ereich verwendet wird. • `pTransformFolder` – Der Name des Ordners im S3-Bucket, der zum Speichern transformierter und partition ierter Datensätze verwendet wird. • `pErrorFolder` – Der Ordner im S3-Bucket, in den die CSV-Quelldatei verschoben wird, wenn sie nicht validiert werden kann. • `pArchiveFolder` – Der Name des Ordners im S3-Bucket, der zum Archivier	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en der CSV-Quelldatei verwendet wird. • `pEmailforNotification` – Eine gültige E-Mail-Adresse für den Empfang von Erfolgs- und Fehlerbenachrichtigungen. • `pPrefix` – Eine Präfixzeichenfolge, die im Namen des AWS Glue Glue-Crawlers verwendet wird. • `pDatasetSchema` – Das Datensatz-Schema, anhand dessen die Quelldatei validiert wird. Das Python-Paket Cerberus wird für die Validierung von Quelldatensätzen verwendet. Weitere Informationen finden Sie auf der Cerberus-Website.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode in den S3-Bucket hoch.	Bevor Sie die CloudFormation Vorlage bereitstellen, die die ETL-Pipeline automatisiert, müssen Sie die Quelldate ien für die CloudFormation Vorlage verpacken und in einen S3-Bucket hochladen . Führen Sie dazu den folgenden AWS-CLI-Befehl mit Ihrem vorkonfigurierten Profil aus: `aws cloudformation package --template-file template.yml --s3-bucket <bucket_name> --output-template-file packaged.template --profile <profile_name>` Wobei: • `<bucket_name>` ist der Name eines vorhanden en S3-Buckets in der AWS-Region, in der Sie den Stack bereitstellen möchten. Dieser Bucket wird verwendet, um das Quellcodepaket für die CloudFormation Vorlage zu speichern. • `<profile_name>` ist ein gültiges AWS-CLI-Profil, das Sie bei der Einrichtung	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von AWS CLI vorkonfiguriert haben.	

Erstellen Sie den -Stack

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Führen Sie den folgenden AWS-CLI-Befehl aus, um die CloudFormation Vorlage bereitzustellen: `aws cloudformation deploy --stack-name <stack_name> --template-file packaged.template --parameter-overrides file://parameter.json --capabilities CAPABILITY_IAM --profile <profile_name>` Wobei: • `<stack_name>` ist ein eindeutiger Bezeichner für den CloudFormation Stack. • `<profile-name>` ist Ihr vorkonfiguriertes AWS-CLI-Profil.	Developer
Überprüfen Sie den Fortschritt.	Überprüfen Sie auf der CloudFormation AWS-Konsole den Fortschritt der Stack-Entwicklung. Wenn der Status	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lautet`CREATE_COMPLETE` , wurde der Stack erfolgreich bereitgestellt.	
Notieren Sie sich den Namen der AWS Glue Glue-Date nbank.	Auf der Registerkarte Ausgaben für den Stack wird der Name der AWS Glue Glue-Datenbank angezeigt. Der Schlüsselname ist`GlueDBOutput` .	Developer

Testen Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die ETL-Pipeline.	1. Navigieren Sie zum Quellordner (oder dem Ordnernamen`source`, den Sie in der `parameter .json` Datei festgelegt haben) im S3-Bucket. 2. Laden Sie eine CSV-Beispieldatei in diesen Ordner hoch. (Das Code-Repository enthält eine Beispieldatei mit dem Namen`Sample_Ba nk_Transaction_Raw _Dataset.csv` , die Sie verwenden können.) Durch das Hochladen der Datei wird die ETL-Pipeline über Step Functions gestartet.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Überprüfen Sie in der Step Functions Functions -Konsole den Status der ETL-Pipeline.	
Suchen Sie nach dem partitionierten Datensatz.	Wenn die ETL-Pipeline abgeschlossen ist, stellen Sie sicher, dass der partitionierte Datensatz im Amazon S3 S3-Transformations ordner (oder dem Ordnernam `entransform` , den Sie in der `parameter.json` Datei festgelegt haben) verfügbar ist.	Developer
Suchen Sie nach der partitionierten AWS Glue Glue-Datenbank.	1. Wählen Sie in der AWS Glue Glue-Konsole die vom Stack erstellte AWS Glue Glue-Datenbank aus (dies ist die Datenbank, die Sie im vorherigen Epic notiert haben). 2. Stellen Sie sicher, dass die partitionierte Tabelle im AWS Glue Glue-Datenkatalog verfügbar ist.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Abfragen aus.	(Optional) Verwenden Sie Amazon Athena, um Ad-hoc-Abfragen in der partition ierten und transformierten Datenbank auszuführen. Anweisungen finden Sie in der AWS-Dokumentation unter Ausführen von SQL-Abfragen mit Amazon Athena.	Datenbank-Analyst

Fehlerbehebung

Problem	Lösung
AWS Identity and Access Management (IAM) -Berechtigungen für den AWS Glue Glue-Job und den Crawler	Wenn Sie den AWS Glue Glue-Job oder den Crawler weiter anpassen, stellen Sie sicher, dass Sie die entsprechenden IAM-Berechtigungen in der vom AWS Glue Glue-Job verwendeten IAM-Rolle gewähren oder AWS Lake Formation Datenberechtigungen gewähren. Weitere Informationen finden Sie in der AWS-Dokumentation.

Zugehörige Ressourcen

AWS-Servicedokumentation

- AWS Step Functions
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SNS

Zusätzliche Informationen

Das folgende Diagramm zeigt den AWS Step Functions Functions-Workflow für eine erfolgreiche ETL-Pipeline im Bereich Step Functions Inspector.

Das folgende Diagramm zeigt den AWS Step Functions Functions-Workflow für eine ETL-Pipeline, die aufgrund eines Eingabevalidierungsfehlers fehlschlägt, im Bereich Step Functions Inspector.

Führen Sie erweiterte Analysen mit Amazon Redshift ML durch

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik; Maschinelles Lernen und KI	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon Redshift; Amazon SageMaker		

Übersicht

In der Amazon Web Services (AWS) -Cloud können Sie Amazon Redshift Machine Learning (Amazon Redshift ML) verwenden, um ML-Analysen für Daten durchzuführen, die entweder in einem Amazon Redshift Redshift-Cluster oder in Amazon Simple Storage Service (Amazon S3) gespeichert sind. Amazon Redshift ML unterstützt überwachtes Lernen, das in der Regel für erweiterte Analysen verwendet wird. Zu den Anwendungsfällen für Amazon Redshift ML gehören Umsatzprognosen, Erkennung von Kreditkartenbetrug und Prognosen zum Customer Lifetime Value (CLV) oder zur Kundenabwanderung.

Amazon Redshift ML macht es Datenbankbenutzern leicht, ML-Modelle mithilfe von Standard-SQL-Befehlen zu erstellen, zu trainieren und bereitzustellen. Amazon Redshift ML verwendet Amazon SageMaker Autopilot, um anhand Ihrer Daten automatisch die besten ML-Modelle für die Klassifizierung oder Regression zu trainieren und zu optimieren, während Sie die Kontrolle und Transparenz behalten.

Alle Interaktionen zwischen Amazon Redshift, Amazon S3 und Amazon SageMaker werden abstrahiert und automatisiert. Nachdem das ML-Modell trainiert und bereitgestellt wurde, ist es als benutzerdefinierte Funktion (UDF) in Amazon Redshift verfügbar und kann in SQL-Abfragen verwendet werden.

Dieses Muster ergänzt die Lernprogramme Erstellen, Trainieren und Bereitstellen von ML-Modellen in Amazon Redshift mithilfe von SQL mit Amazon Redshift ML aus dem AWS-Blog und das SageMaker Tutorial Erstellen, Trainieren und Bereitstellen eines ML-Modells mit Amazon aus dem Getting Started Resource Center.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Bestehende Daten in einer Amazon Redshift Redshift-Tabelle

Fähigkeiten

- Vertrautheit mit den von Amazon Redshift ML verwendeten Begriffen und Konzepten, einschließlich maschinellem Lernen, Training und Prognose. Weitere Informationen dazu finden Sie unter Training ML-Modelle in der Dokumentation zu Amazon Machine Learning (Amazon ML).
- Erfahrung mit der Benutzereinrichtung von Amazon Redshift, der Zugriffsverwaltung und der Standard-SQL-Syntax. Weitere Informationen dazu finden Sie unter Erste Schritte mit Amazon Redshift in der Amazon Redshift Redshift-Dokumentation.
- Wissen und Erfahrung mit Amazon S3 und AWS Identity and Access Management (IAM).
- Erfahrung mit der Ausführung von Befehlen in der AWS-Befehlszeilenschnittstelle (AWS CLI) ist ebenfalls von Vorteil, aber nicht erforderlich.

Einschränkungen

- Der Amazon Redshift Redshift-Cluster und der S3-Bucket müssen sich in derselben AWS-Region befinden.
- Der Ansatz dieses Musters unterstützt nur Modelle des überwachten Lernens wie Regression, binäre Klassifizierung und Mehrklassenklassifizierung.

Architektur

In den folgenden Schritten wird erklärt, wie Amazon Redshift ML beim Erstellen SageMaker , Trainieren und Bereitstellen eines ML-Modells zusammenarbeitet:

1. Amazon Redshift exportiert Trainingsdaten in einen S3-Bucket.
2. SageMaker Autopilot verarbeitet die Trainingsdaten automatisch vor.
3. Nachdem die `CREATE MODEL` Anweisung aufgerufen wurde, verwendet Amazon Redshift ML sie SageMaker für das Training.
4. SageMaker Autopilot sucht nach dem ML-Algorithmus und den optimalen Hyperparametern, die die Bewertungsmetriken optimieren, und empfiehlt diese.

5. Amazon Redshift ML registriert das Ausgabe-ML-Modell als SQL-Funktion im Amazon Redshift Redshift-Cluster.
6. Die Funktion des ML-Modells kann in einer SQL-Anweisung verwendet werden.

Technologie-Stack

- Amazon-Redshift
- SageMaker
- Amazon S3

Tools

- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehousing-Service auf Unternehmensebene im Petabyte-Bereich.
- Amazon Redshift ML — Amazon Redshift Machine Learning (Amazon Redshift ML) ist ein robuster, cloudbasierter Service, der es Analysten und Datenwissenschaftlern aller Qualifikationsstufen leicht macht, ML-Technologie zu nutzen.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.
- Amazon SageMaker — SageMaker ist ein vollständig verwalteter ML-Service.
- Amazon SageMaker Autopilot — SageMaker Autopilot ist ein Funktionsumfang, der wichtige Aufgaben eines automatischen maschinellen Lernprozesses (AutoML) automatisiert.

Code

Sie können ein überwachtes ML-Modell in Amazon Redshift erstellen, indem Sie den folgenden Code verwenden:

```
“CREATE MODEL customer_churn_auto_model
FROM (SELECT state,
             account_length,
             area_code,
             total_charge/account_length AS average_daily_spend,
             cust_serv_calls/account_length AS average_daily_cases,
             churn
      FROM customer_activity
      WHERE  record_date < '2020-01-01'
```

```
    )
TARGET churn
FUNCTION ml_fn_customer_churn_auto
IAM_ROLE 'arn:aws:iam::XXXXXXXXXXXX:role/Redshift-ML'
SETTINGS (
  S3_BUCKET 'your-bucket'
);”)
```

Hinweis: Der `SELECT` Status kann sich auf reguläre Amazon Redshift-Tabellen, externe Amazon Redshift Spectrum-Tabellen oder auf beide beziehen.

Epen

Bereiten Sie einen Trainings- und Testdatensatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie einen Trainings- und Testdatensatz vor.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die SageMaker Amazon-Konsole. Folgen Sie den Anweisungen im Tutorial Ein Modell für maschinelles Lernen erstellen, trainieren und bereitstellen, um eine .csv- oder Apache Parquet-Datei zu erstellen, die eine Labelspalte (betreutes Training) und keinen Header enthält. Hinweis: Wir empfehlen, den Rohdatensatz zu mischen und in einen Trainingssatz für das Training des Modells (70 Prozent) und einen Testsatz für die Leistungsbewertung	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Modells (30 Prozent) aufzuteilen.	

Bereiten Sie den Technologie-Stack vor und konfigurieren Sie ihn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen Amazon Redshift Redshift-Cluster.	Erstellen Sie auf der Amazon Redshift Redshift-Konsole einen Cluster gemäß Ihren Anforderungen. Weitere Informationen dazu finden Sie unter Create a cluster in der Amazon Redshift Redshift-Dokumentation. Wichtig: Amazon Redshift Redshift-Cluster müssen zusammen mit dem `SQL_PREVIEW` Maintenance Track erstellt werden. Weitere Informationen zu Vorschau-Tracks finden Sie unter Cluster-Wartungsspuren auswählen in der Amazon Redshift Redshift-Dokumentation.	DBA, Cloud-Architekt
Erstellen Sie einen S3-Bucket zum Speichern von Trainingsdaten und Modellartefakten.	Erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket für die Trainings- und Testdaten. Weitere Informationen zum Erstellen eines S3-Buckets finden Sie unter	DBA, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellen eines S3-Buckets über AWS Quick Starts. Wichtig: Stellen Sie sicher, dass sich Ihr Amazon Redshift Redshift-Cluster und Ihr S3-Bucket in derselben Region befinden.	
Erstellen Sie eine IAM-Richtlinie und fügen Sie sie dem Amazon Redshift Redshift-Cluster hinzu.	Erstellen Sie eine IAM-Richtlinie, um dem Amazon Redshift Redshift-Cluster den Zugriff auf Amazon S3 SageMaker zu ermöglichen. Anweisungen und Schritte finden Sie unter Cluster-Setup für die Verwendung von Amazon Redshift ML in der Amazon Redshift Redshift-Dokumentation.	DBA, Cloud-Architekt
Erlauben Sie Amazon Redshift Redshift-Benutzern und -Gruppen den Zugriff auf Schemas und Tabellen.	Erteilen Sie Berechtigungen, um Benutzern und Gruppen in Amazon Redshift den Zugriff auf interne und externe Schemas und Tabellen zu ermöglichen. Schritte und Anweisungen finden Sie unter Berechtigungen und Besitz verwalten in der Amazon Redshift Redshift-Dokumentation.	DBA

Erstellen und trainieren Sie das ML-Modell in Amazon Redshift

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und trainieren Sie das ML-Modell in Amazon Redshift.	Erstellen und trainieren Sie Ihr ML-Modell in Amazon Redshift ML. Weitere Informationen finden Sie in der `CREATE MODEL` Erklärung in der Amazon Redshift Redshift-Dokumentation.	Entwickler, Datenwissenschaftler

Batch-Inferenz und -Vorhersage in Amazon Redshift durchführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Inferenz mithilfe der generierten ML-Modellfunktion durch.	Weitere Informationen zur Durchführung von Inferenzen mithilfe der generierten ML-Modellfunktion finden Sie unter Vorhersage in der Amazon Redshift Redshift-Dokumentation.	Datenwissenschaftler, Business Intelligence-Benutzer

Zugehörige Ressourcen

Bereiten Sie einen Trainings- und Testdatensatz vor

- Aufbau, Schulung und Bereitstellung eines Modells für maschinelles Lernen mit Amazon SageMaker

Bereiten Sie den Technologie-Stack vor und konfigurieren Sie ihn

- Einen Amazon Redshift Redshift-Cluster erstellen
- Auswahl von Amazon Redshift Redshift-Cluster-Wartungsplänen

- Erstellen eines S3-Buckets
- Einrichtung eines Amazon Redshift-Clusters für die Verwendung von Amazon Redshift ML
- Verwaltung von Berechtigungen und Eigentum in Amazon Redshift

Erstellen und trainieren Sie das ML-Modell in Amazon Redshift

- CREATE MODEL-Anweisung in Amazon Redshift

Batch-Inferenz und -Vorhersage in Amazon Redshift durchführen

- Prognose in Amazon Redshift

Sonstige Ressourcen

- Erste Schritte mit Amazon Redshift ML
- Erstellen, Trainieren und Bereitstellen von ML-Modellen in Amazon Redshift mithilfe von SQL mit Amazon Redshift ML
- Amazon Redshift Redshift-Partner
- AWS-Kompetenzpartner für maschinelles Lernen

Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden

Erstellt von Moinul Al-Mamun (AWS)

Umgebung: Produktion	Technologien: Analytik; Datenbanken; Serverlos; Große Datenmengen	AWS-Dienste: Amazon Athena; Amazon DynamoDB; AWS Lambda; Amazon S3

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe des Amazon Athena DynamoDB-Connectors eine Verbindung zwischen Amazon Athena und Amazon DynamoDB einrichten. Der Connector verwendet eine AWS-Lambda-Funktion, um die Daten in DynamoDB abzufragen. Sie müssen keinen Code schreiben, um die Verbindung einzurichten. Nachdem die Verbindung hergestellt wurde, können Sie schnell auf DynamoDB-Tabellen zugreifen und diese analysieren, indem Sie Athena Federated Query verwenden, um SQL-Befehle von Athena auszuführen. Sie können auch eine oder mehrere DynamoDB-Tabellen miteinander oder mit anderen Datenquellen wie Amazon Redshift oder Amazon Aurora verbinden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit Berechtigungen zur Verwaltung von DynamoDB-Tabellen, Athena-Datenquellen, Lambda und AWS Identity and Access Management (IAM) -Rollen
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket, in dem Athena Abfrageergebnisse speichern kann
- Ein S3-Bucket, in dem der Athena DynamoDB Connector die Daten kurzfristig speichern kann
- Eine AWS-Region, die Athena Engine Version 2 unterstützt
- IAM-Berechtigungen für den Zugriff auf Athena und die erforderlichen S3-Buckets
- Amazon Athena DynamoDB Connector, installiert

Einschränkungen

Das Abfragen von DynamoDB-Tabellen ist kostenpflichtig. Tabellengrößen, die einige Gigabyte (GB) überschreiten, können hohe Kosten verursachen. Wir empfehlen, dass Sie die Kosten berücksichtigen, bevor Sie einen vollständigen Tabellen-SCAN-Vorgang durchführen. Weitere Informationen finden Sie unter Amazon DynamoDB – Preise. Um die Kosten zu senken und eine hohe Leistung zu erzielen, empfehlen wir, in Ihrer Abfrage immer LIMIT zu verwenden (z. B.`SELECT * FROM table1 LIMIT 10`). Bevor Sie eine JOIN- oder GROUP BY-Abfrage in einer Produktionsumgebung ausführen, sollten Sie außerdem die Größe Ihrer Tabellen berücksichtigen. Wenn Ihre Tabellen zu groß sind, ziehen Sie alternative Optionen in Betracht, z. B. die Migration der Tabelle zu Amazon S3.

Architektur

Das folgende Diagramm zeigt, wie ein Benutzer eine SQL-Abfrage für eine DynamoDB-Tabelle von Athena aus ausführen kann.

Das Diagramm zeigt den folgenden Workflow:

1. Um eine DynamoDB-Tabelle abzufragen, führt ein Benutzer eine SQL-Abfrage von Athena aus.
2. Athena initiiert eine Lambda-Funktion.
3. Die Lambda-Funktion fragt die angeforderten Daten in der DynamoDB-Tabelle ab.
4. DynamoDB gibt die angeforderten Daten an die Lambda-Funktion zurück. Anschließend überträgt die Funktion die Abfrageergebnisse über Athena an den Benutzer.
5. Die Lambda-Funktion speichert Daten im S3-Bucket.

Technologie-Stack

- Amazon Athena
- Amazon-DynamoDB
- Amazon S3
- AWS Lambda

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.

- Amazon Athena DynamoDB Connector ist ein AWS-Tool, mit dem Athena mithilfe von SQL-Abfragen eine Verbindung mit DynamoDB herstellen und auf Ihre Tabellen zugreifen kann.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Epen

DynamoDB-Beispieltabellen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erste Beispieltabelle.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die DynamoDB-Konsole. 2. Wählen Sie Create table (Tabelle erstellen) aus. 3. Geben Sie als Tabellenname dydbtable1 ein. 4. Geben Sie als Partitionsschlüssel PK1 ein. 5. Geben Sie als Sortierschlüssel SK1 ein. 6. Wählen Sie im Bereich Tabelleneinstellungen die Option Einstellungen anpassen aus. 7. Wählen Sie im Abschnitt Tabellenklasse die Option DynamoDB Standard aus. 8. Wählen Sie im Abschnitt Lese-/Schreibkapazitätseins	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tellungen für den Kapazität smodus die Option On-Demand aus. 9. Wählen Sie im Abschnitt Verschlüsselung im Ruhezustand die Option Owned by Amazon DynamoDB aus. 10. Wählen Sie Create table (Tabelle erstellen) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Beispieldaten in die erste Tabelle ein.	1. Öffnen Sie die DynamoDB-Konsole.
	2. Wählen Sie im Navigationsbereich Tabelle und dann Ihre Tabelle in der Spalte Name aus.
	3. Wählen Sie Aktionen und dann Element erstellen aus.
	4. Wählen Sie JSON-Ansicht.
	5. Deaktivieren Sie in der Titelleiste des Attributs-Editors die Option DynamoDB-JSON anzeigen.
	6. Geben Sie im Attribut-Editor nacheinander die folgenden Beispieldaten ein:
	
	`{ "PK1": "1234", "SK1": "info", "Salary": "5000" }`
	
	`{ "PK1": "1235", "SK1": "info", "Salary": "5200" }`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die zweite Beispieltabelle.	1. Öffnen Sie die DynamoDB-Konsole. 2. Wählen Sie Create table aus. 3. Geben Sie als Tabellenname dydbtable2 ein. 4. Geben Sie als Partitionsschlüssel PK2 ein. 5. Geben Sie als Sortierschlüssel SK2 ein. 6. Wählen Sie im Bereich Tabelleneinstellungen die Option Einstellungen anpassen aus. 7. Wählen Sie im Abschnitt Tabellenklasse die Option DynamoDB Standard aus. 8. Wählen Sie im Abschnitt Lese-/Schreibkapazitätseinstellungen für den Kapazitätsmodus die Option On-Demand aus. 9. Wählen Sie im Abschnitt Verschlüsselung im Ruhezustand die Option Owned by Amazon DynamoDB aus. 10. Wählen Sie Create table (Tabelle erstellen) aus.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Beispieldaten in die zweite Tabelle ein.	1. Öffnen Sie die DynamoDB-Konsole.
	2. Wählen Sie im Navigationsbereich Tabelle und dann Ihre Tabelle in der Spalte Name aus.
	3. Wählen Sie Aktionen und dann Element erstellen aus.
	4. Deaktivieren Sie in der Titelleiste des Attributs-Editors die Option DynamoDB-JSON anzeigen.
	5. Geben Sie im Attribut-Editor nacheinander die folgenden Beispieldaten ein:
	`{ "PK2": "1234", "SK2": "bonus", "Bonus": "500" }`
	`{ "PK2": "1235", "SK2": "bonus", "Bonus": "1000" }`
		Developer

Erstellen Sie eine Datenquelle in Athena für DynamoDB

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Datenquellenkonnektor ein.	Erstellen Sie eine Datenquelle für DynamoDB und anschließend eine Lambda-Funktion, um eine Verbindung zu dieser Datenquelle herzustellen. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Athena-Konsole. 2. Wählen Sie im Navigationsbereich Datenquellen und dann Datenquelle erstellen aus. 3. Wählen Sie die Amazon DynamoDB DynamoDB-Datenquelle und dann Weiter. 4. Geben Sie im Abschnitt Datenquellendetails als Datenquellenname TestDynamoDB ein. 5. Wählen Sie im Abschnitt Verbindungsdetails eine Lambda-Funktion aus, die bereits bereitgestellt wurde, oder wählen Sie Lambda-Funktion erstellen, wenn Sie keine Lambda-Funktion für dieses Muster verwenden können. Hinweis: Weitere Informati	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen zum Erstellen einer Lambda-Funktion finden Sie unter Getting started with Lambda im Lambda Developer Guide. 6. (Optional) Wenn Sie die Funktion „Lambda erstellen “ wählen, müssen Sie die CloudFormation AWS-Vorlage konfigurieren, die in der Java-Anwendung enthalten ist, bevor Sie diesen Stack bereitstellen. Die Vorlage umfasst ApplicationName, SpillBucket AthenaCatalogName, und andere Anwendungseinstellungen. Hinweis: Nachdem Sie diese Java-basierte Anwendung bereitgestellt haben, erstellt der Stack eine Lambda-Funktion, die es Athena ermöglicht, mit DynamoDB zu kommunizieren. Dadurch können Sie über SQL-Befehle auf Ihre Tabellen zugreifen. 7. Stellen Sie Ihre Lambda-Funktion bereit. 8. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lambda-Funktion auf den S3-Spill-Bucket zugreifen kann.	1. Öffnen Sie die Lambda-Konsole. 2. Wählen Sie im Navigationsbereich Funktionen und dann die Funktion aus, die Sie zuvor erstellt haben. 3. Wählen Sie die Registerkarte Konfiguration aus. 4. Wählen Sie im linken Bereich die Option Umgebungsvariablen aus, und vergewissern Sie sich dann, dass der Wert für den Schlüssel lautet `spill_bucket` . 5. Wählen Sie im linken Bereich Berechtigungen und dann im Abschnitt Ausführungsrolle die angehängte IAM-Rolle aus. Hinweis: Sie werden zu der IAM-Rolle weitergeleitet, die Ihrer Lambda-Funktion in der IAM-Konsole zugeordnet ist. 6. Vergewissern Sie sich, dass Sie Schreibberechtigungen für den Bucket haben. `spill_bucket` Wenn Sie auf Fehler stoßen, finden Sie im Abschnitt	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zusätzliche Informationen in diesem Muster eine Anleitung.	

Greifen Sie von Athena aus auf DynamoDB-Tabellen zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fragen Sie die DynamoDB-Tabellen ab.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Athena-Konsole. 2. Wählen Sie im Navigationsbereich Datenquellen und dann Datenquelle erstellen aus. 3. Wählen Sie im Navigationsbereich die Option Query Editor (Abfrage-Editor) aus. 4. Wählen Sie auf der Registerkarte Editor im Bereich Daten für Datenquelle Ihre Datenquelle aus. 5. Als Datenbank wählen Sie Ihre Datenbank aus. 6. Geben Sie für Abfrage 1 die folgende Abfrage ein: `SELECT * FROM dydbtable1 t1;` 7. Wählen Sie Ausführen aus, und überprüfen Sie dann die Ausgabe in der Tabelle.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Geben Sie für Abfrage 2 die folgende Abfrage ein: `SELECT * FROM dydbtable2 t2;` 9. Wählen Sie Ausführen aus, und überprüfen Sie dann die Ausgabe in der Tabelle.	
Verbinden Sie die beiden DynamoDB-Tabellen.	DynamoDB ist ein NoSQL-Datenspeicher und unterstützt den SQL-Join-Vorgang nicht. Folglich müssen Sie einen Join-Vorgang für zwei DynamoDB-Tabellen ausführen: 1. Wählen Sie das Plussymbol, um eine weitere Abfrage zu erstellen. 2. Geben Sie für Abfrage 3 die folgende Abfrage ein: `SELECT pk1, salary, bonus FROM dydbtable1 t1 JOIN dydbtable2 t2 ON t1.pk1 = t2.pk2;`	Developer

Zugehörige Ressourcen

- Amazon Athena DynamoDB-Konnektor (AWS Labs)
- Abfragen beliebiger Datenquellen mit der neuen Verbundabfrage von Amazon Athena (AWS Big Data Blog)

- Versionsreferenz der Athena-Engine (Athena-Benutzerhandbuch)
- Vereinfachen Sie die Datenextraktion und -analyse mit Amazon DynamoDB mithilfe von AWS Glue und Amazon Athena (AWS-Datenbank-Blog)

Zusätzliche Informationen

Wenn Sie in Athena eine Abfrage mit `spill_bucket` im `{bucket_name}/folder_name/` Format ausführen, erhalten Sie möglicherweise die folgende Fehlermeldung:

```
"GENERIC_USER_ERROR: Encountered an exception[java.lang.RuntimeException] from your
 LambdaFunction[arn:aws:lambda:us-east-1:xxxxxx:function:testdynamodb] executed in
 context[retrieving meta-data] with message[You do NOT own the spill bucket with the
 name: s3://test-bucket-dynamodbconnector/athena_dynamodb_spill_data/]
This query ran against the "default" database, unless qualified by the query. Please
 post the error message on our forum  or contact customer support with Query Id:
 [query-id]"
```

Um diesen Fehler zu beheben, aktualisieren Sie die Umgebungsvariable der Lambda-Funktion `spill_bucket` auf `{bucket_name_only}` und aktualisieren Sie dann die folgende Lambda-IAM-Richtlinie für den Bucket-Schreibzugriff:

```
{
             "Action": [
                 "s3:GetObject",
                 "s3:ListBucket",
                 "s3:GetBucketLocation",
                 "s3:GetObjectVersion",
                 "s3:PutObject",
                 "s3:PutObjectAcl",
                 "s3:GetLifecycleConfiguration",
                 "s3:PutLifecycleConfiguration",
                 "s3:DeleteObject"
             ],
             "Resource": [
                 "arn:aws:s3:::spill_bucket",
                 "arn:aws:s3:::spill_bucket/*"
             ],
             "Effect": "Allow"
         }
```

Alternativ können Sie den Athena-Datenquellenconnector, den Sie zuvor erstellt haben, entfernen und ihn neu erstellen, indem Sie nur `{bucket_name}` für verwenden. `spill_bucket`

Richten Sie einen nutzbaren Mindestdatenraum ein, um Daten zwischen Organisationen gemeinsam zu nutzen

Erstellt von Ramy Hcini (Think-IT), Ismail Abdellaoui (Think-IT), Malte Gasseling (Think-IT), Jorge Hernandez Suarez (AWS) und Michael Miller (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik; Container und Mikroservices; Data Lakes; Datenbanken; Infrastruktur	Arbeitslast: Open Source
AWS-Services: Amazon Aurora; AWS Certificate Manager (ACM); AWS CloudFormation; Amazon EC2; Amazon EFS; Amazon EKS; Elastic Load Balancing (ELB); Amazon RDS; Amazon S3; AWS Systems Manager		

Übersicht

Datenräume sind föderierte Netzwerke für den Datenaustausch mit Vertrauen und Kontrolle über die eigenen Daten als Kernprinzipien. Sie ermöglichen es Unternehmen, Daten in großem Umfang zu teilen, auszutauschen und zusammenzuarbeiten, indem sie eine kostengünstige und technologieunabhängige Lösung bieten.

Datenräume haben das Potenzial, die Bemühungen für eine nachhaltige future erheblich voranzutreiben, indem datengesteuerte Problemlösungen mit einem end-to-end Ansatz eingesetzt werden, der alle relevanten Interessengruppen einbezieht.

Dieses Muster führt Sie durch das Beispiel, wie zwei Unternehmen die Datenraum-Technologie auf Amazon Web Services (AWS) nutzen können, um ihre Strategie zur Reduzierung der CO2-Emissionen voranzutreiben. In diesem Szenario liefert Unternehmen X Daten zu den CO2-Emissionen, die Unternehmen Y verbraucht. Im Abschnitt Zusätzliche Informationen finden Sie die folgenden Einzelheiten zur Datenraumspezifikation:

- Teilnehmer
- Geschäftsszenario
- Behörde für den Datenraum
- Komponenten des Datenraums
- Dienste für den Datenraum
- Daten, die ausgetauscht werden sollen
- Datenmodell
- Tractus-X EDC-Anschluss

Das Muster umfasst Schritte für Folgendes:

- Bereitstellung der Infrastruktur, die für einen Basisdatenraum erforderlich ist, auf dem zwei Teilnehmer laufen AWS.
- Sicherer Austausch von Daten zur Kohlenstoffemissionsintensität mithilfe der Konnektoren.

Dieses Muster stellt einen Kubernetes-Cluster bereit, der Datenraum-Konnektoren und deren Dienste über Amazon Elastic Kubernetes Service (Amazon EKS) hostet.

Die Steuerungsebene und die Datenebene von Eclipse Dataspace Components (EDC) werden beide auf Amazon EKS bereitgestellt. Das offizielle Tractus-X Helm-Diagramm stellt PostgreSQL- und Vault-Dienste als Abhängigkeiten bereit. HashiCorp

Darüber hinaus wird der Identitätsdienst auf Amazon Elastic Compute Cloud (Amazon EC2) bereitgestellt, um ein reales Szenario mit einem Minimum Viable Data Space (MVDS) zu replizieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Aktiv AWS-Konto zur Bereitstellung der Infrastruktur in der von Ihnen ausgewählten AWS-Region
- Ein AWS Identity and Access Management (IAM-) Benutzer mit Zugriff auf Amazon S3, der vorübergehend als technischer Benutzer verwendet wird (Der EDC-Connector unterstützt derzeit nicht die Verwendung von Rollen. Wir empfehlen, dass Sie einen IAM-Benutzer speziell für diese Demo erstellen und diesem Benutzer eingeschränkte Berechtigungen zuweisen.)

- AWS Command Line Interface (AWS CLI) in der von Ihnen ausgewählten Version installiert und konfiguriert AWS-Region
- AWS Sicherheitsanmeldedaten
- eksctl auf Ihrer Workstation
- Git auf deiner Workstation
- kubectl
- Helm
- Postbote
- Ein AWS Certificate Manager (ACM) SSL/TLS-Zertifikat
- Ein DNS-Name, der auf einen Application Load Balancer verweist (der DNS-Name muss durch das ACM-Zertifikat abgedeckt sein)
- HashiCorp Tresor (Informationen AWS Secrets Manager zur Verwaltung von Geheimnissen finden Sie im Abschnitt Zusätzliche Informationen.)

Produktversionen

- AWS CLI Version 2+
- Postman-Sammlung v2.1

Einschränkungen

- Auswahl des Konnektors – Bei dieser Bereitstellung wird ein EDC-basierter Konnektor verwendet. Achten Sie jedoch darauf, die Stärken und Funktionen der EDC - und FIWARE True-Konnektoren zu berücksichtigen, um eine fundierte Entscheidung zu treffen, die den spezifischen Anforderungen der Implementierung entspricht.
- Aufbau des EDC-Konnektors – Die gewählte Bereitstellungslösung basiert auf der Tractus-X EDC Connector Helm-Übersicht, einer etablierten und ausführlich getesteten Implementierungsoption. Die Entscheidung, dieses Diagramm zu verwenden, basiert auf seiner allgemeinen Verwendung und der Aufnahme wesentlicher Erweiterungen in der bereitgestellten Version. PostgreSQL und HashiCorp Vault sind zwar Standardkomponenten, Sie haben jedoch die Flexibilität, Ihren eigenen Connector-Build bei Bedarf anzupassen.
- Zugriff auf private Cluster – Der Zugriff auf den bereitgestellten EKS-Cluster ist auf private Kanäle beschränkt. Die Interaktion mit dem Cluster erfolgt ausschließlich mithilfe von `kubectl` und IAM. Der öffentliche Zugriff auf die Clusterressourcen kann mithilfe von Load Balancern und

Domainnamen ermöglicht werden. Diese müssen selektiv implementiert werden, um bestimmte Dienste einem breiteren Netzwerk zugänglich zu machen. Wir empfehlen jedoch nicht, öffentlichen Zugriff zu gewähren.

- Sicherheitsfokus – Der Schwerpunkt liegt auf der Abstraktion von Sicherheitskonfigurationen anhand von Standardspezifikationen, sodass Sie sich auf die Schritte konzentrieren können, die beim Datenaustausch mit dem EDC-Konnektor erforderlich sind. Obwohl die Standardsicherheitseinstellungen beibehalten werden, müssen Sie unbedingt die sichere Kommunikation aktivieren, bevor Sie den Cluster dem öffentlichen Netzwerk zugänglich machen. Diese Vorsichtsmaßnahme gewährleistet eine solide Grundlage für eine sichere Datenverarbeitung.
- Infrastrukturkosten – Eine Schätzung der Infrastrukturkosten finden Sie unter. AWS Pricing Calculator Eine einfache Berechnung zeigt, dass die Kosten für die bereitgestellte Infrastruktur bis zu 162,92 USD pro Monat betragen können.

Architektur

Die MVDS-Architektur umfasst zwei virtuelle private Clouds (VPCs), eine für den Identitätsdienst Dynamic Attribute Provisioning System (DAPS) und eine für Amazon EKS.

DAPS-Architektur

Das folgende Diagramm zeigt DAPS, die auf EC2-Instances ausgeführt werden, die von einer Auto Scaling Scaling-Gruppe gesteuert werden. Ein Application Load Balancer und eine Routing-Tabelle machen die DAPS-Server verfügbar. Amazon Elastic File System (Amazon EFS) synchronisiert die Daten zwischen den DAPS-Instances.

Amazon EKS-Architektur

Datenräume sind als technologieunabhängige Lösungen konzipiert, und es gibt mehrere Implementierungen. Dieses Muster verwendet einen Amazon EKS-Cluster, um die technischen Komponenten des Datenraums bereitzustellen. Das folgende Diagramm zeigt die Bereitstellung des EKS-Clusters. Worker-Knoten werden in privaten Subnetzen installiert. Die Kubernetes-Pods greifen auf die Amazon Relational Database Service (Amazon RDS) for PostgreSQL-Instance zu, die sich ebenfalls in den privaten Subnetzen befindet. Die Kubernetes-Pods speichern gemeinsam genutzte Daten in Amazon S3.

Tools

AWS Dienste

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet sichere und skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) hilft Ihnen bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS Cloud.
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf EC2-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Andere Tools

- eksctl ist ein Befehlszeilenprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.
- Git ist ein verteiltes Open-Source-Versionskontrollsystem.
- HashiCorp Vault bietet sicheren Speicher mit kontrolliertem Zugriff auf Anmeldeinformationen und andere vertrauliche Informationen.
- Helm ist ein Open-Source-Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.
- Postman ist eine API-Plattform.

Code-Repository

Die Kubernetes-Konfigurations-YAML-Dateien und Python-Skripte für dieses Muster sind im aws-patterns-edc-Repository verfügbar. GitHub Das Muster verwendet auch das Tractus-X EDC-Repository.

Bewährte Methoden

Amazon EKS und Isolierung der Infrastrukturen der Teilnehmer

Namespaces in Kubernetes trennen nach diesem Muster die Infrastruktur des Anbieters von Unternehmen X von der Infrastruktur des Verbrauchers von Unternehmen Y ab. Weitere Informationen finden Sie in den EKS Best Practices Guides.

In einer realistischeren Situation hätte jeder Teilnehmer einen separaten Kubernetes-Cluster, der in seinem eigenen Cluster läuft. AWS-Konto Die gemeinsame Infrastruktur (DAPS in diesem Muster) wäre für die Teilnehmer des Datenraums zugänglich und gleichzeitig vollständig von den Infrastrukturen der Teilnehmer getrennt.

Epen

Richten Sie die Umgebung ein und stellen Sie einen EKS-Cluster und EC2-Instances bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository auf Ihre Workstation zu klonen: `git clone https://github.com/Think-iT-Labs/aws-patterns-edc` Die Workstation muss Zugriff auf Ihre haben AWS-Konto.	DevOps Ingenieur
Stellen Sie den Kubernetes-Cluster bereit und richten Sie Namespaces ein.	Um einen vereinfachten Standard-EKS-Cluster in Ihrem Konto bereitzustellen, führen Sie den folgenden	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`eksctl` Befehl auf der Workstation aus, auf der Sie das Repo geklont haben:
	
	`eksctl create cluster`
	
	Der Befehl erstellt die VPC sowie private und öffentlic he Subnetze, die sich über drei verschiedene Availability Zones erstrecken. Nachdem die Netzwerkschicht erstellt wurde, erstellt der Befehl zwei `m5.large` EC2-Instances innerhalb einer Auto Scaling Scaling-Gruppe.
	
	Weitere Informationen und Beispielausgaben finden Sie im eksctl-Handbuch.
	
	Nachdem Sie den privaten Cluster bereitgestellt haben, fügen Sie den neuen EKS-Cluster zu Ihrer lokalen Kubernetes-Konfiguration hinzu, indem Sie den folgenden Befehl ausführen:
	
	`aws eks update-ku beconfig --name <EKS CLUSTER NAME> --region <AWS REGION>`
	
	Dieses Muster verwendet den `eu-west-1` AWS-Region ,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um alle Befehle auszuführen. Sie können jedoch dieselben Befehle in Ihrer bevorzugten Version ausführen AWS-Regio n. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Ihre EKS-Knoten ausgeführ t werden und sich im Bereitsch aftszustand befinden: `kubectl get nodes`	

Richten Sie die Namespaces ein.	Führen Sie die folgenden Befehle aus, um Namespace s für den Anbieter und den Verbraucher zu erstellen:
	
	`kubectl create ns provider`
	`kubectl create ns consumer`
	
	In diesem Muster ist es wichtig, `provider` und `consumer` als Namespace s zu verwenden, damit sie den Konfigurationen in den nächsten Schritten entsprech en.
		DevOps Ingenieur

Stellen Sie den Identitätsdienst bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie DAPS bereit, indem Sie AWS CloudFormation	Um die Verwaltung von DAPS-Vorgängen zu vereinfachen, ist der DAPS-Server auf EC2-Instances installiert. Verwenden Sie die Vorlage, um DAPS zu installieren.AWS CloudFormation Sie benötigen das ACM-Zertifikat und den DNS-Namen aus dem Abschnitt Voraussetzungen. Die Vorlage stellt Folgendes bereit und konfiguriert es: • Application Load Balancer • Auto Scaling-Gruppe • EC2-Instances, die mit Benutzerdaten konfiguriert sind, um alle erforderlichen Pakete zu installieren • IAM-Rollen • DAPS Sie können die AWS CloudFormation Vorlage bereitstellen, indem Sie sich bei der AWS CloudFormation Konsole anmelden AWS Management Console und diese verwenden. Sie können die Vorlage auch mithilfe eines	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS CLI Befehls wie dem folgenden bereitstellen: `aws cloudformation create-stack --stack-name daps \ --template-body file://aws-patterns-edc/cloudformation.yml --parameters \ ParameterKey=CertificateARN,ParameterValue=<ACM Certificate ARN> \ ParameterKey=DNSName,ParameterValue=<DNS name> \ ParameterKey=InstanceType,ParameterValue=<EC2 instance type> \ ParameterKey=EnvironmentName,ParameterValue=<Environment Name> --capabilities CAPABILITY_NAMED_IAM`  Der Name der Umgebung ist Ihre eigene Wahl. Wir empfehlen, einen aussagekräftigen Begriff zu verwenden `DapsInfrastructure`, z. B. weil er sich in den AWS Ressourcen-Tags wiederfindet.  Für dieses Muster `t3.small` ist es groß genug, um den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DAPS-Workflow auszuführen, der über drei Docker-Container verfügt. Die Vorlage stellt die EC2-Instances in privaten Subnetzen bereit. Das bedeutet, dass auf die Instances nicht direkt über SSH (Secure Shell) aus dem Internet zugegriffen werden kann. Die Instanzen werden mit der erforderlichen IAM-Rolle und dem AWS Systems Manager Agenten ausgestattet, um den Zugriff auf die laufenden Instanzen über den Session Manager zu ermöglichen, eine Funktion von. AWS Systems Manager Wir empfehlen die Verwendung von Session Manager für den Zugriff. Alternativ könnten Sie einen Bastion-Host bereitstellen, der den SSH-Zugriff aus dem Internet ermöglicht. Bei Verwendung des Bastion-Host-Ansatzes kann es noch einige Minuten dauern, bis die EC2-Instance gestartet wird. Nachdem die AWS CloudFormation Vorlage erfolgreich bereitgestellt wurde,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	verweisen Sie den DNS-Namen auf Ihren Applicati on Load Balancer Balancer-DNS-Namen. Führen Sie zur Bestätigung den folgenden Befehl aus:
	`dig <DNS NAME>`
	Die Ausgabe sollte folgender maßen oder ähnlich aussehen:
	`; <<>> DiG 9.16.1-Ub untu <<>> edc-patte rn.think-it.io ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42344 ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ;; QUESTION SECTION: ;edc-pattern.think-it.io. IN A ;; ANSWER SECTION: edc-pattern.think-it.io. 276 IN CNAME daps-alb-iap9zmwy3kn8-13287`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	73120.eu-west-1.el b.amazonaws.com. daps-alb-iap9zmwy3k n8-1328773120.eu-w est-1.elb.amazonaw s.com. 36 IN A 52.208.240.129 daps-alb-iap9zmwy3kn8 -1328773120.eu-wes t-1.elb.amazonaws. com. 36 IN A 52.210.15 5.124	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Registrieren Sie die Konnektoren der Teilnehmer für den DAPS-Dienst.	Registrieren Sie die Teilnehmer von einer der für DAPS bereitgestellten EC2-Instances aus:
	1. Führen Sie das verfügbare Skript auf der EC2-Instance mithilfe des Root-Benutzers aus:
	`cd /srv/mvds/omejdn-daps`
	2. Registrieren Sie den Anbieter:
	`bash scripts/register_connector.sh <provider_name>`
	3. Registrieren Sie den Verbraucher:
	`bash scripts/register_connector.sh <consumer_name>`
	Die Wahl der Namen hat keinen Einfluss auf die nächsten Schritte. Wir empfehlen, entweder `provider` und `consumer` oder `companyx` und zu verwenden`companyy`.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Registrierungsbefehle konfigurieren den DAPS-Dienst außerdem automatisch mit den erforderlichen Informationen, die aus den erstellten Zertifikaten und Schlüsseln abgerufen werden. Sammeln Sie Informationen, die Sie für spätere Installationsschritte benötigen, während Sie bei einem DAPS-Server angemeldet sind: 1. Von `omejdn-daps/config/clients.yml` get the `client id` für den Anbieter und den Verbraucher. Die `client id` Werte sind lange Zeichenketten mit Hexadezimalziffern. 2. Kopieren Sie aus dem `omejdn-daps/keys` Verzeichnis den Inhalt der Dateien`consumer.cert` , `consumer.key provider.cert` , und`provider.key` . Wir empfehlen, den Text zu kopieren und in Dateien mit ähnlichem Namen `daps-` auf Ihrer Workstation mit dem Präfix „A“ einzufügen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie sollten die Client-IDs für den Anbieter und den Verbraucher haben und vier Dateien in Ihrem Arbeitsverzeichnis auf Ihrer Workstation haben: • Der Name der Quelldatei `consumer.cert` wird zum Namen der Arbeitsstationsdatei `daps-consumer.cert`. • Der Name der Quelldatei `consumer.key` wird zum Namen der Arbeitsstationsdatei `daps-consumer.key`. • Der Name der Quelldatei `provider.cert` wird zum Namen der Arbeitsstationsdatei `daps-provider.cert`. • Der Name der Quelldatei `provider.key` wird zum Namen der Arbeitsstationsdatei `daps-provider.key`.	

Stellen Sie die Konnektoren der Teilnehmer bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Tractus-X EDC-Repository und	Für den Build des Tractus-X EDC-Connectors müssen die	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

verwenden Sie die Version 0.4.1.	Dienste PostgreSQL (Asset Database) und HashiCorp Vault (Secrets Managemen t) bereitgestellt und verfügbar sein.
	
	Es gibt viele verschiedene Versionen von Tractus-X EDC Helm-Charts. Dieses Muster spezifiziert Version 0.4.1, da es den DAPS-Server verwendet.
	
	Die neuesten Versionen verwenden Managed Identity Wallet (MIW) mit einer verteilte n Implementierung des Identitätsdienstes.
	
	Klonen Sie auf der Workstati on, auf der Sie die beiden Kubernetes-Namespa ces erstellt haben, das tractusx-edc-Repository und checken Sie den Branch aus. `release/0.4.1`
	
	`git clone https://g ithub.com/eclipse- tractusx/tractusx-edc`
	
	`cd tractusx-edc`
	
	`git checkout release/0 .4.1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Tractus-X EDC Helm-Diagramm.	Ändern Sie die Konfiguration der Tractus-X-Helm-Diagrammvorlage, damit beide Konnektoren miteinander interagieren können. Dazu würden Sie den Namespace zum DNS-Namen des Dienstes hinzufügen, sodass er von anderen Diensten im Cluster aufgelöst werden kann. Diese Änderungen sollten an der `charts/tractusx-connector/templates/_helpers.tpl` Datei vorgenommen werden. Dieses Muster bietet eine endgültige modifizierte Version dieser Datei, die Sie verwenden können. Kopieren Sie es und fügen Sie es in den `daps` Abschnitt der Datei ein`charts/tractusx-connector/templates/_helpers.tpl` . Stellen Sie sicher, dass Sie alle DAPS-Abhängigkeiten kommentieren in`charts/tractusx-connector/Chart.yaml` : `dependencies:`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> # IDS Dynamic Attribute Provisioning Service (IAM)
	  # - name: daps
	  # version: 0.0.1
	  # repository: "file://./subcharts/omejdn"
	  # alias: daps
	  # condition: install.daps</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Konnektoren für die Verwendung von PostgreSQL auf Amazon RDS.	(Optional) Die Amazon Relational Database Service (Amazon RDS) -Instance ist in diesem Muster nicht erforderlich. Wir empfehlen jedoch dringend, Amazon RDS oder Amazon Aurora zu verwenden, da sie Funktione n wie Hochverfügbarkeit sowie Sicherung und Wiederher stellung bieten.
	
	Gehen Sie wie folgt vor, um PostgreSQL auf Kubernete s durch Amazon RDS zu ersetzen:
	
	1. Stellen Sie die Amazon RDS for PostgreSQL PostgreSQL-Instance bereit.
	2. Kommentieren `Chart.yam l` Sie den `PostgreSQL` Abschnitt in.
	3. In `provider_ values.yml` und `consumer_values.ym l` konfigurieren Sie den `postgresql` Abschnitt wie folgt:
	
	`postgresql:`
	`auth:`
	`database: edc`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>password: <RDS PASSWORD>
	username: <RDS Username>
	jdbcUrl: jdbc:postgresql://<RDS DNS NAME>:5432/edc
	username: <RDS Username>
	password: <RDS PASSWORD>
	primary:
	persistence:
	enabled: false
	readReplicas:
	persistence:
	enabled: false</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implement ieren Sie den Provider-Connector und seine Dienste.	Gehen Sie wie folgt vor, um den Provider-Connector und seine Dienste zu konfiguri eren: 1. Führen Sie den folgenden Befehl aus, um die `provider_edc.yaml` Datei aus dem `edc_helm_configs` Verzeichnis in den aktuellen Helm-Chart-Ordner herunterzuladen: `wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/provider_edc.yaml> -P charts/tractusx-connector/` 2. Ersetzen Sie die folgenden Variablen (ebenfalls in der Datei markiert) durch ihre Werte: • `CLIENT_ID` – Die vom DAPS generierte ID. Die `CLIENT_ID` sollte sich `/srv/mvds/omejdn-daps/config/clients.yml/config/clients.yml` auf dem DAPS-Server befinden. Es sollte eine	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Folge von Hexadezim alzeichen sein. • `DAPS_URL`– Die URL des DAPS-Servers. Er sollte den DNS-Namen `https://{DNS name}` verwenden, den Sie bei der Ausführung der AWS CloudFormation Vorlage eingerichtet haben. • `VAULT_TOKEN` – Das Token, das für die Vault-Autorisierung verwendet werden soll. Wählen Sie einen beliebigen Wert. • `vault.fullnameOverride` – `vault-provider` . • `vault.hashicorp.url` – `http://vault-provider:8200/` . Bei den vorherigen Werten wird davon ausgegangen, dass es sich bei dem Bereitstellungsnamen und dem Namespace-Namen um einen Anbieter handelt. 3. Verwenden Sie die folgenden Befehle, um das Helm-Diagramm von Ihrer Workstation aus auszuführen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd charts/tractusx-connector`
	
	`helm dependency build`
	
	`helm upgrade --install provider ./ -f provider_edc.yaml -n provider`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie das Zertifikat und die Schlüssel zum Provider-Tresor hinzu.	Um Verwirrung zu vermeiden , sollten Sie die folgenden Zertifikate außerhalb des `tractusx-edc/charts` Verzeichnisses erstellen.
	
	Führen Sie beispielsweise den folgenden Befehl aus, um zu Ihrem Home-Verzeichnis zu wechseln:
	
	`cd ~`
	
	Sie müssen jetzt die vom Anbieter benötigten Geheimnisse zum Tresor hinzufügen.
	
	Die Namen der Geheimnis se im Tresor entsprechen den Werten der Schlüssel im `secretNames:` Abschnitt der `provider_edc.yml` Datei. Standardmäßig sind sie wie folgt konfiguriert:
	
	`secretNames:`
	`transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key`
	`transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>transferP
	roxyTokenEncryptio
	nAesKey: transfer-
	proxy-token-encryp
	tion-aes-key
	dapsPriva
	teKey: daps-private-
	key
	dapsPubli
	cKey: daps-public-key</pre>
	Zunächst werden ein AES-Schlüssel (Advanced Encryption Standard), ein privater Schlüssel, ein öffentlicher Schlüssel und ein selbstsigniertes Zertifikat generiert. Diese werden anschließend als Geheimnisse zum Tresor hinzugefügt.
	Außerdem sollte dieses Verzeichnis die `daps-provider.key` Dateien `daps-provider.cert` und enthalten, die Sie vom DAPS-Server kopiert haben.
	1. Führen Sie die folgenden Befehle aus:
	<pre># generate a private
	key
	openssl ecparam -name
	prime256v1 -genkey
	-noout -out provider-
	private-key.pem</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>```
	# generate correspon
	ding public key
	openssl ec -in
	 provider-private-k
	ey.pem -pubout -out
	 provider-public-ke
	y.pem
	# create a self-sign
	ed certificate
	openssl req -new -
	x509 -key provider-
	private-key.pem -out
	 provider-cert.pem -
	days 360
	# generate aes key
	openssl rand -base64
	 32 > provider-
	aes.key
	``</pre>	

	2. Bevor Sie die Geheimnis se zum Tresor hinzufüge n, konvertieren Sie sie von mehreren Zeilen in einzelne Zeilen, indem Sie die Zeilenumbrüche durch Folgendes ersetzen: \n
	<pre>```
	cat provider-private-
	key.pem | sed 's/$/\
	\\\n/'|tr -d '\\n' >
	 provider-private-k
	ey.pem.line
	cat provider-public-
	key.pem | sed 's/$/\
	\\\n/'|tr -d '\\n' >
	 provider-public-ke
	y.pem.line
	cat provider-cert.pem
	 | sed 's/$/\\\\
	n/'|tr -d '\\n' >
	``</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>provider-cert.pem.
	line
	cat provider-aes.key
	| sed 's/$/\\\\
	n/'|tr -d '\\n' >
	provider-aes.key.l
	ine
	
	## The following block
	is for daps certifica
	te and key
	openssl x509 -in
	daps-provider.cert -
	outform PEM | sed 's/
	$/\\\\n/'|tr -d '\\n'
	> daps-provider.cert
	.line
	cat daps-provider.key
	| sed 's/$/\\\\n/'|
	tr -d '\\n' > daps-
	provider.key.line</pre>	

	3. Führen Sie die folgenden Befehle aus, um die Geheimnisse zu formatier en, die dem Tresor hinzugefügt werden: <pre>JSONFORMAT='{"cont ent": "%s"}' #create a single line in JSON format printf "${JSONFO RMAT}\\n" "`cat provider-private- key.pem.line`" > provider-private-k ey.json printf "${JSONFO RMAT}\\n" "`cat provider-public-</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	key.pem.line`" > provider-public-key.json printf "${JSONFORMAT}\\n" "`cat provider-cert.pem.line`" > provider-cert.json printf "${JSONFORMAT}\\n" "`cat provider-aes.key.line`" > provider-aes.json  printf "${JSONFORMAT}\\n" "`cat daps-provider.key.line`" > daps-provider.key.json printf "${JSONFORMAT}\\n" "`cat daps-provider.cert.line`" > daps-provider.cert.json Die Geheimnisse liegen jetzt im JSON-Format vor und können dem Tresor hinzugefügt werden. 4. Führen Sie den folgenden Befehl aus, um den Pod-Namen für den Tresor abzurufen: kubectl get pods -n provider|egrep "vault|NAME"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Pod-Name wird ähnlich sein wie`"vault-provider-0"` . Dieser Name wird verwendet , wenn eine Portweiterleitung zum Tresor erstellt wird. Mit der Portweiterleitung können Sie auf den Tresor zugreifen, um den geheimen Schlüssel hinzuzufügen. Sie sollten dies von einer Workstation aus ausführen, für die AWS-Anmeldeinformationen konfiguriert sind. 5. Um auf den Tresor zuzugreifen, verwenden Sie, `kubectl` um eine Portweiterleitung zu konfigurieren: `kubectl port-forward <VAULT_POD_NAME> 8200:8200 -n provider` Sie sollten jetzt über Ihren Browser oder die CLI auf den Tresor zugreifen können. Browser 1. Navigieren Sie im Browser zu http://127.0.0.1:8200, wo der von Ihnen konfigurierte	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Port Forward verwendet wird. 2. Melden Sie sich mit dem Token an, das Sie zuvor konfiguri ert haben`provider_ edc.yml` . Erstellen Sie in der Secrets-Engine drei Secrets. Jedes Geheimnis hat einen `Path for this secret` Wert, bei dem es sich um den Geheimnam en handelt, der in der folgenden Liste aufgeführt ist. Innerhalb des `secret data` Abschnitts wird der Name des Schlüssels `content` und der Wert ist die einzelne Textzeile aus der jeweiligen Datei benannt`.line`. 3. Die geheimen Namen stammen aus dem `secretNames` Abschnitt in der `provider_ edc.yml` Datei. 4. Erstellen Sie die folgenden Geheimnisse: • Geheimnis `transfer-proxy-tok en-signer-private-key` mit dem Dateinamen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`provider-private-key.pem.line` • `transfer-proxy-token-signer-public-key` Geheim mit dem Dateinamen `provider-cert.pem.line` • `transfer-proxy-token-encryption-aes-key` Geheim mit dem Dateinamen `provider-aes.key.line` • `daps-private-key`Geheim mit dem Dateinamen `daps-provider.key.line` • `daps-public-key`Geheim mit dem Dateinamen `daps-provider.cert.line` Vault-CLI Die CLI verwendet auch den Port Forward, den Sie konfiguriert haben. 1. Installieren Sie Vault CLI auf Ihrer Workstation, indem Sie den Anweisungen in der HashiCorp Vault-Dokumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Um sich mit dem Token, das Sie eingerichtet haben, beim Tresor anzumelde nprovider_edc.yml , führen Sie den folgenden Befehl aus:
	`vault login -address= http://127.0.0.1:8 200`
	Mit dem richtigen Token sollte die Meldung angezeigt werden `"Success! You are now authenticated."`
	3. Führen Sie den folgenden Code aus, um die Secrets mithilfe der zuvor erstellte n Dateien im JSON-Format zu erstellen:
	`vault kv put -address= http://127.0.0.1:8 200 secret/transfer- proxy-token-signer-p rivate-key @provider -private-key.json vault kv put - address=http://12 7.0.0.1:8200 secret/ transfer-proxy-token -signer-public-key @provider-cert.json vault kv put -address= http://127.0.0.1:8 200 secret/transfer- proxy-token-encrypti`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on-aes-key @provider -aes.json vault kv put -address= http://127.0.0.1:8 200 secret/daps- private-key @daps-pro vider.key.json vault kv put - address=http://12 7.0.0.1:8200 secret/ daps-public-key @daps-provider.cer t.json	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implementieren Sie den Consumer-Connector und seine Dienste.	Die Schritte zur Konfiguration und Bereitstellung des Consumer ähneln denen, die Sie für den Anbieter ausgeführt haben: 1. Führen Sie die folgenden Befehle `consumer_edc.yaml` aus, um sie aus dem aws-patterns-edc-Repository in den Ordner `tractusx-edc/charts/tractusx-connector` zu kopieren: ``` cd tractusx-edc wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/consumer_edc.yaml -P charts/tractusx-connector/ ``` 2. Aktualisieren Sie die folgenden Variablen mit ihren tatsächlichen Werten: • `CONSUMER_CLIENT_ID` – Die von DAPS generierte ID. Die `CONSUMER_CLIENT_ID` sollte sich `config/clients.yml` auf dem DAPS-Server befinden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• `DAPS_URL`– Dieselbe DAPS-URL, die Sie für den Anbieter verwendet haben.
	• `VAULT_TOKEN` – Das Token, das für die Vault-Autorisierung verwendet werden soll. Wählen Sie einen beliebigen Wert.
	• `vault.fullnameOverride` – `vault-consumer`
	• `vault.hashicorp.url` – `http://vault-provider:8200/`
	
	Bei den vorherigen Werten wird davon ausgegangen, dass der Bereitstellungsname und der Namespace-Name `consumer`
	3. Verwenden Sie die folgenden Befehle, um das Helm-Diagramm auszuführen:
	
	`cd charts/tractusx-connector`
	
	`helm upgrade --install consumer ./ -f consumer_edc.yaml -n consumer`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Zertifikat und die Schlüssel zum Verbrauch ertresor hinzu.	Aus Sicherheitsgründen empfehlen wir, die Zertifika te und Schlüssel für jeden Datenraum-Teilnehmer neu zu generieren. Dieses Muster generiert Zertifikate und Schlüssel für den Verbraucher neu. Die Schritte sind denen für den Anbieter sehr ähnlich. Sie können die geheimen Namen in der `consumer_edc.yml` Datei überprüfen. Die Namen der Geheimnis se im Tresor entsprechen den Werten der Schlüssel im `secretNames:` Abschnitt von`consumer_edc.yml file`. Standardmäßig sind sie wie folgt konfiguriert: `secretNames: transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key transferProxyTokenEncryptionAesKey: transfer-`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>proxy-token-encryption-aes-key
	  dapsPrivateKey: daps-private-key
	  dapsPublicKey: daps-public-key</pre>
	Die `daps-consumer.key` Dateien `daps-consumer.cert` und, die Sie vom DAPS-Server kopiert haben, sollten bereits in diesem Verzeichnis vorhanden sein.
	1. Führen Sie die folgenden Befehle aus:
	<pre># generate a private key
	openssl ecparam -name prime256v1 -genkey -noout -out consumer-private-key.pem
	# generate corresponding public key
	openssl ec -in consumer-private-key.pem -pubout -out consumer-public-key.pem
	# create a self-signed certificate
	openssl req -new -x509 -key consumer-private-key.pem -out consumer-cert.pem -days 360
	# generate aes key</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`openssl rand -base64 32 > consumer-aes.key`
	2. Bearbeiten Sie die Dateien manuell, um Zeilenumbrüche durch sie zu ersetzen\n, oder verwenden Sie drei Befehle, die den folgenden ähneln:
	`cat consumer-private-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-private-key.pem.line`
	`cat consumer-public-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-public-key.pem.line`
	`cat consumer-cert.pem | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-cert.pem.line`
	`cat consumer-aes.key | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-aes.key.line`
	`cat daps-consumer.cert | sed 's/$/\\\\n/'|tr -d '\\n' > daps-consumer.cert.line`
	`cat daps-consumer.key | sed 's/$/\\\\n/'| tr -d '\\n' > daps-consumer.key.line`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Führen Sie die folgenden Befehle aus, um die Geheimnisse zu formatier en, die zu Vault hinzugefügt werden:
	
	`JSONFORMAT='{"cont ent": "%s"}'`
	
	`#create a single line in JSON format`
	
	`printf "${JSONFO RMAT}\\n" "`cat consumer-private- key.pem.line`" > consumer-private-k ey.json`
	`printf "${JSONFO RMAT}\\n" "`cat consumer-public- key.pem.line`" > consumer-public-ke y.json`
	`printf "${JSONFO RMAT}\\n" "`cat consumer-cert.pem. line`" > consumer- cert.json`
	`printf "${JSONFO RMAT}\\n" "`cat consumer-aes.key.l ine`" > consumer- aes.json`
	
	`printf "${JSONFO RMAT}\\n" "`cat daps- consumer.key.line`" > daps-consumer.key. json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`printf "${JSONFO RMAT}\\n" "`cat daps-consumer.cert.line`" > daps-consumer.cert .json`
	
	Die Geheimnisse liegen jetzt im JSON-Format vor und können dem Tresor hinzugefügt werden.
	
	4. Führen Sie den folgenden Befehl aus, um den Pod-Namen für den Consumer-Tresor abzurufen:
	
	`kubectl get pods -n consumer | egrep "vault|NAME"`
	
	Der Pod-Name wird ähnlich sein wie`"vault-consumer-0"` . Dieser Name wird verwendet , wenn eine Portweiterleitung zum Tresor erstellt wird. Mit der Portweiterleitung können Sie auf den Tresor zugreifen, um den geheimen Schlüssel hinzuzufügen. Sie sollten dies von einer Workstation aus ausführen, für die AWS Anmeldeinformationen konfiguriert sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Um auf den Tresor zuzugreifen, verwenden Sie, `kubectl` um eine Portweiterleitung zu konfigurieren: `kubectl port-forward <VAULT_POD_NAME> 8201:8200 -n consumer` Der lokale Port ist diesmal 8201, sodass Sie Portweiterleitungen sowohl für den Hersteller als auch für den Verbraucher einrichten können. Browser Sie können Ihren Browser verwenden, um eine Verbindung zu http://localhost:8201/ herzustellen, um auf den Verbraucher-Tresor zuzugreifen und die Secrets mit Namen und Inhalt wie beschrieben zu erstellen. Die Geheimnisse und Dateien, die den Inhalt enthalten, sind die folgenden: • Geheim `transfer-proxy-token-signer-private-key` mit dem Namen der Datei	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`consumer-private-key.pem.line`
	• `transfer-proxy-token-signer-public-key` Geheim mit dem Dateinamen `consumer-cert.pem.line`
	• `transfer-proxy-token-encryption-aes-key` Geheim mit dem Dateinamen `consumer-aes.key.line`
	
	Vault-CLI
	
	Mit der Vault-CLI können Sie die folgenden Befehle ausführen, um sich beim Tresor anzumelden und die Secrets zu erstellen:
	
	1. Melden Sie sich mit dem Token, das Sie darin konfiguriert haben, beim Tresor an`consumer_edc.yml` :
	
	`vault login -address=http://127.0.0.1:8201`
	
	Mit dem richtigen Token sollte die Meldung angezeigt werden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`"Success! You are now authenticated."`
	2. Führen Sie den folgenden Code aus, um die Secrets mithilfe der zuvor erstellten Dateien im JSON-Format zu erstellen:
	`vault kv put -address=http://127.0.0.1:8201 secret/transfer-proxy-token-signer-private-key @consumer-private-key.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/transfer-proxy-token-signer-public-key @consumer-cert.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/transfer-proxy-token-encryption-aes-key @consumer-aes.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/daps-private-key @daps-consumer.key.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/daps-public-key @daps-consumer.cert.json`	

Richten Sie einen HTTP-Client ein, um mit der Management-API der Konnektoren zu interagieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die Portweiterleitung ein.	1. Führen Sie die folgenden Befehle aus, um den Status der Pods zu überprüfen:
	`kubectl get pods -n provider`
	`kubectl get pods -n consumer`
	2. Um sicherzustellen, dass die Kubernetes-Bereitstellungen erfolgreich waren, schauen Sie sich die Protokolle der Kubernetes-Pods für Anbieter und Verbraucher an, indem Sie die folgenden Befehle ausführen:
	`kubectl logs -n provider <producer control plane pod name>`
	`kubectl logs -n consumer <consumer control plane pod name>`
	Der Cluster ist privat und nicht öffentlich zugänglich. Um mit den Konnektoren zu interagieren, verwenden Sie die Kubernetes-Port-Forwarding-Funktion, um
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den von Ihrem Computer generierten Datenverkehr an die Connector-Steuerebene weiterzuleiten.
	
	1. Leiten Sie auf dem ersten Terminal die Anfragen des Verbrauchers über Port 8300 an die Management-API weiter:
	
	`kubectl port-forward deployment/consumer-tractusx-connector-controlplane 8300:8081 -n consumer`
	
	2. Leiten Sie auf dem zweiten Terminal die Anfragen des Anbieters über Port 8400 an die Management-API weiter:
	
	`kubectl port-forward deployment/provider-tractusx-connector-controlplane 8400:8081 -n provider`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie S3-Buckets für den Anbieter und den Verbraucher.	Der EDC-Connector verwendet derzeit keine temporären AWS-Anmel deinformationen, wie sie beispielsweise bei der Übernahme einer Rolle bereitgestellt werden. Der EDC unterstützt nur die Verwendung einer Kombinati on aus IAM-Zugriffsschlüs sel-ID und geheimer Zugriffss chlüssel-ID. Für spätere Schritte sind zwei S3-Buckets erforderl ich. Ein S3-Bucket wird zum Speichern von Daten verwendet, die vom Anbieter zur Verfügung gestellt werden. Der andere S3-Bucket ist für Daten vorgesehen, die vom Verbraucher empfangen werden. Der IAM-Benutzer sollte nur die Berechtigung haben, Objekte in den beiden benannten Buckets zu lesen und zu schreiben. Eine Zugangsschlüssel-ID und ein geheimes Zugriffss chlüsselpaar müssen erstellt und sicher aufbewahrt werden. Nach der Außerbetriebnahme	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieses MVDS sollte der IAM-Benutzer gelöscht werden. Der folgende Code ist ein Beispiel für eine IAM-Richtlinie für den Benutzer: `{ "Version": "2012-10-17", "Statement": [{ "Sid": "Stmt1708699805237", "Action": ["s3:GetObject", "s3:GetObjectVersion", "s3:ListAllMyBuckets", "s3:ListBucket", "s3:ListBucketMultipartUploads", "s3:ListBucketVersions", "s3:PutObject"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<S3 Provider Bucket>", "arn:aws:s3:::<S3 Consumer Bucket>", "arn:aws:s3:::<S3 Provider Bucket>/*",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"arn:aws: s3:::<S3 Consumer Bucket>/*"] }] }	
Richten Sie Postman so ein, dass es mit dem Konnektor interagiert.	Sie können jetzt über Ihre EC2-Instance mit den Konnektoren interagieren. Verwenden Sie Postman als HTTP-Client und stellen Sie Postman-Sammlungen sowohl für den Provider- als auch für den Consumer-Connector bereit. Importieren Sie die Sammlungen aus dem `aws-pattern-edc` Repository in Ihre Postman-Instanz. Dieses Muster verwendet Postman-Sammlungsvariablen, um Eingaben für Ihre Anfragen bereitzustellen.	App-Entwickler, Dateningenieur

Stellen Sie über den Konnektor Daten zum CO2-Fußabdruck von Unternehmen X bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Daten zur CO2-Emissionsintensität für die gemeinsame Nutzung vor.	Zunächst müssen Sie entscheiden, welche Datenmenge gemeinsam genutzt werden soll. Die Daten von Unternehmen	Dateningenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	X stellen den CO2-Fußab druck seiner Fahrzeugf lotte dar. Das Gewicht ist das Bruttofahrzeuggewicht (GVW) in Tonnen, und die Emissionen werden gemäß der Wheel-to-Well (WTW) - Messung in Gramm CO2 pro Tonnenkilometer (g CO2 e/t-km) angegeben: • Fahrzeugtyp: Van; Gewicht: < 3,5; Emissionen: 800 • Fahrzeugtyp: Stadtlast er; Gewicht: 3,5—7,5; Emissionen: 315 • Fahrzeugtyp: Mittlerer Nutzfahrzeug (MGV); Gewicht: 7,5—20; Emissionen: 195 • Fahrzeugtyp: Schwerlas twagen (Lkw); Gewicht: > 20; Emissionen: 115 Die Beispieldaten befinden sich in der `carbon_em issions_data.json` Datei im `aws-patterns-edc` Repository. Unternehmen X verwendet Amazon S3 zum Speichern von Objekten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Erstellen Sie den S3-Bucket und speichern Sie dort das Beispieldatenobjekt. Die folgenden Befehle erstellen einen S3-Bucket mit Standardsicherheitseinstellungen. Wir empfehlen dringend, sich mit den bewährten Sicherheitsmethoden für Amazon S3 vertraut zu machen.
	
	`aws s3api create-bucket --bucket <BUCKET_NAME> --region <AWS_REGION>`
	`# You need to add '--create-bucket-configuration LocationConstraint=<AWS_REGION>' if you want to create # the bucket outside of us-east-1 region`
	
	`aws s3api put-object --bucket <BUCKET_NAME> \`
	`--key <S3 OBJECT NAME> \`
	`--body <PATH OF THE FILE TO UPLOAD>`
	
	Der S3-Bucket-Name sollte weltweit eindeutig sein. Weitere Informationen zu Benennungsregeln finden Sie in der AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie das Datenobjekt mithilfe von Postman beim Connector des Anbieters.	Ein EDC-Connector-Datenobjekt enthält den Namen der Daten und ihren Speicherort. In diesem Fall zeigt das EDC-Connector-Datenobjekt auf das erstellte Objekt im S3-Bucket: • Konnektor: Anbieter • Anfrage: Asset erstellen • Sammlungsvariablen: Aktualisieren`ASSET_NAME`. Wählen Sie einen aussagekräftigen Namen, der das Asset repräsentiert. • Hauptteil der Anfrage: Aktualisieren Sie den Hauptteil der Anfrage mit dem S3-Bucket, den Sie für den Anbieter erstellt haben. `"dataAddress": { "edc:type": "AmazonS3", "name": "Vehicle Carbon Footprint", "bucketName": "<REPLACE WITH THE SOURCE BUCKET NAME>", "keyName": "<REPLACE WITH YOUR OBJECT NAME>", "region": "<REPLACE WITH THE BUCKET REGION>",`	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"accessKeyId": "<REPLACE WITH YOUR ACCESS KEY ID>", "secretAccessKey": "<REPLACE WITH SECRET ACCESS KEY>" }</pre> • Antwort: Eine erfolgreiche Anfrage gibt die Erstellungszeit und die Asset-ID des neu erstellten Assets zurück. <pre>{ "@id": "c89aa31c-ec4c-44ed-9e8c-1647f19d7583" }</pre> • Sammlungsvariable ASSET_ID: Aktualisieren Sie die Sammlungsvariable Postman `ASSET_ID` mit der ID, die nach der Erstellung automatisch vom EDC-Connector generiert wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Definieren Sie die Nutzungsrichtlinie des Assets.	Ein EDC-Datenbestand muss klaren Nutzungsrichtlinien zugeordnet sein. Erstellen Sie zunächst die Richtliniendefinition im Provider-Connector.
	
	Die Richtlinie von Unternehmen X besteht darin, den Teilnehmern des Datenraums die Nutzung der Daten zum CO2-Fußabdruck zu ermöglichen.
	
	• Hauptteil der Anfrage:
	  • Anschluss: Anbieter
	  • Anfrage: Richtlinie erstellen
	  • Sammlungsvariablen: Aktualisieren Sie die `Policy Name` Variable mit dem Namen der Richtlinie.
	• Antwort: Bei einer erfolgreichen Anfrage werden die Uhrzeit der Erstellung und die Richtlinien-ID der neu erstellten Richtlinie zurückgegeben. Aktualisieren Sie die Sammlungsvariable `POLICY_ID` mit der ID der Richtlinie, die vom EDC-Connector nach der Erstellung generiert wurde.
		App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie ein EDC-Vertr agsangebot für das Asset und dessen Nutzungsrichtlinien.	Damit andere Teilnehme r Zugriff auf Ihre Daten beantragen können, bieten Sie diesen in einem Vertrag an, der die Nutzungsbedingungen und Berechtigungen festlegt: • Konnektor: Anbieter • Anfrage: Vertragsdefinition erstellen • Sammlungsvariablen : Aktualisieren Sie die `Contract Name` Variable mit einem Namen für das Vertragsangebot oder die Vertragsdefinition.	App-Entwickler, Dateninge nieur

Entdecken Sie die Vorteile und erzielen Sie eine Einigung über die definierten Verträge

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fordern Sie den von Unternehmen X gemeinsam genutzten Datenkatalog an.	Als Datenkonsument im Datenraum muss Unternehm en Y zunächst herausfinden, welche Daten von anderen Teilnehmern gemeinsam genutzt werden. In dieser Grundkonfiguration können Sie dazu den Consumer-Connector bitten, den Katalog der verfügbar en Ressourcen direkt vom	App-Entwickler, Dateninge nieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Provider-Connector anzuforderrn. • Konnektor: Consumer • Anfrage: Katalog anfordern • Antwort: Alle verfügbaren Datenbestände des Anbieters zusammen mit den beigefügten Nutzungsrichtlinien. Suchen Sie als Datenverbraucher nach dem Vertrag, für den Sie sich interessieren, und aktualisieren Sie die folgenden Erfassungsvariablen entsprechend. • `CONTRACT_OFFER_ID` – Die ID des Vertragsangebots, das der Verbraucher aushandeln möchte • `ASSET_ID`– Die ID des Vermögenswerts, den der Verbraucher aushandeln möchte • `PROVIDER_CLIENT_ID` – Die ID des Provider-Connectors, mit dem verhandelt werden soll	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie eine Vertragsverhandlung für die Daten zur CO2-Emissionsintensität von Unternehmen X.	Nachdem Sie nun den Vermögenswert identifiziert haben, den Sie nutzen möchten, leiten Sie einen Vertragsverhandlungsprozess zwischen dem Verbraucher und dem Anbieter ein. • Konnektor: Verbraucher • Anfrage: Vertragsverhandlung • Sammlungsvariablen: Aktualisieren Sie die `CONSUMER_CLIENT_ID` Variable mit der ID des Consumer-Connectors, mit dem Sie verhandeln möchten. Der Vorgang kann einige Zeit dauern, bis der Status VERIFIED erreicht wird. Mithilfe der `Get Negotiation` Anfrage können Sie den Status der Vertragsverhandlung und die entsprechende Vereinbarungs-ID überprüfen.	App-Entwickler, Dateningenieur

Verbrauchen Sie die Daten mithilfe der Vertragsvereinbarung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbrauchen Sie Daten von HTTP-Endpunkten.	(Option 1) Um die HTTP-Datenebene für die Nutzung von Daten im Datenraum zu verwenden, können Sie webhook.site verwenden, um einen HTTP-Server zu emulieren und den Übertragungsprozess im Consumer-Connector zu initiieren: • Konnektor: Verbraucher • Anfrage: Vertragsverhandlung • Sammlungsvariablen: Aktualisieren Sie die `Contract Agreement ID` Variable mit der ID der Vertragsvereinbarung, die vom EDC-Connector generiert wurde. • Hauptteil der Anfrage: Aktualisieren Sie den Hauptteil der Anfrage und geben Sie HTTP `dataDestination` neben dem Webhook folgende URL an: `{ "dataDestination": { "type": "HttpProxy"`	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
    },
    "privateP
roperties": {
      "receiver
HttpEndpoint":
 "<WEBHOOK URL>"
    }
}
```

Der Connector sendet die zum Herunterladen der Datei erforderlichen Informationen direkt an die Webhook-URL.

Die empfangene Nutzlast ähnelt der folgenden:

```
{
  "id": "dcc90391
-3819-4b54-b401-1a
005a029b78",
  "endpoint":
 "http://consumer-t
ractusx-connector-
dataplane.consumer
:8081/api/public",
  "authKey":
 "Authorization",
  "authCode": "<AUTH
 CODE YOU RECEIVE IN
 THE ENDPOINT>",
  "properties": {
    "https://
w3id.org/edc/v0.0.
1/ns/cid": "vehicle-
carbon-footprint-c
ontract:4563abf7-5
dc7-4c28-bc3d-97f4
5e32edac:b073669b-
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	db20-4c83-82df-46b 583c4c062" } } Verwenden Sie die empfangenen Anmeldeinformationen, um das S3-Asset abzurufen, das vom Anbieter gemeinsam genutzt wurde. In diesem letzten Schritt müssen Sie die Anfrage an die Consumer-Datenebene senden (Ports ordnungsgemäß weiterleiten), wie in der Payload (`endpoint`) angegeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten aus S3-Buckets direkt konsumieren.	(Option 2) Verwenden Sie die Amazon S3 S3-Integration mit dem EDC-Connector und verweisen Sie direkt auf den S3-Bucket in der Verbrauch erinfrastruktur als Ziel: • Hauptteil der Anfrage: Aktualisieren Sie den Hauptteil der Anfrage, um den S3-Bucket als DataDestination anzugeben. Dies sollte der S3-Bucket sein, den Sie zuvor zum Speichern von Daten erstellt haben, die vom Verbraucher empfangen wurden. `{ "dataDestination": { "type": "AmazonS3", "bucketName": "{{ REPLACE WITH THE DESTINATION BUCKET NAME }}", "keyName": "{{ REPLACE WITH YOUR OBJECT NAME }}", "region": "{{ REPLACE WITH THE BUCKET REGION }}", "accessKeyId": "{{ REPLACE WITH YOUR ACCESS KEY ID }}",`	Dateningenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"secretAc
	cessKey": "{{ REPLACE
	WITH SECRET ACCESS
	KEY }}"
	}
	}
	}</pre>	

Fehlerbehebung

Problem	Lösung
Der Konnektor könnte ein Problem mit dem PEM-Format des Zertifikats aufwerfen.	Verketten Sie den Inhalt jeder Datei zu einer einzigen Zeile, indem Sie Folgendes hinzufügen. \n

Zugehörige Ressourcen

- DSSC
- Aufbau von Datenräumen für Anwendungsfälle im Bereich Nachhaltigkeit (AWS Prescriptive Guidance Guidance-Strategie von Think-IT)
- AWS für Datenräume
- Tractus-X-Dokumentation
- DAPS
- Aktivierung der gemeinsamen Nutzung von Daten über Datenräume und AWS (Blogbeitrag)

Zusätzliche Informationen

Spezifikationen für den Datenraum

Teilnehmer

Teilnehmer	Beschreibung des Unternehmens	Schwerpunkt des Unternehmens
Firma X	Betreibt eine Fahrzeugflotte in ganz Europa und Südamerika, um verschiedene Güter zu transportieren.	Zielt darauf ab, datengestützte Entscheidungen zu treffen, um die Intensität seines CO2-Fußabdrucks zu reduzieren.
Firma Y	Eine Umweltregulierungsbehörde	Setzt Umweltvorschriften und -richtlinien durch, die darauf abzielen, die Umweltauswirkungen von Unternehmen und Branchen, einschließlich der Intensität der CO2-Emissionen, zu überwachen und zu mindern.

Geschäftsszenario

Unternehmen X nutzt Datenraumtechnologie, um Daten zum CO2-Fußabdruck an einen Compliance-Auditor, Unternehmen Y, weiterzugeben, um die Umweltauswirkungen der Logistikaktivitäten von Unternehmen X zu bewerten und zu berücksichtigen.

Behörde für den Datenraum

Die Data Space Authority ist ein Konsortium der Organisationen, die für den Datenraum zuständig sind. In diesem Muster bilden sowohl Unternehmen X als auch Unternehmen Y das Leitungsorgan und stellen eine föderierte Datenschutzbehörde dar.

Komponenten des Datenraums

Komponente	Gewählte Implementierung	Zusätzliche Informationen
Protokoll für den Austausch von Datensätzen	Dataspace-Protokoll, Version 0.8	• JSON-LD • Datenkatalog-Wortschatz (DCAT)

Anschluss für den Datenraum	Tractus-X EDC-Anschluss Version 0.4.1	• EDC-Erweiterungen
Richtlinien für den Datenaustausch	Standard-USE-Richtlinie	• Öffnen Sie die Sprache für digitale Rechte (ODRL)

Dienste für den Datenraum

Service	Implementierung	Zusätzliche Informationen
Identitätsdienst	Dynamisches Attributbereitstellungssystem (DAPS)	„Ein Dynamic Attribute Provisioning System (DAPS) hat die Absicht, bestimmte Eigenschaften von Organisationen und Konnektoren zu ermitteln. Daher müssen Dritte letzteren nicht vertrauen, vorausgesetzt, sie vertrauen den DAPS-Assertionen.“ — DAPS Um sich auf die Logik des Connectors zu konzentrieren, wird der Datenraum mithilfe von Docker Compose auf einem Amazon EC2 EC2-Computer bereitgestellt.
Discovery Service	Föderierter Gaia-X-Katalog	„Der Federated Catalogue stellt eine indexierte Sammlung von Gaia-X-Selbstbeschreibungen dar, die es ermöglichen, Anbieter und deren Serviceangebote zu finden und auszuwählen. Bei den Selbstbeschreibungen handelt es sich um Informati

		onen, die von den Teilnehme rn über sich selbst und ihre Dienstleistungen in Form von Eigenschaften und Ansprüche n bereitgestellt werden.“ — Kickstarter für das Gaia-X-Ök osystem

Daten, die ausgetauscht werden sollen

Datenbestände	Beschreibung	Format
Daten zu den CO2-Emiss ionen	Intensitätswerte für verschied ene Fahrzeugtypen in der angegebenen Region (Europa und Südamerika) aus der gesamten Fahrzeugflotte	JSON-Datei

Datenmodell

```
{
  "region": "string",
  "vehicles": [
// Each vehicle type has its Gross Vehicle Weight (GVW) category and its emission
 intensity in grams of CO2 per Tonne-Kilometer (g CO2 e/t-km) according to the "Well-
to-Wheel" (WTW) measurement.
    {
      "type": "string",
      "gross_vehicle_weight": "string",
      "emission_intensity": {
        "CO2": "number",
        "unit": "string"
      }
    }
  ]
}
```

Tractus-X EDC-Anschluss

Die Dokumentation der einzelnen Tractus-X EDC-Parameter finden Sie in der Datei mit den Originalwerten.

In der folgenden Tabelle sind alle Dienste zusammen mit ihren entsprechenden exponierten Ports und Endpunkten als Referenz aufgeführt.

Name des Dienstes	Port und Pfad
Steuerebene	• Verwaltung: – Port: 8081 Pfad: `/management` • Steuerung – Port: 8083 Pfad: `/control` • Protokoll-Port: 8084 Pfad: `/api/v1/dsp` • Metriken – Port: 9090 Pfad: `/metrics` • Beobachtbarkeit – Port: 8085 Pfad: `/observability`
Datenebene	Standard – Port: 8080 Pfad: `/api` public – Port: 8081 Pfad: `/api/dataplane/control` proxy – Port: 8186 Pfad: `/proxy` Metriken – Port: 9090 Pfad: `/metrics` Beobachtbarkeit – Port: 8085 Pfad: `/observability`
Vault	Anschluss: 8200
PostgreSQL	Hafen: 5432

Manager verwenden AWS Secrets Manager

Es ist möglich, Secrets Manager anstelle von HashiCorp Vault als Secrets Manager zu verwenden. Dazu müssen Sie die AWS Secrets Manager EDC-Erweiterung verwenden oder erstellen.

Sie sind für die Erstellung und Pflege Ihres eigenen Images verantwortlich, da Tractus-X keine Unterstützung für Secrets Manager bietet.

Um dies zu erreichen, müssen Sie die Build-Gradle-Dateien sowohl der Steuerungsebene als auch der Datenebene des Konnektors ändern, indem Sie Ihre AWS Secrets Manager EDC-Erweiterung eingeben (ein Beispiel finden Sie in diesem Maven-Artefakt) und dann das Docker-Image erstellen, verwalten und referenzieren.

Weitere Informationen zum Refactoring des Docker-Images des Tractus-X-Connectors finden Sie unter Refactor Tractus-X EDC Helm-Diagramme.

Der Einfachheit halber vermeiden wir es, das Connector-Image nach diesem Muster neu zu erstellen, und verwenden Vault. HashiCorp

Einrichten einer sprachspezifischen Sortierung für Amazon-Redshift-Abfrageergebnisse mithilfe einer skalaren Python-UDF

Erstellt von Ethan Stark (AWS)

Umgebung: Produktion	Technologien: Analytik	AWS-Services: Amazon Redshift

Übersicht

Dieses Muster enthält Schritte und Beispielcode für die Verwendung einer skalaren Python-UDF (benutzerdefinierte Funktion), um die linguistische Sortierung ohne Berücksichtigung der Groß- und Kleinschreibung für Amazon-Redshift-Abfrageergebnisse einzurichten. Es ist erforderlich, eine skalare Python-UDF zu verwenden, da Amazon Redshift Ergebnisse basierend auf der binären UTF-8-Reihenfolge zurückgibt und keine sprachspezifische Sortierung unterstützt. Eine Python-UDF ist Nicht-SQL-Verarbeitungscode, der auf einem Python-2.7-Programm basiert und in einem Data Warehouse ausgeführt wird. Sie können Python-UDF-Code mit einer SQL-Anweisung in einer einzigen Abfrage ausführen. Weitere Informationen finden Sie im Beitrag Introduction to Python UDFs im Amazon Redshift AWS Big Data Blog.

Die Beispieldaten in diesem Muster basieren zu Demonstrationszwecken auf dem Türkischen Alphabet. Die skalare Python-UDF in diesem Muster wurde entwickelt, damit die Standardabfrageergebnisse von Amazon Redshift der sprachlichen Reihenfolge der Zeichen in der Türkischen Sprache entsprechen. Weitere Informationen finden Sie im Beispiel für eine Türkische Sprache im Abschnitt Zusätzliche Informationen dieses Musters. Sie können die skalare Python-UDF in diesem Muster für andere Sprachen ändern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Amazon-Redshift-Cluster mit einer Datenbank, einem Schema und Tabellen
- Amazon-Redshift-Benutzer mit Berechtigungen CREATE TABLE und CREATE FUNCTION
- Python 2.7 oder höher

Einschränkungen

Bei der linguistischen Sortierung, die von den Abfragen in diesem Muster verwendet wird, wird die Groß- und Kleinschreibung nicht beachtet.

Architektur

Technologie-Stack

- Amazon Redshift
- Python-UDF

Tools

AWS-Services

- Amazon Redshift ist ein verwalteter Data Warehouse-Service im Petabyte-Bereich in der AWS Cloud. Amazon Redshift ist in Ihren Data Lake integriert, sodass Sie Ihre Daten verwenden können, um neue Erkenntnisse für Ihr Unternehmen und Ihre Kunden zu gewinnen.

Andere Tools

- Benutzerdefinierte Python-Funktionen (UDFs)sind Funktionen, die Sie in Python schreiben und dann in SQL-Anweisungen aufrufen können.

Polen

Entwickeln von Code zum Sortieren von Abfrageergebnissen in sprachlicher Reihenfolge

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle für Ihre Beispieldaten.	Verwenden Sie die folgenden SQL-Anweisungen, um eine Tabelle in Amazon Redshift zu erstellen und Ihre Beispieldaten in die Tabelle einzufügen:	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`CREATE TABLE my_table (first_name varchar(30));`
	
	`INSERT INTO my_table (first_name) VALUES ('ali'), ('Ali'), ('ırmak'), ('IRMAK'), ('irem'), ('İREM'), ('oğuz'), ('OĞUZ'), ('ömer'), ('ÖMER'), ('sedat'), ('SEDAT'), ('şule'),`
	
	Hinweis: Die Vornamen in den Beispieldaten enthalten Sonderzeichen aus dem englischen Alphabet. Weitere Informationen zu Überlegungen in Türkischer Sprache für dieses Beispiel finden Sie im Beispiel für eine Türkische Sprache im Abschnitt Zusätzliche Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Standards ortierung der Beispieldaten.	Um die Standardsortierung Ihrer Beispieldaten in Amazon Redshift anzuzeigen, führen Sie die folgende Abfrage aus:
	`SELECT first_name FROM my_table ORDER BY first_name;`
	Die Abfrage gibt die Liste der Vornamen aus der Tabelle zurück, die Sie zuvor erstellt haben:
	`first_name`
	`---------------`
	`Ali`
	`IRMAK`
	`OĞUZ`
	`SEDAT`
	`ali`
	`irem`
	`oğuz`
	`sedat`
	`ÖMER`
	`ömer`
	`İREM`
	`ırmak`
	`ŞULE`
	`şule`
	Die Abfrageergebnisse liegen nicht in der richtigen Reihenfol ge vor, da die standardmäßige binäre UTF-8-Reihenfolge die sprachliche Reihenfolge der
		Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Türkischen Sonderzeichen nicht berücksichtigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine skalare Python-UDF.	Verwenden Sie den folgenden SQL-Code, um eine skalare Python-UDF zu erstellen: `CREATE OR REPLACE FUNCTION collate_sort (value varchar) RETURNS varchar IMMUTABLE AS $$ def sort_str(val): import string dictionary = { 'I': 'ı', 'ı': 'h~', 'İ': 'i', 'Ş': 's~', 'ş': 's~', 'Ğ': 'g~', 'ğ': 'g~', 'Ü': 'u~', 'ü': 'u~', 'Ö': 'o~', 'ö': 'o~', 'Ç': 'c~', 'ç': 'c~' } for key, value in dictionary.items(): val = val.replace(key, value) return val.lower()`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`    return sort_str( value)`
	
	`$$ LANGUAGE plpythonu;`	

Fragen Sie die Beispieldaten ab.	Um die Beispieldaten mithilfe der Python-UDF abzufragen, führen Sie die folgende SQL-Abfrage aus:
	
	`SELECT first_name FROM my_table ORDER BY collate_order(firs t_name);`
	
	Die Abfrage gibt jetzt die Beispieldaten in türkische r sprachlicher Reihenfolge zurück:
	
	`first_name`
	`---------------`
	`ali`
	`Ali`
	`ırmak`
	`IRMAK`
	`irem`
	`İREM`
	`oğuz`
	`OĞUZ`
	`ömer`
	`Ömer`
	`sedat`
	`SEDAT`
	`şule`
	`ŞULE`
		Dateningenieur

Zugehörige Ressourcen

- ORDER BY-Klausel (Amazon-Redshift-Dokumentation)
- Erstellen einer skalaren Python-UDF (Amazon-Redshift-Dokumentation)

Zusätzliche Informationen

Beispiel für eine Türkische Sprache

Amazon Redshift gibt Abfrageergebnisse basierend auf binärer UTF-8-Sortierreihenfolge zurück, nicht sprachspezifische Sortierreihenfolge. Das heißt, wenn Sie eine Amazon-Redshift-Tabelle mit Türkischen Zeichen abfragen, werden die Abfrageergebnisse nicht entsprechend der sprachlichen Reihenfolge der Türkischen Sprache sortiert. Die Türkische Sprache enthält sechs Sonderzeichen (, , , ö, und ü), die nicht im lateinischen Alphabet vorkommen. Diese Sonderzeichen werden an das Ende einer sortierten Ergebnismenge platziert, die auf der binären UTF-8-Reihenfolge basiert, wie die folgende Tabelle zeigt.

Binäre UTF-8-Reihenfolge	Türkische Sprachreihenfolge
a	a
b	b
c	c
d	CCP (*)
e	d
f	e
g	f
h	g
i	(*)
j	h
k	Telefonie (*)

l	i
m	j
n	k
o	l
p	m
r	n
S	o
t	ö (*)
u	p
V	r
y	S
z	(*)
CCP (*)	t
(*)	u
Bol (*)	ü (*)
ö (*)	V
(*)	y
ü (*)	z

Hinweis: Das Sternchen (*) steht für ein Sonderzeichen in der Sprache Türkisch.

Wie die obige Tabelle zeigt, liegt das Sonderzeichen zwischen c und d in der türkischen sprachlichen Reihenfolge, erscheint aber nach z in der binären UTF-8-Reihenfolge. Die skalare Python-UDF in diesem Muster verwendet das folgende Zeichenersetzungswörterbuch, um die Türkischen Sonderzeichen durch entsprechende lateinische Zeichen zu ersetzen.

Türkisches Sonderzeichen	Lateinisch-Lanisch-Zeichen
ç	c~
ı	h~
ğ	g~
ö	o~
ş	s~
ü	u~

Hinweis: Ein Tildezeichen (~) wird an das Ende der lateinischen Zeichen angehängt, die ihre entsprechenden Türkischen Sonderzeichen ersetzen.

Ändern einer skalaren Python-UDF-Funktion

Verwenden Sie den folgenden SQL-Code, um die skalare Python-UDF-Funktion von diesem Muster zu ändern, sodass die Funktion einen Ortungsparameter akzeptiert und ein Mehrfachtransaktionswörterbuch unterstützt:

```
CREATE OR REPLACE FUNCTION collate_sort (value varchar, locale varchar)
RETURNS varchar
IMMUTABLE
AS
$$
    def sort_str(val):
       import string
       # Turkish Dictionary
       if locale == 'tr-TR':
            dictionary = {
               'I': 'ı',
               'ı': 'h~',
               'İ': 'i',
               'Ş': 's~',
               'ş': 's~',
               'Ğ': 'g~',
               'ğ': 'g~',
               'Ü': 'u~',
```

```
                'ü': 'u~',
                'Ö': 'o~',
                'ö': 'o~',
                'Ç': 'c~',
                'ç': 'c~'
        }
        # German Dictionary
        if locale == 'de-DE':
            dictionary = {
                ....
                ....
        }

        for key, value in dictionary.items():
            val = val.replace(key, value)

        return val.lower()

    return sort_str(value)

$$ LANGUAGE plpythonu;
```

Der folgende Beispielcode zeigt, wie die geänderte Python-UDF abgefragt wird:

```
SELECT first_name FROM my_table ORDER BY collate_order(first_name, 'tr-TR');
```

Abonnieren einer Lambda-Funktion für Ereignisbenachrichtigungen aus S3-Buckets in verschiedenen AWS-Regionen

Erstellt von Bolsh Konathala (AWS) und Arindomkar (AWS)

Umgebung: Produktion	Technologien: Analytik	AWS-Services: AWS Lambda ;Amazon S3; Amazon SNS ;Amazon SQS

Übersicht

Amazon Simple Storage Service (Amazon S3) Event Notifications veröffentlicht Benachrichtigungen für bestimmte Ereignisse in Ihrem S3-Bucket (z. B. objekterstellte Ereignisse, Ereignisse zum Entfernen von Objekten oder Wiederherstellen von Objektereignissen). Sie können eine AWS Lambda-Funktion verwenden, um diese Benachrichtigungen entsprechend den Anforderungen Ihrer Anwendung zu verarbeiten. Die Lambda-Funktion kann jedoch keine Benachrichtigungen von S3-Buckets direkt abonnieren, die in verschiedenen AWS-Regionen gehostet werden.

Der Ansatz dieses Musters stellt ein Fanout-Szenario bereit, um Amazon S3-Benachrichtigungen aus regionsübergreifenden S3-Buckets mithilfe eines Amazon Simple Notification Service (Amazon SNS)-Themas für jede Region zu verarbeiten. Diese regionalen SNS-Themen senden die Amazon S3-Ereignisbenachrichtigungen an eine Amazon Simple Queue Service (Amazon SQS)-Warteschlange in einer zentralen Region, die auch Ihre Lambda-Funktion enthält. Die Lambda-Funktion abonniert diese SQS-Warteschlange und verarbeitet die Ereignisbenachrichtigungen entsprechend den Anforderungen Ihrer Organisation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Bestehende S3-Buckets in mehreren Regionen, einschließlich einer zentralen Region zum Hosten der Amazon SQS-Warteschlange und der Lambda-Funktion.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI in der AWS CLI-Dokumentation.

- Vertrautheit mit dem Fanout-Szenario in Amazon SNS . Weitere Informationen dazu finden Sie unter Allgemeine Amazon SNS-Szenarien in der Amazon SNSDokumentation.

Architektur

Das folgende Diagramm zeigt die Architektur für den Ansatz dieses Musters.

Das Diagramm zeigt den folgenden Workflow:

1. Amazon S3 sendet Ereignisbenachrichtigungen über S3-Buckets (z. B. erstelltes Objekt, entferntes Objekt oder wiederhergestelltes Objekt) an ein SNS-Thema in derselben Region.
2. Das SNS-Thema veröffentlicht das Ereignis in einer SQS-Warteschlange in der zentralen Region.
3. Die SQS-Warteschlange ist als Ereignisquelle für Ihre Lambda-Funktion konfiguriert und puffert die Ereignismeldungen für die Lambda-Funktion.
4. Die Lambda-Funktion fragt die SQS-Warteschlange nach Nachrichten ab und verarbeitet die Amazon S3-Ereignisbenachrichtigungen gemäß den Anforderungen Ihrer Anwendung.

Technologie-Stack

- Lambda
- Amazon SNS
- Amazon SQS
- Amazon S3

Tools

- AWS CLI – Die AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS CLI-Befehle ausführen, die Funktionen implementieren, die denen entsprechen, die von der browserbasierten AWS-Managementkonsole über eine Eingabeaufforderung bereitgestellt werden.
- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während

ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.

- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.
- Amazon SQS – Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können. Amazon SQS unterstützt sowohl Standard- als auch FIFO-Warteschlangen.

Polen

Erstellen der SQS-Warteschlange und der Lambda-Funktion in Ihrer zentralen Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine SQS-Warteschlange mit einem Lambda-Auslöser.	Melden Sie sich bei der AWS-Managementkonsole an und verwenden Sie die Anweisungen aus dem Tutorial Using Lambda with Amazon SQS in der AWS Lambda-Dokumentation, um die folgenden Ressourcen in Ihrer zentralen Region zu erstellen: • Eine Lambda-Ausführungsrolle	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Eine Lambda-Funktion zur Verarbeitung der Amazon S3-Ereignisse • Eine SQS-Warteschlange Hinweis: Stellen Sie sicher, dass Sie die SQS-Warte schlange als Ereignisquelle für Ihre Lambda-Funktion konfigurieren.	

Erstellen Sie ein SNS-Thema und richten Sie Ereignisbenachrichtigungen für die S3-Buckets in jeder erforderlichen Region ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema , um Amazon S3-Ereign isbenachrichtigungen zu erhalten.	Erstellen Sie ein SNS-Thema in einer Region, aus der Sie Amazon S3-Ereignisbenachr ichtigungen erhalten möchten. Weitere Informationen dazu finden Sie unter Erstellen eines SNS-Themas in der Amazon SNS-Dokumentation. Wichtig: Stellen Sie sicher, dass Sie den Amazon-Re ssourcennamen (ARN) Ihres SNS-Themas aufzeichnen.	AWS DevOps, Cloud-Architekt
Abonnieren Sie das SNS-Thema für die zentrale SQS-Warteschlange.	Abonnieren Sie Ihr SNS-Thema für die SQS-Warte schlange, die von Ihrer zentralen Region gehostet	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird. Weitere Informationen dazu finden Sie unter Abonnieren eines SNS-Themas in der Amazon SNS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Zugriffsr ichtlinie des SNS-Themas.	1. Öffnen Sie die Amazon SNS-Konsole, wählen Sie Themen und dann das SNS-Thema aus, das Sie zuvor erstellt haben. 2. Wählen Sie Bearbeiten und erweitern Sie dann den Abschnitt Zugriffsrichtlinie – optional. 3. Fügen Sie Ihrem SNS-Thema die folgende Zugriffsrichtlinie hinzu, um die `sns:publish` Berechtigung für Amazon S3 zu erteilen, und wählen Sie dann Speichern aus: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "0", "Effect": "Allow", "Principal": { "Service": "s3.amazonaws.com" }, "Action": "sns:Publish", "Resource": "arn:aws:sns:us-west-2::s3Events-SNSTopic-us-west-2" } ]`	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>}</pre>	
Richten Sie Benachric htigungen für jeden S3-Bucket in der Region ein.	Richten Sie Ereignisb enachrichtigungen für jeden S3-Bucket in der Region ein. Weitere Informationen dazu finden Sie unter Aktivieren und Konfigurieren von Ereignisb enachrichtigungen mit der Amazon S3-Konsole in der Amazon S3Dokumentation. Hinweis: Wählen Sie im Abschnitt Ziel die Option SNS-Thema aus und geben Sie den ARN des SNS-Themas an, das Sie zuvor erstellt haben.	AWS DevOps, Cloud-Architekt
Wiederholen Sie dieses Epic für alle erforderlichen Regionen.	Wichtig: Wiederholen Sie die Aufgaben in diesem Epi für jede Region, aus der Sie Amazon S3-Ereignisbenachr ichtigungen erhalten möchten, einschließlich Ihrer zentralen Region.	AWS DevOps, Cloud-Architekt

Zugehörige Ressourcen

- Konfigurieren einer Zugriffsrichtlinie (Amazon SQS-Dokumentation)
- Konfigurieren einer SQS-Warteschlange als Ereignisquelle (AWS Lambda-Dokumentation)
- Konfigurieren einer SQS-Warteschlange zum Initiieren einer Lambda-Funktion (Amazon SQS-Dokumentation)
- -AWS::Lambda::Function Ressource (AWS- CloudFormation Dokumentation)

Drei AWS Glue ETL-Auftragstypen für die Konvertierung von Daten in Apache Parquet

Erstellt von Adnan Alvee (AWS), Karthikeyan Ramachandran und Nith Govindasivan (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik	Arbeitslast: Alle anderen Workloads
AWS-Services: AWS Glue		

Übersicht

In der Amazon Web Services (AWS) Cloud ist AWS Glue ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Mit AWS Glue können Sie Ihre Daten kostengünstig kategorisieren, bereinigen, anreichern und zuverlässig zwischen verschiedenen Datenspeichern und Datenströmen verschieben.

Dieses Muster bietet verschiedene Auftragstypen in AWS Glue und verwendet drei verschiedene Skripts, um die Erstellung von ETL-Jobs zu demonstrieren.

Sie können AWS Glue verwenden, um ETL-Jobs in einer Python-Shell-Umgebung zu schreiben. Sie können auch Batch- und Streaming-ETL-Jobs mithilfe von Python (PySpark) oder Scala in einer verwalteten Apache Spark-Umgebung erstellen. Um Ihnen den Einstieg in die Erstellung von ETL-Jobs zu erleichtern, konzentriert sich dieses Muster auf Batch-ETL-Jobs mit Python-Shell und Scala. PySpark Python-Shell-Jobs sind für Workloads gedacht, die weniger Rechenleistung benötigen. Die verwaltete Apache Spark-Umgebung ist für Workloads gedacht, die eine hohe Rechenleistung erfordern.

Apache Parquet wurde entwickelt, um effiziente Komprimierungs- und Kodierungsschemata zu unterstützen. Es kann Ihre Analytics-Workloads beschleunigen, da es Daten spaltenweise speichert. Durch die Konvertierung von Daten in Parquet können Sie auf längere Sicht Speicherplatz, Kosten und Zeit sparen. Weitere Informationen zu Parquet finden Sie im Blogbeitrag Apache Parquet: How to be a hero with the open-source columnar data format.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Rolle AWS Identity and Access Management (IAM) (Wenn Sie noch keine Rolle haben, lesen Sie den Abschnitt Zusätzliche Informationen.)

Architektur

Zieltechnologie-Stack

- AWS Glue
- Amazon-Simple-Storage-Service (Amazon-S3)
- Apache Parquet

Automatisierung und Skalierung

- AWS Glue Glue-Workflows unterstützen die vollständige Automatisierung einer ETL-Pipeline.
- Sie können die Anzahl der Datenverarbeitungseinheiten (DPUs) oder Workertypen ändern, um sie horizontal und vertikal zu skalieren.

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Glue ist ein vollständig verwalteter ETL-Service zum Kategorisieren, Bereinigen, Anreichern und Verschieben Ihrer Daten zwischen verschiedenen Datenspeichern und Datenströmen.

Andere Tools

- Apache Parquet ist ein spaltenorientiertes Open-Source-Datendateiformat, das zum Speichern und Abrufen entwickelt wurde.

Konfiguration

Verwenden Sie die folgenden Einstellungen für die Konfiguration der Rechenleistung von AWS Glue ETL. Um die Kosten zu senken, sollten Sie die minimalen Einstellungen verwenden, wenn Sie den Workload ausführen, der in diesem Muster bereitgestellt wird.

- Python-Shell — Sie können 1 DPU verwenden, um 16 GB Speicher zu nutzen, oder 0,0625 DPU, um 1 GB Speicher zu nutzen. Dieses Muster verwendet 0,0625 DPU, was die Standardeinstellung in der AWS Glue Glue-Konsole ist.
- Python oder Scala für Spark — Wenn Sie die Spark-bezogenen Jobtypen in der Konsole auswählen, verwendet AWS Glue standardmäßig 10 Worker und den G.1X-Workertyp. Bei diesem Muster werden zwei Worker verwendet, was der zulässigen Mindestanzahl entspricht. Der Standard-Worker-Typ ist ausreichend und kostengünstig.

In der folgenden Tabelle sind die verschiedenen AWS Glue Glue-Worker-Typen für die Apache Spark-Umgebung aufgeführt. Da ein Python-Shell-Job die Apache Spark-Umgebung nicht zum Ausführen von Python verwendet, ist er nicht in der Tabelle enthalten.

	Standard	G.1X	G.2X
vCPU	4	4	8
Arbeitsspeicher	16 GB	16 GB	32 GB
Festplattenkapazität	50 GB	64 GB	128 GB
Testamentsvollstrecker pro Arbeiter	2	1	1

Code

Den Code, der in diesem Muster verwendet wird, einschließlich der IAM-Rolle und der Parameterkonfiguration, finden Sie im Abschnitt Zusätzliche Informationen.

Epen

Laden Sie die Daten hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Daten in einen neuen oder vorhandenen S3-Bucket hoch.	Erstellen oder verwenden Sie einen vorhandenen S3-Bucket in Ihrem Konto. Laden Sie die	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei sample_data.csv aus dem Bereich Anlagen hoch und notieren Sie sich den S3-Bucket und den Speicherort des Präfixes.	

Den AWS Glue Glue-Job erstellen und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS Glue Glue-Job.	Fügen Sie im ETL-Bereich der AWS Glue Glue-Kons ole einen AWS Glue Glue-Job hinzu. Wählen Sie den entsprechenden Jobtyp, die AWS Glue Glue-Version und den entsprechenden DPU-/ Worker-Typ und die Anzahl der Worker aus. Einzelhei ten finden Sie im Abschnitt Konfiguration.	Entwickler, Cloud oder Daten
Ändern Sie die Eingabe- und Ausgabeorte.	Kopieren Sie den Code, der Ihrem AWS Glue Glue-Job entspricht, und ändern Sie den Eingabe- und Ausgabeor t, den Sie im Abschnitt Daten hochladen notiert haben.	Entwickler, Cloud oder Daten
Konfigurieren Sie die Parameter.	Sie können die im Abschnitt Zusätzliche Informationen bereitgestellten Codefragm ente verwenden, um Parameter für Ihren ETL-Job festzulegen. AWS	Entwickler, Cloud oder Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Glue verwendet intern vier Argumentnamen: • `--conf` • `--debug` • `--mode` • `--JOB_NAME` Der `--JOB_NAME` Parameter muss explizit in der AWS Glue Glue-Konsole eingegeben werden. Wählen Sie Jobs, Job bearbeiten, Sicherheitskonfiguration, Skriptbibliotheken und Jobparameter (optional). Geben Sie `--JOB_NAME` den Schlüssel ein und geben Sie einen Wert ein. Sie können diesen Parameter auch über die AWS-Befehlszeilenschnittstelle (AWS CLI) oder die AWS Glue Glue-API festlegen. Der `--JOB_NAME` Parameter wird von Spark verwendet und wird in einem Python-Shell-Umgebungsjob nicht benötigt. Sie müssen `--` vor jedem Parameter einen Namen hinzufügen, sonst funktioniert der Code nicht. Für die Codefragmente müssen die Standortparameter beispiels	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	weise mit und aufgerufen werden. `--input_loc --output_loc`	
Führen Sie den ETL-Job aus.	Führen Sie Ihren Job aus und überprüfen Sie die Ausgabe. Beachten Sie, wie viel Speicherplatz gegenüber der Originaldatei reduziert wurde.	Entwickler, Cloud oder Daten

Zugehörige Ressourcen

Referenzen

- Apache Spark
- AWS Glue: So funktioniert's
- Preise für AWS Glue

Tutorials und Videos

- Was ist AWS Glue?

Zusätzliche Informationen

IAM role (IAM-Rolle)

Wenn Sie die AWS Glue Glue-Jobs erstellen, können Sie entweder eine vorhandene IAM-Rolle mit den im folgenden Codeausschnitt angegebenen Berechtigungen oder eine neue Rolle verwenden.

Verwenden Sie den folgenden YAML-Code, um eine neue Rolle zu erstellen.

```
# (c) 2022 Amazon Web Services, Inc. or its affiliates. All Rights Reserved. This AWS
 Content is provided subject to the terms of the AWS Customer
# Agreement available at https://aws.amazon.com/agreement/ or other written agreement
 between Customer and Amazon Web Services, Inc.
```

```
AWSTemplateFormatVersion: "2010-09-09"

Description: This template will setup IAM role for AWS Glue service.

Resources:
  rGlueRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "glue.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole
      Policies:
        - PolicyName: !Sub "${AWS::StackName}-s3-limited-read-write-inline-policy"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - "s3:PutObject"
                  - "s3:GetObject"
                Resource: "arn:aws:s3:::*/*"
      Tags:
        - Key  : "Name"
          Value : !Sub "${AWS::StackName}"

Outputs:
  oGlueRoleName:
    Description: AWS Glue IAM role
    Value:
      Ref: rGlueRole
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", rGlueRole ] ]
```

AWS Glue Python-Shell

Der Python-Code verwendet die Pandas und PyArrow Bibliotheken, um Daten in Parquet zu konvertieren. Die Pandas-Bibliothek ist bereits verfügbar. Die PyArrow Bibliothek wird heruntergeladen, wenn Sie das Pattern ausführen, da es sich um eine einmalige Ausführung handelt. Sie können Raddateien verwenden, um sie in eine Bibliothek PyArrow zu konvertieren und die Datei als Bibliothekspaket bereitzustellen. Weitere Informationen zum Verpacken von Raddateien finden Sie unter Bereitstellen einer eigenen Python-Bibliothek.

Python-Shell-Parameter von AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["input_loc", "output_loc"])
```

Python-Shellcode von AWS Glue

```
from io import BytesIO
import pandas as pd
import boto3
import os
import io
import site
from importlib import reload
from setuptools.command import easy_install
install_path = os.environ['GLUE_INSTALLATION']
easy_install.main( ["--install-dir", install_path, "pyarrow"] )
reload(site)
import pyarrow


input_loc = "bucket-name/prefix/sample_data.csv"
output_loc = "bucket-name/prefix/"


input_bucket = input_loc.split('/', 1)[0]
object_key = input_loc.split('/', 1)[1]


output_loc_bucket = output_loc.split('/', 1)[0]
output_loc_prefix = output_loc.split('/', 1)[1]


s3 = boto3.client('s3')
```

```
obj = s3.get_object(Bucket=input_bucket, Key=object_key)
df = pd.read_csv(io.BytesIO(obj['Body'].read()))


parquet_buffer = BytesIO()
s3_resource = boto3.resource('s3')
df.to_parquet(parquet_buffer, index=False)
s3_resource.Object(output_loc_bucket, output_loc_prefix +  'data' +
 '.parquet').put(Body=parquet_buffer.getvalue())
```

AWS Glue Spark-Auftrag mit Python

Um einen AWS Glue Spark-Auftragstyp mit Python zu verwenden, wählen Sie Spark als Auftragstyp. Wählen Sie Spark 3.1, Python 3 mit verbesserter Jobstartzeit (Glue Version 3.0) als AWS Glue Glue-Version.

Python-Parameter von AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["JOB_NAME", "input_loc", "output_loc"])
```

AWS Glue Spark-Job mit Python-Code

```
import sys
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.transforms import *
from awsglue.dynamicframe import DynamicFrame
from awsglue.utils import getResolvedOptions
from awsglue.job import Job


sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)

input_loc = "bucket-name/prefix/sample_data.csv"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(\
```

```
    connection_type = "s3", \
    connection_options = {
        "paths": [input_loc]}, \
    format = "csv",
    format_options={
        "withHeader": True,
        "separator": ","
    })


outputDF = glueContext.write_dynamic_frame.from_options(\
    frame = inputDyf, \
    connection_type = "s3", \
    connection_options = {"path": output_loc \
        }, format = "parquet")
```

Verwenden Sie für eine große Anzahl komprimierter großer Dateien (z. B. 1.000 Dateien mit einer Größe von jeweils etwa 3 MB) den `compressionType` Parameter mit dem `recurse` Parameter, um alle Dateien zu lesen, die innerhalb des Präfixes verfügbar sind, wie im folgenden Code gezeigt.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Verwenden Sie für eine große Anzahl komprimierter kleiner Dateien (z. B. 1.000 Dateien mit jeweils etwa 133 KB) den `groupFiles` Parameter zusammen mit den `recurse` Parametern `compressionType` und. Der `groupFiles` Parameter gruppiert kleine Dateien in mehrere große Dateien, und der `groupSize` Parameter steuert die Gruppierung auf die angegebene Größe in Byte (z. B. 1 MB). Der folgende Codeausschnitt bietet ein Beispiel für die Verwendung dieser Parameter im Code.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"
```

```
inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                           "groupFiles" :"inPartition",
 "groupSize" :"1048576",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Ohne Änderung der Worker-Knoten ermöglichen diese Einstellungen dem AWS Glue Glue-Job, mehrere Dateien (groß oder klein, mit oder ohne Komprimierung) zu lesen und sie im Parquet-Format auf das Ziel zu schreiben.

AWS Glue Spark-Auftrag mit Scala

Um einen AWS Glue Spark-Auftragstyp mit Scala zu verwenden, wählen Sie Spark als Auftragstyp und Sprache als Scala. Wählen Sie Spark 3.1, Scala 2 mit verbesserter Jobstartzeit (Glue Version 3.0) als AWS Glue Glue-Version. Um Speicherplatz zu sparen, verwendet das folgende Beispiel für AWS Glue mit Scala die `applyMapping` Funktion auch zum Konvertieren von Datentypen.

AWS Glue Scala-Parameter

```
import com.amazonaws.services.glue.util.GlueArgParser val args =
 GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME", "inputLoc",
 "outputLoc").toArray)
```

AWS Glue Spark-Job mit Scala-Code

```
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.DynamicFrame
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._
```

```
object GlueScalaApp {
  def main(sysArgs: Array[String]) {

    @transient val spark: SparkContext = SparkContext.getOrCreate()
    val glueContext: GlueContext = new GlueContext(spark)

    val inputLoc = "s3://bucket-name/prefix/sample_data.csv"
    val outputLoc = "s3://bucket-name/prefix/"

    val readCSV = glueContext.getSource("csv", JsonOptions(Map("paths" ->
 Set(inputLoc)))).getDynamicFrame()

    val applyMapping = readCSV.applyMapping(mappings = Seq(("_c0", "string", "date",
 "string"), ("_c1", "string", "sales", "long"),
    ("_c2", "string", "profit", "double")), caseSensitive = false)

    val formatPartition = applyMapping.toDF().coalesce(1)

    val dynamicFrame = DynamicFrame(formatPartition, glueContext)

    val dataSink = glueContext.getSinkWithFormat(
        connectionType = "s3",
        options = JsonOptions(Map("path" -> outputLoc )),
        transformationContext = "dataSink", format =
 "parquet").writeDynamicFrame(dynamicFrame)
  }
}
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Visualisieren von Amazon-Redshift-Prüfungsprotokollen mit Amazon Athena und Amazon QuickSight

Erstellt von Sanketsikar (AWS) und Gopal Krishna Bhatia (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Analytik; Big Data; Data Lakes	AWS-Services: Amazon Athena; Amazon Redshift; Amazon S3; Amazon QuickSight

Übersicht

Sicherheit ist ein integraler Bestandteil von Datenbankoperationen in der Amazon Web Services (AWS) Cloud. Ihre Organisation sollte sicherstellen, dass sie die Aktivitäten und Verbindungen von Datenbankbenutzern überwacht, um potenzielle Sicherheitsvorfälle und Risiken zu erkennen. Dieses Muster hilft Ihnen dabei, Ihre Datenbanken zu Sicherheits- und Fehlerbehebungszwecken zu überwachen. Dabei handelt es sich um einen Prozess, der als Datenbanküberwachung bezeichnet wird.

Dieses Muster bietet ein SQL-Skript, das die Erstellung einer Amazon Athena-Tabelle und -Ansichten für ein Berichts-Dashboard in Amazon automatisiert QuickSight , mit dem Sie Amazon-Redshift-Protokolle überprüfen können. Dadurch wird sichergestellt, dass Benutzer, die für die Überwachung von Datenbankaktivitäten verantwortlich sind, bequem auf Datensicherheitsfunktionen zugreifen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon-Redshift-Cluster. Weitere Informationen dazu finden Sie unter Erstellen eines Amazon-Redshift-Clusters in der Amazon-Redshift-Dokumentation.
- Zugriff auf eine vorhandene Athena-Arbeitsgruppe. Weitere Informationen finden Sie unter Funktionsweise von Arbeitsgruppen in der Amazon Athena-Dokumentation.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3)-Quell-Bucket mit den erforderlichen AWS Identity and Access Management (IAM)-Berechtigungen. Weitere

Informationen finden Sie unter Bucket-Berechtigungen für die Amazon-Redshift-Prüfungsprotokollierung aus der Datenbank-Prüfungsprotokollierung in der Amazon-Redshift-Dokumentation.

Architektur

Technologie-Stack

- Athena
- Amazon Redshift
- Amazon S3
- QuickSight

Tools

- Amazon Athena – Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mit Standard-SQL erleichtert.
- Amazon QuickSight – QuickSight ist ein skalierbarer, Serverless-, einbettbarer und Machine Learning-gestützter Business Intelligence (BI)-Service.
- Amazon Redshift – Amazon Redshift ist ein vollständig verwalteter Data-Warehousing-Service auf Unternehmensebene im Petabyte-Bereich.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.

Polen

Konfigurieren des Amazon-Redshift-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Prüfungsprotokollierung für den Amazon-Redshift-Cluster.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Redshift-Konsole, wählen	DBA, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie CLUSTERS und dann den Cluster aus, für den Sie die Protokollierung aktiviere n möchten. 2. Wählen Sie die Registerk arte Eigenschaften und aktivieren Sie dann die Prüfung, indem Sie den Anweisungen unter Konfiguration der Prüfung mithilfe der Konsole in der Amazon-Redshift-Do kumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Protokollierung in der Amazon-Redshift-Cluster-Parametergruppe.	Sie können die gleichzeitige Prüfung von Verbindungsprotokollen, Benutzerprotokollen und Benutzeraktivitätsprotokollen aktivieren, indem Sie die AWS-Managementkonsole, die Amazon Redshift-API-Referenz oder die AWS Command Line Interface (AWS CLI) verwenden. Für die Prüfung von Benutzeraktivitätsprotokollen müssen Sie den `enable_user_activity_logging` Datenbankparameter aktivieren. Wenn Sie nur die Prüfungsprotokollierungsfunktion aktivieren, aber nicht den zugehörigen Parameter, protokolliert die Datenbankprüfung die Protokollierungsinformationen für die Verbindungs- und Benutzerprotokolle, aber nicht für die Benutzeraktivitätsprotokolle. Der `enable_user_activity_logging` Parameter ist standardmäßig nicht aktiviert, aber Sie können ihn aktivieren, indem Sie ihn von `false` in ändern`true`.	DBA, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Sie müssen eine neue Cluster-Parameterg ruppe mit aktiviertem `user_activity_logg ing` Parameter erstellen und sie an Ihren Amazon-Redshift-Cluster anhängen. Weitere Informationen dazu finden Sie unter Ändern eines Clusters in der Amazon-Redshift-Do kumentation. Weitere Informationen zu dieser Aufgabe finden Sie unter Amazon-Redshift-Pa rametergruppen und Konfiguri eren der Prüfung mithilfe der Konsole in der Amazon-Re dshift-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie S3-Bucket -Berechtigungen für die Amazon-Redshift-Clusterprotokollierung.	Wenn Sie die Protokollierung aktivieren, sammelt Amazon Redshift Protokollinformationen und lädt sie in Protokolldateien hoch, die in einem S3-Bucket gespeichert sind. Sie können einen vorhandenen S3-Bucket verwenden oder einen neuen Bucket erstellen. Wichtig: Stellen Sie sicher, dass Amazon Redshift über die erforderlichen IAM-Berechtigungen für den Zugriff auf den S3-Bucket verfügt. Weitere Informationen dazu finden Sie unter Bucket-Berechtigungen für die Amazon-Redshift-Prüfungsprotokollierung aus der Datenbank-Prüfungsprotokollierung in der Amazon-Redshift-Dokumentation.	DBA, Dateningenieur

Erstellen der Athena-Tabelle und -Ansichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Athena-Tabelle und Ansichten, um Amazon-Redshift-Prüfungsprotokolldaten aus dem S3-Bucket abzufragen.	Öffnen Sie die Amazon Athena-Konsole und verwenden Sie die DDL-Abfrage (Data Definition Language) aus dem SQL`AuditLogging.sql` -Skript (angefügt),	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um die Tabelle und Ansichten für Benutzeraktivitätsprotokolle, Benutzerprotokolle und Verbindungsprotokolle zu erstellen. Weitere Informationen und Anweisungen finden Sie im Tutorial Tabellen erstellen und Abfragen ausführen aus dem Amazon Athena-Workshop.	

Einrichten der Protokollüberwachung im QuickSight Dashboard

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein QuickSight Dashboard mit Athena als Datenquelle.	Öffnen Sie die Amazon-QuickSight Konsole und erstellen Sie ein QuickSight Dashboard, indem Sie den Anweisungen im Tutorial Visualisieren mit QuickSight mithilfe von Athena aus dem Amazon Athena-Workshop folgen.	DBA, Dateningenieur

Zugehörige Ressourcen

- Erstellen von Tabellen und Ausführen von Abfragen in Athena
- Visualisieren mit QuickSight mithilfe von Athena

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Visualisieren von IAM-Anmeldeinformationsberichten für alle AWS-Konten mit Amazon QuickSight

Erstellt von Parag Nagwekar (AWS) und Arun Chpillai (AWS)

Code-Repository: Organisationsweite Sichtbarkeit Ihrer IAM-Anmeldeinformationsberichte	Umgebung: Produktion	Technologien: Analytik; Advisory; Management & Governance; Sicherheit, Identität, Compliance
Workload: Alle anderen Workloads	AWS-Services: Amazon Athena; AWS CloudFormation; Amazon EventBridge; AWS Identity and Access Management; Amazon QuickSight	

Übersicht

> Warnung: IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, dass Sie diesen Benutzern nur die Berechtigungen gewähren, die sie zur Ausführung der Aufgabe benötigen, und dass Sie diese Benutzer entfernen, wenn sie nicht mehr benötigt werden.

Sie können AWS Identity and Access Management (IAM)-Anmeldeinformationsberichte verwenden, um die Sicherheits-, Prüfungs- und Compliance-Anforderungen Ihrer Organisation zu erfüllen. Berichte zu Anmeldeinformationen enthalten eine Liste aller Benutzer in Ihren AWS-Konten und zeigen den Status ihrer Anmeldeinformationen an, z. B. Passwörter, Zugriffsschlüssel und Geräte für die Multi-Faktor-Authentifizierung (MFA). Sie können Berichte zu Anmeldeinformationen für mehrere AWS-Konten verwenden, die von AWS Organizations verwaltet werden.

Dieses Muster enthält Schritte und Code, mit dem Sie mithilfe von Amazon- QuickSight Dashboards IAM-Anmeldeinformationsberichte für alle AWS-Konten in Ihrer Organisation erstellen und freigeben

können. Sie können die Dashboards mit Stakeholdern in Ihrer Organisation teilen. Die Berichte können Ihrer Organisation helfen, die folgenden angestrebten Geschäftsergebnisse zu erzielen:

- Identifizieren von Sicherheitsvorfällen im Zusammenhang mit IAM-Benutzern
- Nachverfolgen der Echtzeitmigration von IAM-Benutzern zur Single Sign-On (SSO)-Authentifizierung
- Verfolgen Sie AWS-Regionen, auf die IAM-Benutzer zugreifen
- Konformität bleiben
- Informationen mit anderen Stakeholdern teilen

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Organisation mit Mitgliedskonten
- Eine IAM-Rolle mit Berechtigungen für den Zugriff auf Konten in Organizations
- AWS Command Line Interface (AWS CLI) Version 2, installiert und konfiguriert
- Ein Abonnement für Amazon QuickSight Enterprise Edition

Architektur

Technologie-Stack

- Amazon Athena
- Amazon EventBridge
- Amazon QuickSight
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Organizations

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur zum Einrichten eines Workflows, der IAM-Anmeldeinformationsberichtsdaten aus mehreren AWS-Konten erfasst.

1. EventBridge ruft täglich eine Lambda-Funktion auf.
2. Die Lambda-Funktion übernimmt in jedem AWS-Konto in der gesamten Organisation eine IAM-Rolle. Anschließend erstellt die Funktion den Bericht zu den IAM-Anmeldeinformationen und speichert die Berichtsdaten in einem zentralen S3-Bucket. Sie müssen die Verschlüsselung aktivieren und den öffentlichen Zugriff auf dem S3-Bucket deaktivieren.
3. Ein AWS Glue-Crawler crawlt den S3-Bucket täglich und aktualisiert die Athena-Tabelle entsprechend.
4. QuickSight importiert und analysiert die Daten aus dem Bericht zu Anmeldeinformationen und erstellt ein Dashboard, das von den Stakeholdern visualisiert und mit ihnen geteilt werden kann.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mithilfe von Standard-SQL vereinfacht.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufrufendpunkte mit API-Zielen oder Event Buses in anderen AWS-Konten.
- Amazon QuickSight ist ein Cloud-Scale Business Intelligence (BI)-Service, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

Code

Der Code für dieses Muster ist im GitHub getiamcredsreport-allaccounts-orgRepository verfügbar. Sie können den Code aus diesem Repository verwenden, um Berichte zu IAM-Anmeldeinformationen über AWS-Konten in Organizations hinweg zu erstellen und sie an einem zentralen Ort zu speichern.

Polen

Einrichten der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Amazon QuickSight Enterprise Edition ein.	1. Aktivieren Sie die Amazon QuickSight Enterprise Edition in Ihrem AWS-Konto . Weitere Informationen finden Sie unter Verwalten des Benutzerzugriffs in Amazon QuickSight in der -QuickSight Dokumentation. 2. Um Dashboard-Berechti gungen zu erteilen, rufen Sie den Amazon-Re ssourcennamen (ARN) der QuickSight Benutzer ab.	AWS-Administrator, AWS DevOps, Cloud-Administrator, Cloud-Architekt
Integrieren Sie Amazon QuickSight mit Amazon S3 und Athena.	Sie müssen autorisie renQuickSight , Amazon S3 und Athena zu verwenden , bevor Sie den AWS-CloudFormation Stack bereitstellen.	AWS-Administrator, AWS DevOps, Cloud-Administrator, Cloud-Architekt

Bereitstellen der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	1. Klonen Sie das GitHub getiamcredsreport-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	allaccounts-org Repository auf Ihren lokalen Computer, indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samples/getiamcredsreport-allaccounts-org`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Infrastruktur bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Wählen Sie im Navigationsbereich Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 4. Wählen Sie auf der Seite Vorlage angeben für Vorlagenquelle die Option Vorlagendatei hochladen aus. 5. Wählen Sie Datei auswählen, wählen Sie die `Cloudformation-createcredrepo.yaml` Datei aus Ihrem geklonten GitHub Repository aus und klicken Sie dann auf Weiter. 6. Aktualisieren Sie unter Parameter `IAMRoleName` mit Ihrer IAM-Rolle. Dies sollte die IAM-Rolle sein, die Lambda in jedem Konto der Organisation übernehmen soll. Diese Rolle erstellt den Bericht zu den Anmeldeinformationen. Hinweis: Die Rolle muss in	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	diesem Schritt der Stack-Erstellung nicht in allen Konten vorhanden sein. 7. Aktualisieren Sie unter Parameter `S3BucketName` mit dem Namen des S3-Buckets, in dem Lambda die Anmeldeinformationen für alle Konten speichern kann. 8. Geben Sie für Stack-Name Ihren Stack-Namen ein. 9. Wählen Sie Absenden aus. 10. Notieren Sie sich den Rollennamen der Lambda-Funktion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Berechtigungsrichtlinie.	Erstellen Sie eine IAM-Richtlinie für jedes AWS-Konto in Ihrer gesamten Organisation mit den folgenden Berechtigungen: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:GenerateCredentialReport", "iam:GetCredentialReport" ], "Resource": "*" } ] }`	AWS DevOps, Cloud-Administrator, Cloud-Architekt, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle mit einer Vertrauensrichtlinie.	1. Erstellen Sie eine IAM-Rolle für die AWS-Konten und fügen Sie die Berechtigungsrichtlinie an, die Sie im vorherigen Schritt erstellt haben. 2. Fügen Sie der IAM-Rolle die folgende Vertrauensrichtlinie hinzu: `{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Principal":{ "AWS":[ "arn:aws:iam::<MasterAccountID>:role/<LambdaRole>" ] }, "Action": "sts:AssumeRole" } ] }` Wichtig: Ersetzen Sie durch `arn:aws:iam::<MasterAccountID>:role/<LambdaRole>` den ARN der Lambda-Rolle, die Sie zuvor notiert haben.	Cloud-Administrator, Cloud-Architekt, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Organisationen verwenden in der Regel Automatisierung, um IAM-Rollen für ihre AWS-Konten zu erstellen. Wir empfehlen Ihnen, diese Automatisierung zu verwenden, falls verfügbar . Alternativ können Sie das `CreateRoleforOrg.py` Skript aus dem Code-Repo sitory verwenden. Das Skript erfordert eine vorhandene Administratorrolle oder eine andere IAM-Rolle, die über die Berechtigung zum Erstellen einer IAM-Richtlinie und -Rolle in jedem AWS-Konto verfügt.	
Konfigurieren Sie Amazon QuickSight so, dass die Daten visualisiert werden.	1. Melden Sie sich bei QuickSight mit Ihren -Anmeldeinformationen an. 2. Erstellen Sie einen Datensatz mithilfe von Athena (mit der `iamcredreportdb` Datenbank und `“cfn_iamcredreport”` Tabelle) und aktualisieren Sie dann den Datensatz automatisch. 3. Erstellen Sie eine Analyse in QuickSight. 4. Erstellen Sie ein QuickSight Dashboard .	AWS DevOps, Cloud-Administrator, Cloud-Architekt, Dateningenieur

Zusätzliche Informationen

Zusätzliche Überlegungen

Berücksichtigen Sie dabei Folgendes:

- Nachdem Sie CloudFormation die Infrastruktur mit bereitgestellt haben, können Sie warten, bis die Berichte in Amazon S3 erstellt und von Athena analysiert wurden, bis Lambda und AWS Glue gemäß ihren Zeitplänen ausgeführt werden. Alternativ können Sie Lambda manuell ausführen, um die Berichte in Amazon S3 abzurufen, und dann den AWS Glue-Crawler ausführen, um die Athena-Tabelle abzurufen, die aus den Daten erstellt wird.
- QuickSight ist ein leistungsstarkes Tool zum Analysieren und Visualisieren von Daten basierend auf Ihren Geschäftsanforderungen. Sie können Parameter in verwenden QuickSight , um Widget-Daten basierend auf von Ihnen ausgewählten Datenfeldern zu steuern. Außerdem können Sie eine QuickSight Analyse verwenden, um Parameter (z. B. Konto-, Datums- und Benutzerfelder wie `partition_0`, `user` bzw.) aus Ihrem Datensatz zu erstellen `partition_1`und Steuerelemente für die Parameter für Konto, Datum und Benutzer hinzuzufügen.
- Informationen zum Erstellen Ihrer eigenen QuickSight Dashboards finden Sie unter QuickSight Workshops auf der AWS Workshop Studio-Website.
- Beispiele für QuickSight Dashboards finden Sie im GitHub getiamcredsreport-allaccounts-org Code-Repository.

Gezielte Geschäftsergebnisse

Sie können dieses Muster verwenden, um die folgenden angestrebten Geschäftsergebnisse zu erzielen:

- Identifizieren von Sicherheitsvorfällen im Zusammenhang mit IAM-Benutzern – Untersuchen Sie jeden Benutzer in jedem AWS-Konto in Ihrer Organisation mithilfe eines einzigen Glasfensters. Sie können den Trend der zuletzt aufgerufenen einzelnen AWS-Regionen und der von ihnen verwendeten Services eines IAM-Benutzers verfolgen.
- Verfolgen Sie die Echtzeitmigration von IAM-Benutzern zur SSO-Authentifizierung – Mit SSO können sich Benutzer einmal mit einer einzigen Anmeldeinformation anmelden und auf mehrere AWS-Konten und -Anwendungen zugreifen. Wenn Sie planen, Ihre IAM-Benutzer zu SSO zu migrieren, kann dieses Muster Ihnen helfen, zu SSO zu wechseln und die gesamte Verwendung von IAM-Benutzeranmeldeinformationen (z. B. den Zugriff auf die AWS-Managementkonsole oder die Verwendung von Zugriffsschlüsseln) über alle AWS-Konten hinweg zu verfolgen.

- Verfolgen Sie AWS-Regionen, auf die IAM-Benutzer zugreifen – Sie können den Zugriff von IAM-Benutzern auf Regionen für verschiedene Zwecke steuern, z. B. für Datenhoheit und Kostenkontrolle. Sie können auch die Verwendung von Regionen durch jeden IAM-Benutzer verfolgen.
- Konformität bleiben – Wenn Sie dem Prinzip der geringsten Berechtigung folgen, können Sie nur die spezifischen IAM-Berechtigungen erteilen, die für die Ausführung einer bestimmten Aufgabe erforderlich sind. Außerdem können Sie den Zugriff auf AWS-Services, die AWS-Managementkonsole und die Nutzung langfristiger Anmeldeinformationen verfolgen.
- Informationen mit anderen Stakeholdern teilen – Sie können kuratierte Dashboards mit anderen Stakeholdern teilen, ohne ihnen Zugriff auf Berichte zu IAM-Anmeldeinformationen oder AWS-Konten zu gewähren.

Mehr Muster

- ???
- Automatisches Extrahieren von Inhalten aus PDF-Dateien mit Amazon Textract
- Erstellen einer Datenpipeline zur Aufnahme, Transformation und Analyse von Google Analytics-Daten mit dem AWS DataOps Development Kit
- ???
- Kostengünstige Aufnahme von IoT-Daten direkt in Amazon S3 mit AWS IoT Greengrass
- Erstellen detaillierter Kosten- und Nutzungsberichte für Amazon EMR-Cluster mithilfe von AWS Cost Explorer
- Erstellen detaillierter Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora
- Erstellen detaillierter Kosten- und Nutzungsberichte für AWS Glue-Aufträge mithilfe von AWS Cost Explorer
- Kontoübergreifende Automatisierung der Datenfreigabe
- Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden
- Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein
- Sicherstellen, dass ein Amazon-Redshift-Cluster bei der Erstellung verschlüsselt wird
- Sicherstellen, dass die Verschlüsselung für Amazon-EMR-Daten im Ruhezustand beim Start aktiviert ist
- Extrahieren und Abfragen von AWS IoT SiteWise -Metadatenattributen in einem Data Lake
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Gewähren Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Identifizieren und warnen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS-Schlüssel verschlüsselt sind
- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas in der AWS-Cloud
- Migrieren einer Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle GoldenGate Flat File Adaptern
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift

- Migrieren von Daten aus einer lokalen Hadoop-Umgebung zu Amazon S3 mithilfe von DistCp mit AWS PrivateLink für Amazon S3
- ???
- Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS
- Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung
- Einrichten eines Grafana-Überwachungs-Dashboards für AWS ParallelCluster
- Stellen Sie sicher, dass neue Amazon-Redshift-Cluster über erforderliche SSL-Endpunkte verfügen
- Überprüfen, ob neue Amazon-Redshift-Cluster in einer VPC gestartet werden
- ???

Produktivität von Unternehmen

Themen

Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein

Umgebung: Produktion	Technologien: Unternehmensproduktivität; Infrastruktur; Web- und mobile Apps; Datenbanken	Arbeitslast: Oracle
AWS-Services: Amazon EC2 Auto Scaling; Amazon EFS; Elastic Load Balancing (ELB); Amazon RDS		

Übersicht

Wenn Sie Ihre PeopleSoft Workloads zu AWS migrieren, ist Resilienz ein wichtiges Ziel. Es stellt sicher, dass Ihre PeopleSoft Anwendung immer hochverfügbar ist und nach Ausfällen schnell wiederhergestellt werden kann.

Dieses Muster bietet eine Architektur für Ihre PeopleSoft Anwendungen auf AWS, um Hochverfügbarkeit (HA) auf Netzwerk-, Anwendungs- und Datenbankebene sicherzustellen. Es verwendet eine Amazon Relational Database Service (Amazon RDS) für Oracle- oder Amazon RDS for SQL Server Server-Datenbank für die Datenbankebene. Diese Architektur umfasst auch AWS-Services wie Amazon Route 53, Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instances, Amazon Elastic Block Storage (Amazon EBS), Amazon Elastic File System (Amazon EFS) und einen Application Load Balancer und ist skalierbar.

Oracle PeopleSoft bietet eine Reihe von Tools und Anwendungen für das Personalmanagement und andere Geschäftsabläufe.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine PeopleSoft Umgebung mit den erforderlichen Lizenzen für die Einrichtung auf AWS

- Eine in Ihrem AWS-Konto eingerichtete Virtual Private Cloud (VPC) mit den folgenden Ressourcen:
  - Mindestens zwei Availability Zones
  - Ein öffentliches Subnetz und drei private Subnetze in jeder Availability Zone
  - Ein NAT-Gateway und ein Internet-Gateway
  - Routing-Tabellen für jedes Subnetz zur Weiterleitung des Datenverkehrs
  - Netzwerkzugriffskontrolllisten (Netzwerk-ACLs) und Sicherheitsgruppen wurden so definiert, dass sie die Sicherheit der PeopleSoft Anwendung gemäß den Standards Ihres Unternehmens gewährleisten

Einschränkungen

- Dieses Muster bietet eine Hochverfügbarkeitslösung (HA). Es unterstützt keine Notfallwiederherstellungsszenarien (DR). In dem seltenen Fall, dass die gesamte AWS-Region für die HA-Implementierung ausfällt, ist die Anwendung nicht mehr verfügbar.

Produktversionen

- PeopleSoft Anwendungen, auf denen PeopleTools 8.52 und höher ausgeführt wird

Architektur

Zielarchitektur

Ausfallzeiten oder Ausfälle Ihrer PeopleSoft Produktionsanwendung wirken sich auf die Verfügbarkeit der Anwendung aus und führen zu erheblichen Störungen Ihres Geschäftsbetriebs.

Wir empfehlen Ihnen, Ihre PeopleSoft Produktionsanwendung so zu gestalten, dass sie stets hochverfügbar ist. Sie können dies erreichen, indem Sie einzelne Fehlerquellen eliminieren, zuverlässige Crossover- oder Failover-Points hinzufügen und Fehler erkennen. Das folgende Diagramm zeigt eine HA-Architektur für PeopleSoft auf AWS.

Diese Architekturbereitstellung verwendet Amazon RDS for Oracle als PeopleSoft Datenbank und EC2-Instances, die auf Red Hat Enterprise Linux (RHEL) ausgeführt werden. Sie können Amazon RDS for SQL Server auch als Peoplesoft-Datenbank verwenden.

Diese Architektur enthält die folgenden Komponenten:

- Amazon Route 53 wird als Domain Name Server (DNS) für die Weiterleitung von Anfragen aus dem Internet an die PeopleSoft Anwendung verwendet.
- AWS WAF schützt Sie vor gängigen Web-Exploits und Bots, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können. AWS Shield Advanced (nicht abgebildet) bietet einen viel umfassenderen Schutz.
- Ein Application Load Balancer verteilt den HTTP- und HTTPS-Verkehr mit erweitertem Anforderungsrouting, das auf die Webserver ausgerichtet ist.
- Die Webserver, Anwendungsserver, Process Scheduler-Server und Elasticsearch-Server, die die PeopleSoft Anwendung unterstützen, werden in mehreren Availability Zones ausgeführt und verwenden Amazon EC2 Auto Scaling.
- Die von der PeopleSoft Anwendung verwendete Datenbank läuft auf Amazon RDS in einer Multi-AZ-Konfiguration.
- Die von der PeopleSoft Anwendung verwendete Dateifreigabe ist in Amazon EFS konfiguriert und wird für den instanzübergreifenden Zugriff auf Dateien verwendet.
- Amazon Machine Images (AMIs) werden von Amazon EC2 Auto Scaling verwendet, um sicherzustellen, dass PeopleSoft Komponenten bei Bedarf schnell geklont werden.
- Die NAT-Gateways verbinden Instances in einem privaten Subnetz mit Diensten außerhalb Ihrer VPC und stellen sicher, dass externe Dienste keine Verbindung mit diesen Instances initiieren können.
- Das Internet-Gateway ist eine horizontal skalierte, redundante und hochverfügbare VPC-Komponente, die die Kommunikation zwischen Ihrer VPC und dem Internet ermöglicht.
- Die Bastion-Hosts im öffentlichen Subnetz ermöglichen den Zugriff auf die Server im privaten Subnetz über ein externes Netzwerk, z. B. das Internet oder ein lokales Netzwerk. Die Bastion-Hosts bieten kontrollierten und sicheren Zugriff auf die Server in den privaten Subnetzen.

Einzelheiten zur Architektur

Die PeopleSoft Datenbank befindet sich in einer Amazon RDS-Datenbank für Oracle (oder Amazon RDS for SQL Server) in einer Multi-AZ-Konfiguration. Die Amazon RDS Multi-AZ-Funktion repliziert Datenbankaktualisierungen in zwei Availability Zones, um die Haltbarkeit und Verfügbarkeit zu erhöhen. Amazon RDS führt bei geplanten Wartungsarbeiten und ungeplanten Störungen automatisch einen Failover zur Standby-Datenbank durch.

Das PeopleSoft Web und die Middle Tier sind auf EC2-Instances installiert. Diese Instances sind über mehrere Availability Zones verteilt und durch eine Auto Scaling Scaling-Gruppe verknüpft. Dadurch

wird sichergestellt, dass diese Komponenten immer hochverfügbar sind. Es wird eine Mindestanzahl erforderlicher Instanzen verwaltet, um sicherzustellen, dass die Anwendung immer verfügbar ist und bei Bedarf skaliert werden kann.

Wir empfehlen, dass Sie einen EC2-Instance-Typ der aktuellen Generation für die OEM EC2-Instances verwenden. Instance-Typen der aktuellen Generation, wie Instances, die auf dem AWS Nitro System basieren, unterstützen virtuelle Hardware-Maschinen (HVMs). Die HVM-AMIs sind erforderlich, um die Vorteile erweiterter Netzwerke nutzen zu können, und sie bieten auch mehr Sicherheit. Die EC2-Instances, die Teil jeder Auto Scaling Scaling-Gruppe sind, verwenden ihr eigenes AMI, wenn sie Instances ersetzen oder hochskalieren. Wir empfehlen, dass Sie die EC2-Instance-Typen auf der Grundlage der Last, die Ihre PeopleSoft Anwendung bewältigen soll, und der von Oracle empfohlenen Mindestwerte für Ihre PeopleSoft Anwendung und PeopleTools Version auswählen. Weitere Informationen zu den Hardware- und Softwareanforderungen finden Sie auf der Oracle-Support-Website.

PeopleSoft Web und Middle Tier teilen sich einen Amazon EFS-Mount, um Berichte, Datendateien und (falls erforderlich) das `PS_HOME` Verzeichnis gemeinsam zu nutzen. Amazon EFS ist aus Leistungs- und Kostengründen mit Mount-Zielen in jeder Availability Zone konfiguriert.

Ein Application Load Balancer wird bereitgestellt, um den Datenverkehr zu unterstützen, der auf die PeopleSoft Anwendung zugreift, und für den Lastenausgleich des Datenverkehrs zwischen den Webservern in verschiedenen Availability Zones. Ein Application Load Balancer ist ein Netzwerkgerät, das HA in mindestens zwei Availability Zones bereitstellt. Die Webserver verteilen den Datenverkehr mithilfe einer Lastenausgleichskonfiguration auf verschiedene Anwendungsserver. Der Lastenausgleich zwischen dem Webserver und dem Anwendungsserver stellt sicher, dass die Last gleichmäßig auf die Instanzen verteilt wird, und hilft, Engpässe und Serviceunterbrechungen aufgrund überlasteter Instanzen zu vermeiden.

Amazon Route 53 wird als DNS-Service verwendet, um den Datenverkehr aus dem Internet an den Application Load Balancer weiterzuleiten. Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

HA-Einzelheiten

- Datenbanken: Die Multi-AZ-Funktion von Amazon RDS betreibt zwei Datenbanken in mehreren Availability Zones mit synchroner Replikation. Dadurch entsteht eine hochverfügbare Umgebung mit automatischem Failover. Amazon RDS verfügt über eine Erkennung von Failover-Ereignissen und leitet ein automatisches Failover ein, wenn diese Ereignisse auftreten. Sie können auch ein manuelles Failover über die Amazon RDS-API einleiten. Eine ausführliche Erklärung finden

Sie im Blogbeitrag Amazon RDS Under The Hood: Multi-AZ. Der Failover ist nahtlos und die Anwendung stellt in diesem Fall automatisch wieder eine Verbindung zur Datenbank her. Alle Process Scheduler-Jobs während des Failovers erzeugen jedoch Fehler und müssen erneut eingereicht werden.

- PeopleSoft Anwendungsserver: Die Anwendungsserver sind auf mehrere Availability Zones verteilt und für sie wurde eine Auto Scaling Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Anwendungsservervorlage geklont wurde. Insbesondere ist Jolt-Pooling aktiviert. Wenn also eine Anwendungsserver-Instance ausfällt, werden die Sitzungen automatisch auf einen anderen Anwendungsserver umgeleitet, und die Auto Scaling Scaling-Gruppe startet automatisch eine weitere Instance, startet den Anwendungsserver und registriert ihn im Amazon EFS-Mount. Der neu erstellte Anwendungsserver wird mithilfe des `PSSTRSETUP.SH` Skripts auf den Webservern automatisch zu den Webservern hinzugefügt. Dadurch wird sichergestellt, dass der Anwendungsserver immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.
- Prozessplaner: Die Process Scheduler-Server sind auf mehrere Availability Zones verteilt und für sie wurde eine Auto Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Process Scheduler-Servervorlage geklont wurde. Insbesondere wenn eine Prozessplaner-Instanz ausfällt, startet die Auto Scaling Scaling-Gruppe automatisch eine weitere Instanz und startet den Prozessplaner. Alle Jobs, die ausgeführt wurden, als die Instanz ausfiel, müssen erneut eingereicht werden. Dadurch wird sichergestellt, dass der Prozessplaner immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.
- Elasticsearch-Server: Für die Elasticsearch-Server wurde eine Auto Scaling Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Elasticsearch-Servervorlage geklont wird. Insbesondere wenn eine Elasticsearch-Instance ausfällt, erkennt der Application Load Balancer, der Anfragen an sie sendet, den Fehler und sendet keinen Traffic mehr an sie. Die Auto Scaling Scaling-Gruppe startet automatisch eine weitere Instance und ruft die Elasticsearch-Instance auf. Wenn die Elasticsearch-Instance wieder verfügbar ist, erkennt der Application Load Balancer, dass sie fehlerfrei ist, und sendet erneut Anfragen an sie. Dadurch wird sichergestellt, dass der Elasticsearch-Server immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.
- Webserver: Für die Webserver ist eine Auto Scaling Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Webservervorlage geklont wurde. Insbesondere wenn eine Webserver-Instance ausfällt, erkennt der Application Load Balancer, der Anfragen an sie weiterleitet, den Fehler und beendet das Senden von Datenverkehr an sie. Die Auto Scaling Scaling-Gruppe startet

automatisch eine weitere Instance und ruft die Webserver-Instance auf. Wenn die Webserver-Instance wieder verfügbar ist, erkennt der Application Load Balancer, dass sie fehlerfrei ist, und sendet erneut Anfragen an sie. Dadurch wird sichergestellt, dass der Webserver immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.

Tools

AWS-Services

- Application Load Balancer verteilen den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. EC2-Instances, in mehreren Availability Zones.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Bewährte Methoden

Bewährte Methoden für den Betrieb

- Wenn Sie PeopleSoft auf AWS arbeiten, verwenden Sie Route 53, um den Datenverkehr aus dem Internet und lokal weiterzuleiten. Verwenden Sie die Failover-Option, um den Datenverkehr zur Disaster Recovery (DR) -Site umzuleiten, falls die primäre DB-Instance nicht verfügbar ist.
- Verwenden Sie immer einen Application Load Balancer vor der PeopleSoft Umgebung. Dadurch wird sichergestellt, dass der Datenverkehr auf sichere Weise auf die Webserver verteilt wird.
- Stellen Sie in den Zielgruppeneinstellungen des Application Load Balancer sicher, dass Stickiness mit einem vom Load Balancer generierten Cookie aktiviert ist.

Hinweis: Möglicherweise müssen Sie ein anwendungsbasiertes Cookie verwenden, wenn Sie externes Single Sign-On (SSO) verwenden. Dadurch wird sichergestellt, dass die Verbindungen zwischen den Webservern und Anwendungsservern konsistent sind.

- Für eine PeopleSoft Produktionsanwendung muss das Leerlauf-Timeout des Application Load Balancer mit den Einstellungen in dem von Ihnen verwendeten Webprofil übereinstimmen. Dadurch wird verhindert, dass Benutzersitzungen auf der Load Balancer-Ebene ablaufen.
- Legen Sie für eine PeopleSoft Produktionsanwendung den Wert für die Anzahl der Wiederverwendungsvorgänge auf dem Anwendungsserver auf einen Wert fest, der Speicherlecks minimiert.
- Wenn Sie eine Amazon RDS-Datenbank für Ihre PeopleSoft Produktionsanwendung verwenden, wie in diesem Muster beschrieben, führen Sie sie für hohe Verfügbarkeit im Multi-AZ-Format aus.
- Wenn Ihre Datenbank auf einer EC2-Instance für Ihre PeopleSoft Produktionsanwendung läuft, stellen Sie sicher, dass eine Standby-Datenbank in einer anderen Availability Zone läuft, um Hochverfügbarkeit zu gewährleisten.
- Stellen Sie für DR sicher, dass Ihre Amazon RDS-Datenbank oder EC2-Instance über einen Standby-Modus verfügt, der in einer von der Produktionsdatenbank getrennten AWS-Region konfiguriert ist. Dadurch wird sichergestellt, dass Sie im Falle eines Notfalls in der Region die Anwendung auf eine andere Region umstellen können.
- Verwenden Sie für DR Amazon Elastic Disaster Recovery, um Komponenten auf Anwendungsebene in einer von den Produktionskomponenten getrennten Region einzurichten. Dadurch wird sichergestellt, dass Sie bei einem Notfall in der Region die Anwendung auf eine andere Region umstellen können.
- Verwenden Sie Amazon EFS (für moderate I/O-Anforderungen) oder Amazon FSx (für hohe I/O-Anforderungen), um Ihre PeopleSoft Berichte, Anlagen und Datendateien zu speichern. Dadurch wird sichergestellt, dass der Inhalt an einem zentralen Ort gespeichert wird und von überall innerhalb der Infrastruktur abgerufen werden kann.
- Verwenden Sie Amazon CloudWatch (einfach und detailliert), um die AWS-Cloud-Ressourcen, die Ihre PeopleSoft Anwendung verwendet, nahezu in Echtzeit zu überwachen. Dadurch wird sichergestellt, dass Sie sofort über Probleme informiert werden und diese schnell beheben können, bevor sie die Verfügbarkeit der Umgebung beeinträchtigen.
- Wenn Sie eine Amazon RDS-Datenbank als Datenbank verwenden, verwenden Sie Enhanced Monitoring. PeopleSoft Diese Funktion bietet Zugriff auf über 50 Messwerte, darunter CPU, Arbeitsspeicher, Dateisystem-I/O und Festplatten-I/O.

- Verwenden Sie AWS CloudTrail, um API-Aufrufe auf den AWS-Ressourcen zu überwachen, die Ihre PeopleSoft Anwendung verwendet. Dies hilft Ihnen bei der Durchführung von Sicherheitsanalysen, der Nachverfolgung von Ressourcenänderungen und der Überprüfung der Einhaltung von Vorschriften.

Bewährte Methoden für die Gewährleistung der Sicherheit

- Verwenden Sie AWS WAF, um Ihre PeopleSoft Anwendung vor häufigen Exploits wie SQL-Injection oder Cross-Site Scripting (XSS) zu schützen. Erwägen Sie die Nutzung von AWS Shield Advanced für maßgeschneiderte Erkennungs- und Schadensbegrenzungsservices.
- Fügen Sie dem Application Load Balancer eine Regel hinzu, um den Datenverkehr automatisch von HTTP zu HTTPS umzuleiten, um Ihre PeopleSoft Anwendung zu schützen.
- Richten Sie eine separate Sicherheitsgruppe für den Application Load Balancer ein. Diese Sicherheitsgruppe sollte nur eingehenden HTTPS/HTTP-Verkehr und keinen ausgehenden Datenverkehr zulassen. Dadurch wird sichergestellt, dass nur beabsichtigter Datenverkehr zulässig ist, und trägt zur Sicherheit Ihrer Anwendung bei.
- Verwenden Sie private Subnetze für die Anwendungsserver, Webserver und die Datenbank und verwenden Sie NAT-Gateways für ausgehenden Internetverkehr. Dadurch wird sichergestellt, dass die Server, die die Anwendung unterstützen, nicht öffentlich erreichbar sind, und gleichzeitig wird der öffentliche Zugriff nur den Servern gewährt, die ihn benötigen.
- Verwenden Sie verschiedene VPCs für den Betrieb Ihrer PeopleSoft Produktions- und Nichtproduktionsumgebungen. Verwenden Sie AWS Transit Gateway, VPC-Peering, Netzwerk-ACLs und Sicherheitsgruppen, um den Datenfluss zwischen den VPC und, falls erforderlich, Ihrem lokalen Rechenzentrum zu steuern.
- Folgen Sie dem Prinzip der geringsten Rechte. Gewähren Sie den Zugriff auf die von der PeopleSoft Anwendung verwendeten AWS-Ressourcen nur Benutzern, die ihn unbedingt benötigen. Gewähren Sie nur die Mindestberechtigungen, die zur Ausführung einer Aufgabe erforderlich sind. Weitere Informationen finden Sie in der Sicherheitssäule des AWS Well-Architected Framework.
- Verwenden Sie nach Möglichkeit AWS Systems Manager, um auf die EC2-Instances zuzugreifen, die die PeopleSoft Anwendung verwendet.

Bewährte Methoden zur Zuverlässigkeit

- Wenn Sie einen Application Load Balancer verwenden, registrieren Sie ein einzelnes Ziel für jede aktivierte Availability Zone. Dadurch ist der Load Balancer am effektivsten.
- Wir empfehlen, dass Sie für jede PeopleSoft Produktionsumgebung drei unterschiedliche URLs verwenden: eine URL für den Zugriff auf die Anwendung, eine für den Integration Broker und eine für die Anzeige von Berichten. Wenn möglich, sollte jede URL ihre eigenen dedizierten Webserver und Anwendungsserver haben. Dieses Design trägt dazu bei, Ihre PeopleSoft Anwendung sicherer zu machen, da jede URL über eine eigene Funktionalität und einen kontrollierten Zugriff verfügt. Es minimiert auch den Umfang der Auswirkungen, wenn die zugrunde liegenden Dienste ausfallen.
- Wir empfehlen Ihnen, Integritätsprüfungen für die Load Balancer-Zielgruppen für Ihre PeopleSoft Anwendung zu konfigurieren. Die Integritätsprüfungen sollten auf den Webservern und nicht auf den EC2-Instances durchgeführt werden, auf denen diese Server ausgeführt werden. Dadurch wird sichergestellt, dass der Application Load Balancer diese Informationen korrekt wiedergibt, wenn der Webserver abstürzt oder die EC2-Instance, die den Webserver hostet, ausfällt.
- Für eine PeopleSoft Produktionsanwendung empfehlen wir, die Webserver auf mindestens drei Availability Zones zu verteilen. Dadurch wird sichergestellt, dass die PeopleSoft Anwendung immer hochverfügbar ist, auch wenn eine der Availability Zones ausfällt.
- Für eine PeopleSoft Produktionsanwendung aktivieren Sie Jolt Pooling ()`joltPooling=true`. Dadurch wird sichergestellt, dass Ihre Anwendung ein Failover auf einen anderen Anwendungsserver durchführt, falls ein Server zu Patching-Zwecken oder aufgrund eines VM-Fehlers ausgefallen ist.
- Legen Sie für eine PeopleSoft Produktionsanwendung den Wert 1 fest`DynamicConfigReload` . Diese Einstellung wird in PeopleTools Version 8.52 und höher unterstützt. Sie fügt dem Webserver dynamisch neue Anwendungsserver hinzu, ohne die Server neu zu starten.
- Um Ausfallzeiten bei der Installation von PeopleTools Patches zu minimieren, verwenden Sie die blaue/grüne Bereitstellungsmethode für Ihre Auto Scaling Scaling-Gruppenstartkonfigurationen für die Web- und Anwendungsserver. Weitere Informationen finden Sie im AWS-Whitepaper „Überblick über Bereitstellungsoptionen“.
- Verwenden Sie AWS Backup, um Ihre PeopleSoft Anwendung auf AWS zu sichern. AWS Backup ist ein kostengünstiger, vollständig verwalteter und richtlinienbasierter Service, der den Datenschutz in großem Maßstab vereinfacht.

Bewährte Methoden zur Leistung

- Beenden Sie das SSL am Application Load Balancer, um eine optimale Leistung der PeopleSoft Umgebung zu erzielen, es sei denn, Ihr Unternehmen benötigt verschlüsselten Datenverkehr in der gesamten Umgebung.
- Erstellen Sie VPC-Endpunkte mit Schnittstellen für AWS-Services wie Amazon Simple Notification Service (Amazon SNS), CloudWatchsodass der Datenverkehr immer intern ist. Das ist kostengünstig und trägt zur Sicherheit Ihrer Anwendung bei.

Bewährte Methoden zur Kostenoptimierung

- Kennzeichnen Sie alle Ressourcen, die von Ihrer PeopleSoft Umgebung verwendet werden, und aktivieren Sie Tags zur Kostenzuweisung. Diese Tags helfen Ihnen dabei, Ihre Ressourcenkosten einzusehen und zu verwalten.
- Richten Sie für eine PeopleSoft Produktionsanwendung Auto Scaling Scaling-Gruppen für die Webserver und die Anwendungsserver ein. Dadurch wird eine minimale Anzahl von Web- und Anwendungsservern zur Unterstützung Ihrer Anwendung bereitgestellt. Sie können Auto Scaling Scaling-Gruppenrichtlinien verwenden, um die Server nach Bedarf hoch- und herunterzuskalieren.
- Verwenden Sie Fakturierungsalarme, um Benachrichtigungen zu erhalten, wenn die Kosten einen von Ihnen angegebenen Budgetschwellenwert überschreiten.

Bewährte Praktiken im Bereich Nachhaltigkeit

- Verwenden Sie Infrastructure as Code (IaC) zur Wartung Ihrer PeopleSoft Umgebungen. Auf diese Weise können Sie konsistente Umgebungen aufbauen und die Kontrolle über Änderungen behalten.

Epen

Migrieren Sie Ihre PeopleSoft Datenbank zu Amazon RDS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DB-Subnet zgruppe.	Wählen Sie in der Amazon RDS-Konsole im Navigatio nsbereich Subnetzgruppen aus und erstellen Sie dann eine Amazon RDS-DB-Su	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bnetzgruppe mit Subnetzen in mehreren Availability Zones. Dies ist erforderlich, damit die Amazon RDS-Datenbank in einer Multi-AZ-Konfiguration ausgeführt werden kann.	
Erstellen Sie die Amazon RDS-Datenbank.	Erstellen Sie eine Amazon RDS-Datenbank in einer Availability Zone der AWS-Region, die Sie für die PeopleSoft HA-Umgebung ausgewählt haben. Achten Sie beim Erstellen der Amazon RDS-Datenbank darauf, die Multi-AZ-Option (Standby-Instance erstellen) und die Datenbank-Subnetzgruppe auszuwählen, die Sie im vorherigen Schritt erstellt haben. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	Cloud-Administrator, Oracle-Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Ihre PeopleSoft Datenbank zu Amazon RDS.	Migrieren Sie Ihre bestehende PeopleSoft Datenbank mithilfe des AWS Database Migration Service (AWS DMS) in die Amazon RDS-Datenbank. Weitere Informationen finden Sie in der AWS-DMS-Dokumentation und im AWS-Blogbeitrag Migration von Oracle-Datenbanken mit nahezu null Ausfallzeiten mithilfe von AWS DMS.	Cloud-Administrator PeopleSoft , DBA

Richten Sie Ihr Amazon EFS-Dateisystem ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Dateisystems.	Erstellen Sie auf der Amazon EFS-Konsole ein Dateisystem und mounten Sie Ziele für jede Availability Zone. Anweisungen finden Sie in der Amazon EFS-Dokumentation. Wenn das Dateisystem erstellt wurde, notieren Sie sich seinen DNS-Namen. Sie werden diese Informationen verwenden, wenn Sie das Dateisystem mounten.	Cloud-Administrator

Richten Sie Ihre PeopleSoft Anwendung und Ihr Dateisystem ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten einer EC2-Instance.	Starten Sie eine EC2-Instance für Ihre PeopleSoft Anwendung. Anweisungen finden Sie in der Amazon EC2 EC2-Dokumentation. • Geben Sie unter Name `APP_TEMPLATE` ein. • Wählen Sie für Betriebssystem-Images Red Hat. • Wählen Sie unter Instanztyp den Instanztyp aus, der für Ihre PeopleSoft Anwendung geeignet ist. Weitere Informationen finden Sie unter Architekturdetails im Abschnitt Architektur.	Cloud-Administrator, PeopleSoft Administrator
PeopleSoft Auf der Instanz installieren.	Installieren Sie Ihre PeopleSoft Anwendung und PeopleTools auf der EC2-Instance, die Sie erstellt haben. Anweisungen finden Sie in der Oracle-Dokumentation.	Cloud-Administrator, PeopleSoft Administrator
Erstellen Sie den Anwendungsserver.	Erstellen Sie den Anwendungsserver für die AMI-Vorlage und stellen Sie sicher, dass er erfolgreich eine Verbindung zur Amazon RDS-Datenbank herstellt.	Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Mounten Sie das Amazon-EFS-Dateisystem ein.	Melden Sie sich als Root-Benutzer bei der EC2-Instance an und führen Sie die folgenden Befehle aus, um das Amazon EFS-Dateisystem in einem Ordner namens `PSFTMNT` Server zu mounten.
	`sudo su -`
	`mkdir /psftmnt`
	`cat /etc/fstab`
	Hängen Sie die folgende Zeile an die `/etc/fstab` Datei an. Verwenden Sie den DNS-Namen, den Sie sich bei der Erstellung des Dateisystems notiert haben.
	`fs-09e064308f11453 88.efs.us-east-1.a mazonaws.com:/ / psftmnt nfs4 nfsvers=4 .1,rsize=1048576,w size=1048576,hard, timeo=600,retrans= 2,noresvport,_netdev 0 0`
	`mount -a`
		Cloud-Administrator, PeopleSoft Administrator

Überprüfen Sie die Berechtigungen.	Stellen Sie sicher, dass der `PSFTMNT` Ordner über die richtigen Berechtigungen verfügt, damit der PeopleSoft Benutzer ordnungsgemäß darauf zugreifen kann.	Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie zusätzliche Instanzen.	Wiederhole die vorherige n Schritte in diesem Epos, um Template-Instances für den Process Scheduler , den Webserver und den Elasticsearch-Server zu erstellen. Nennen Sie diese InstanzenPRCS_TEMP LATE ,WEB_TEMPLATE , und. SRCH_TEMPLATE Legen Sie für den Webserver joltPooling=true und festDynamicConfigReloa d=1 .	Cloud-Administrator, PeopleSoft Administrator

Erstellen Sie Skripts zum Einrichten von Servern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Skript zur Installation des Anwendung sservers.	Erstellen Sie in der Amazon EC2 APP_TEMPLATE EC2-Instance als PeopleSoft Benutzer das folgende Skript. Benennen Sie es appstart. sh und platzieren Sie es im PS_HOME Verzeichn is. Sie verwenden dieses Skript, um den Anwendung sserver aufzurufen und den Servernamen auf dem Amazon EFS-Mount aufzuzeic hnen. `#!/bin/ksh`	PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`. /usr/homes/hcmdemo /.profile.`
	`psadmin -c configure -d HCMDEMO`
	`psadmin -c parallelboot -d HCMDEMO`
	`touch /psftmnt/`echo $HOSTNAME`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Skript zur Installation des Process Scheduler-Servers.	Erstellen Sie in der Amazon EC2 `PRCS_TEMPLATE` EC2-Instance als PeopleSoft Benutzer das folgende Skript. Benennen Sie es `prcsstart.sh` und platzieren Sie es im `PS_HOME` Verzeichnis. Sie werden dieses Skript verwenden, um den Process Scheduler-Server aufzurufen.
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/. profile`
	`/* The following line ensures that the process scheduler always has a unique name during replaceme nt or scaling activity. */`
	`sed -i "s/.*Prcs ServerName.*/`host name -I | awk -F. '{print "PrcsServ erName=PSUNX"$3$4} '`/" $HOME/appserv/ prcs/*/psprcs.cfg`
	`psadmin -p configure -d HCMDEMO`
	`psadmin -p start -d HCMDEMO`
		PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Skript zur Installation des Elasticsearch-Servers.	Erstellen Sie in der Amazon EC2 `SRCH_TEMPLATE` EC2-Instance als Elasticsearch-Benutzer das folgende Skript. Benennen Sie es `srchstart.sh` und platzieren Sie es im `HOME` Verzeichnis.
	`#!/bin/ksh`
	`/* The following line ensures that the correct IP is indicated in the elasticsearch.yaml file. */`
	`sed -i "s/.*network.host.*/`hostname -I
		awk '{print "host:"$0}'`/" $ES_HOME_DIR/config/elasticsearch.yaml`
		`nohup $ES_HOME_DIR/bin/elasticsearch &`
			PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Skript zur Installation des Webservers.	Erstellen Sie in der Amazon EC2 `WEB_TEMPLATE` EC2-Instance als Webserver-Benutzer die folgenden Skripts im `HOME` Verzeichnis. `renip.sh`: Dieses Skript stellt sicher, dass der Webserver die richtige IP hat, wenn er aus dem AMI geklont wird. `#!/bin/ksh` `hn=`hostname`` `/* On the following` ` line, change the IP` ` with the hostname with` ` the hostname of the web` ` template. */` `for text_file in `find` ` * -type f -exec grep` ` -l '<hostname-of-the-` `web-template>' {} \;` `do` `sed -e 's/<hostn` `ame-of-the-web-tem` `plate>/'$hn'/g'` ` $text_file > temp` `mv -f temp $text_file` `done`  `psstrsetup.sh` : Dieses Skript stellt sicher, dass der Webserver die richtigen Anwendungsserver-IPs verwendet, die derzeit ausgeführt werden. Es versucht, eine Verbindung zu jedem Anwendungsserver am	PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Jolt-Port herzustellen und fügt ihn der Konfigurationsdatei hinzu. `#!/bin/ksh` `c2=""` `for ctr in `ls -1 /psftmnt/*.internal`` `do` `c1=`echo $ctr | awk -F "/" '{print $3}'`` `/* In the following lines, 9000 is the jolt port. Change it if necessary. */` `if nc -z $c1 9000 2> /dev/null; then` `if [[ $c2 = "" ]]; then` `c2="psserver="`echo $c1`":9000"` `else` `c2=`echo $c2`","`echo $c1`":9000"` `fi` `fi` `done` `webstart.sh` : Dieses Skript führt die beiden vorherigen Skripten aus und startet die Webserver. `#!/bin/ksh` `/* Change the path in the following if necessary. */` `cd /usr/homes/hcmdemo` `./renip.sh` `./psstrsetup.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`webserv/peoplesoft/bin/startPIA.sh`	
Fügen Sie einen Crontab-E intrag hinzu.	Fügen Sie in der Amazon EC2 `WEB_TEMPLATE` EC2-Instance als Webserver-Benutzer die folgende Zeile zu crontab hinzu. Ändern Sie die Zeit und den Pfad, um die benötigten Werte widerzuspiegeln. Dieser Eintrag stellt sicher, dass Ihr Webserver immer die richtigen Anwendungsserver-Einträge in der `configuration.properties` Datei hat. `* * * * * /usr/homes/hcmdemo/psstrsetup.sh`	PeopleSoft Administrator

AMIs und Auto Scaling Scaling-Gruppenvorlagen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AMI für die Anwendungsservervorlage.	Erstellen Sie auf der Amazon EC2 EC2-Konsole ein AMI-Image der Amazon EC2 EC2-Instance`APP_TEMPLATE` . Nennen Sie das `AMIPSAPPSRV-SCG-VER1` . Anweisungen finden Sie in der Amazon EC2 EC2-Dokumentation.	Cloud-Administrator, PeopleSoft Administrator
Erstellen Sie AMIs für die anderen Server.	Wiederholen Sie den vorherigen Schritt, um AMIs	Cloud-Administrator, Administrator PeopleSoft

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für den Process Scheduler, den Elasticsearch-Server und den Webserver zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Anwendung sservers.	Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Anwendung sservers. Benennen Sie die Vorlage Wählen Sie `PSAPPSRV_TEMPLATE.` in der Vorlage das AMI aus, das Sie für die `APP_TEMPL ATE` Instance erstellt haben. Anweisungen finden Sie in der Amazon EC2 EC2-Dokumentation.
	• Wählen Sie in der Startvorlage den Instance-Typ entsprechend Ihren Anforderungen aus.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `appstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/homes/ hcmdemo/appstart.sh” - hcmdemo`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Process Scheduler-Servers.	Wiederholen Sie den vorherigen Schritt, um eine Startvorlage für die Auto Scaling Scaling-Gruppe des Process Scheduler-Servers zu erstellen. Benennen Sie die Vorlage`PSPRCS_TEMPLATE` . Wählen Sie in der Vorlage das AMI aus, das Sie für den Prozessplaner erstellt haben.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `prcsstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/hcmdemo/prcssta`
	`rt.sh” - hcmdemo`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Elasticsearch-Servers.	Wiederholen Sie die vorherigen Schritte, um eine Startvorlage für die Auto Scaling Scaling-Gruppe des Elasticsearch-Servers zu erstellen. Benennen Sie die Vorlage`SRCH_TEMPLATE` . Wählen Sie in der Vorlage das AMI aus, das Sie für den Suchserver erstellt haben.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `srchstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/essearch/srchst`
	`art.sh” - essearch`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Webservers.	Wiederholen Sie die vorherigen Schritte, um eine Startvorlage für die Auto Scaling Scaling-Gruppe des Webservers zu erstellen. Benennen Sie die Vorlage `WEB_TEMPLATE`. Wählen Sie in der Vorlage das AMI aus, das Sie für den Webserver erstellt haben.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `webstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/homes/hcmdemo/webstart.sh”`
	`- hcmdemo`
		Cloud-Administrator, PeopleSoft Administrator

Auto Scaling Scaling-Gruppen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Auto Scaling Scaling-Gruppe für den Anwendungsserver.	Erstellen Sie auf der Amazon EC2 EC2-Konsole mithilfe der `PSAPPSRV_TEMPLATE` Vorlage eine Auto Scaling Scaling-Gruppe, die `PSAPPSRV_ASG` für den Anwendungsserver aufgerufen wird. Anweisungen finden Sie in der Amazon EC2 EC2-Dokumentation. • Wählen Sie auf der Seite Instance-Startoptionen auswählen die richtige VPC aus und wählen Sie dann mehrere Subnetze aus verschiedenen Availability Zones aus. • Wählen Sie auf der Seite Erweiterte Optionen konfigurieren keinen Load Balancer aus. • Wählen Sie auf der Seite Gruppengröße und Skalierungsrichtlinien konfigurieren Einstellungen aus, je nachdem, für wie viel Last Sie Ihr System einrichten möchten und ob Sie eine Skalierungsrichtlinie verwenden möchten. Es wird empfohlen, die gewünschte Kapazität	Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Mindestkapazität auf mindestens 2 festzulegen, sodass zu jedem Zeitpunkt mindestens eine Instanz für den Datenverkehr verfügbar ist. Weitere Informationen zu Auto Scaling Scaling-R ichtlinien finden Sie in der Amazon EC2 EC2-Dokum entation.	
Erstellen Sie Auto Scaling Scaling-Gruppen für die anderen Server.	Wiederholen Sie den vorherigen Schritt, um Auto Scaling Scaling-Gruppen für den Prozessplaner, den Elasticsearch-Server und den Webserver zu erstellen.	Cloud-Administrator, Administr ator PeopleSoft

Zielgruppen erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe für den Webserver.	Erstellen Sie auf der Amazon EC2 EC2-Konsole eine Zielgruppe für den Webserver . Anweisungen finden Sie in der Elastic Load Balancing Balancing-Dokumentation. Stellen Sie den Port auf den Port ein, den der Webserver abhört.	Cloud-Administrator
Konfigurieren Sie Integritä tsprüfungen.	Vergewissern Sie sich, dass die Zustandsprüfungen die richtigen Werte haben, um	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre Geschäftsanforderungen widerzuspiegeln. Weitere Informationen finden Sie im Elastic Load Balancing-Benutzerhandbuch.	
Erstellen Sie eine Zielgruppe für den Elasticsearch-Server.	Wiederholen Sie die vorherigen Schritte, um eine Zielgruppe mit dem Namen `PSFTSRCH` Elasticsearch-Server zu erstellen, und legen Sie den richtigen Elasticsearch-Port fest.	Cloud-Administrator
Fügen Sie Zielgruppen zu Auto Scaling Scaling-Gruppen hinzu.	Öffnen Sie die Auto Scaling Scaling-Gruppe des Webservers mit dem Namen`PSPIA_ASG` , die Sie zuvor erstellt haben. Wählen Sie auf der Registerkarte Load Balancing die Option Bearbeiten aus und fügen Sie die `PSFTWEB` Zielgruppe dann der Auto Scaling Scaling-Gruppe hinzu. Wiederholen Sie diesen Schritt für die Elasticsearch Auto Scaling Scaling-Gruppe`PSSRCH_ASG` , um die zuvor `PSFTSRCH` erstellte Zielgruppe hinzuzufügen.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Dauer der Sitzung fest.	Wählen Sie in der Zielgrupp e PSFTWEB die Registerkarte Attribute und dann Bearbeite n aus und legen Sie die Sitzungsbindung fest. Wählen Sie für den Typ „Stickiness“ die Option Load Balancer generated cookie aus und legen Sie die Dauer auf 1 fest. Weitere Informationen finden Sie im Elastic Load Balancing-Benutzerhandbuch. Wiederholen Sie diesen Schritt für die Zielgruppe. PSFTSRCH	Cloud-Administrator

Erstellen und konfigurieren Sie Load Balancer für Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Load Balancer für die Webserver.	Erstellen Sie einen Applicati on Load Balancer mit dem Namen PSFTLB für den Lastenausgleich des Datenverkehrs zu den Webservern. Anweisung en finden Sie in der Elastic Load Balancing Balancing-Dokumentation. • Geben Sie den Namen des Load Balancers an. • Für Scheme, wählen Sie Internet-facing.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie im Abschnitt Netzwerkzuordnung die richtige VPC und mindesten s zwei öffentliche Subnetze aus verschiedenen Availabil ity Zones aus. • Wählen Sie im Abschnitt Listener und Routing die Zielgruppe aus `PSFTWEB` und geben Sie das richtige Protokoll und die richtige Portnummer an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Load Balancer für die Elasticsearch-Server.	Erstellen Sie einen Application Load Balancer mit dem Namen für `PSFTSCH` den Lastenausgleich des Datenverkehrs zu den Elasticsearch-Servern. • Geben Sie den Namen des Load Balancers an. • Wählen Sie für Schema die Option Intern aus. • Wählen Sie im Abschnitt Netzwerkzuordnung die richtige VPC und die richtigen privaten Subnetze aus. • Wählen Sie im Abschnitt Listener und Routing die Zielgruppe aus `PSFTSRCH` und geben Sie das richtige Protokoll und die richtige Portnummer an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Route 53	Erstellen Sie auf der Amazon Route 53 53-Konsole einen Datensatz in der Hosting-Zone, der die PeopleSoft Anwendung bedienen wird. Anweisungen finden Sie in der Dokumentation zu Amazon Route 53 Dadurch wird sichergestellt, dass der gesamte Datenverkehr den Load PSFTLB Balancer durchläuft.	Cloud-Administrator

Zugehörige Ressourcen

- PeopleSoft Oracle-Webseite
- AWS-Dokumentation

Mehr Muster

- Bereitstellen einer geclusterten Anwendung in Amazon ECS mithilfe von AWS Copilot
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Dokumentieren Sie institutionelles Wissen anhand von Spracheingaben mithilfe von Amazon Bedrock und Amazon Transcribe

Cloud-nativ

Themen

- Erstellen einer Videoverarbeitungs-Pipeline mithilfe von Amazon Kinesis Video Streams und AWS Fargate
- Überwachen von SAP RHEL-Pacemaker-Clustern mithilfe von AWS-Services
- Erfolgreiches Importieren eines S3-Buckets als AWS- CloudFormation Stack
- Mehr Muster

Erstellen einer Videoverarbeitungs-Pipeline mithilfe von Amazon Kinesis Video Streams und AWS Fargate

Erstellt von Piotr Chotkowski (AWS) und Pushparaju Thangavel (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Cloudnativ; Softwareentwicklung und -tests; Medienservices	AWS-Services: AWS Fargate; Amazon Kinesis ;Amazon S3

Übersicht

Dieses Muster zeigt, wie Sie Amazon Kinesis Video Streams und AWS Fargate verwenden, um Frames aus einem Videostream zu extrahieren und sie als Bilddateien zur weiteren Verarbeitung in Amazon Simple Storage Service (Amazon S3) zu speichern.

Das Muster stellt eine Beispielanwendung in Form eines Java-Maven-Projekts bereit. Diese Anwendung definiert die AWS-Infrastruktur mithilfe des AWS Cloud Development Kit (AWS CDK). Sowohl die Frame-Verarbeitungslogik als auch die Infrastrukturdefinitionen werden in der Programmiersprache Java geschrieben. Sie können diese Beispielanwendung als Grundlage für die Entwicklung Ihrer eigenen Echtzeit-Videoverarbeitungspipeline oder für die Erstellung des Videovorverarbeitungsschritts einer Machine-Learning-Pipeline verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java SE Development Kit (JDK) 11, installiert
- Apache Maven , installiert
- AWS Cloud Development Kit (AWS CDK), installiert
- AWS Command Line Interface (AWS CLI) Version 2, installiert
- Docker (erforderlich für die Erstellung von Docker-Images zur Verwendung in AWS Fargate-Aufgabendefinitionen), installiert

Einschränkungen

Dieses Muster dient als Machbarkeitsnachweis oder als Grundlage für die weitere Entwicklung. Es sollte nicht in seiner aktuellen Form in Produktionsbereitstellungen verwendet werden.

Produktversionen

- Dieses Muster wurde mit der AWS-CDK-Version 1.77.0 getestet (siehe AWS-CDK-Versionen)
- JDK 11
- AWS CLI Version 2

Architektur

Zieltechnologie-Stack

- Amazon Kinesis Video Streams
- AWS Fargate-Aufgabe
- Amazon Simple Queue Service-Warteschlange (Amazon SQS)
- Amazon S3-Bucket

Zielarchitektur

Der Benutzer erstellt einen Kinesis-Videostrom, lädt ein Video hoch und sendet eine JSON-Nachricht, die Details zum Kinesis-Videostrom und zum S3-Ausgabe-Bucket enthält, an eine SQS-Warteschlange. AWS Fargate, auf dem die Hauptanwendung in einem Container ausgeführt wird, ruft die Nachricht aus der SQS-Warteschlange ab und beginnt mit dem Extrahieren von Frames. Jeder Frame wird in einer Bilddatei und im S3-Ziel-Bucket gespeichert.

Automatisierung und Skalierung

Die Beispielanwendung kann sowohl horizontal als auch vertikal innerhalb einer einzigen AWS-Region skaliert werden. Eine horizontale Skalierung kann erreicht werden, indem die Anzahl der bereitgestellten AWS Fargate-Aufgaben erhöht wird, die aus der SQS-Warteschlange lesen. Die vertikale Skalierung kann erreicht werden, indem die Anzahl der Frame-Splitting- und Image-Publishing-Threads in der Anwendung erhöht wird. Diese Einstellungen werden in der Definition der QueueProcessingFargateService Ressource im AWS-CDK als Umgebungsvariablen an die Anwendung übergeben. Aufgrund der Art der AWS-CDK-Stack-Bereitstellung können Sie diese Anwendung ohne zusätzlichen Aufwand in mehreren AWS-Regionen und -Konten bereitstellen.

Tools

Tools

- AWS CDK ist ein Softwareentwicklungs-Framework zur Definition Ihrer Cloud-Infrastruktur und -Ressourcen mithilfe von Programmiersprachen wie TypeScript, JavaScript, Python, Java und C#/.Netz.
- Amazon Kinesis Video Streams ist ein vollständig verwalteter AWS-Service, mit dem Sie Live-Videos von Geräten in die AWS Cloud streamen oder Anwendungen für die Echtzeit-Videoverarbeitung oder batchorientierte Videoanalysen erstellen können.
- AWS Fargate ist eine Serverless-Rechen-Engine für Container. Fargate macht die Bereitstellung und Verwaltung von Servern überflüssig und ermöglicht es Ihnen, sich auf die Entwicklung Ihrer Anwendungen zu konzentrieren.
- Amazon S3 ist ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.
- Amazon SQS ist ein vollständig verwalteter Service zur Nachrichtenwarteschlange, mit dem Sie Microservices, verteilte Systeme und Serverless-Anwendungen entkoppeln und skalieren können.

Code

- Eine ZIP-Datei des Beispielanwendungsprojekts (`frame-splitter-code.zip`) ist angehängt.

Polen

Bereitstellen der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Docker-Da emon.	Starten Sie den Docker-Daemon auf Ihrem lokalen System. Das AWS-CDK verwendet Docker, um das Image zu erstellen, das in der AWS Fargate-Aufgabe verwendet wird. Sie müssen Docker ausführen, bevor Sie	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit dem nächsten Schritt fortfahren.	
Erstellen Sie das Projekt.	Laden Sie die `frame-splitter-code` Beispielanwendung (angefügt) herunter und extrahieren Sie ihren Inhalt in einen Ordner auf Ihrem lokalen Computer. Bevor Sie die Infrastruktur bereitstellen können, müssen Sie das Java Maven-Projekt erstellen. Navigieren Sie an einer Eingabeaufforderung zum Stammverzeichnis des Projekts und erstellen Sie das Projekt, indem Sie den Befehl ausführen: `mvn clean install`	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrappen Sie das AWS-CDK.	(Nur erstmalige AWS-CDK-Benutzer) Wenn Sie das AWS-CDK zum ersten Mal verwenden, müssen Sie möglicherweise einen Bootstrap für die Umgebung ausführen, indem Sie den AWS CLI-Befehl ausführen: `cdk bootstrap --profile "$AWS_PROFILE_NAME"` wobei den Namen des AWS-Profils aus Ihren AWS-Anmeldeinformationen `$AWS_PROFILE_NAME` enthält. Sie können diesen Parameter auch entfernen, um das Standardprofil zu verwenden. Weitere Informationen finden Sie in der AWS-CDK-Dokumentation.	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS-CDK-Stack bereit.	In diesem Schritt erstellen Sie die erforderlichen Infrastrukturressourcen (SQS-Warteschlange, S3-Bucket, AWS Fargate-Aufgabendefinition) in Ihrem AWS-Konto, erstellen das Docker-Image, das für die AWS Fargate-Aufgabe erforderlich ist, und stellen die Anwendung bereit. Navigieren Sie an einer Eingabeaufforderung zum Stammverzeichnis des Projekts und führen Sie den Befehl aus: `cdk deploy --profile "$AWS_PROFILE_NAME" --all` wobei den Namen des AWS-Profils aus Ihren AWS-Anmeldeinformationen `$AWS_PROFILE_NAME` enthält. Sie können diesen Parameter auch entfernen, um das Standardprofil zu verwenden. Bestätigen Sie die Bereitstellung. Notieren Sie die Bucket-Werte QueueUrlund aus der CDK-Bereitstellungsausgabe. Sie benötigen diese in späteren Schritten. Das AWS-CDK erstellt die Komponenten, lädt sie in Ihr AWS-Konto hoch und erstellt	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	alle Infrastrukturressourcen. Sie können den Prozess der Ressourcenerstellung in der AWS- CloudFormation Konsole beobachten. Weitere Informationen finden Sie in der AWS- CloudFormation Dokumentation und in der AWS-CDK-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Videostream.	In diesem Schritt erstellen Sie einen Kinesis-Videostream, der als Eingabestream für die Videoverarbeitung dient. Stellen Sie sicher, dass Sie die AWS CLI installiert und konfiguriert haben. Führen Sie in der AWS CLI Folgendes aus: `aws kinesisvideo --profile "$AWS_PROFILE_NAME" create-stream --stream-name "$STREAM_NAME" --data-retention-in-hours "24"` wobei den Namen des AWS-Profils aus Ihren AWS-Anmeldeinformationen `$AWS_PROFILE_NAME` enthält (oder diesen Parameter entfernt, um das Standardprofil zu verwenden) und ein gültiger Stream-Name `$STREAM_NAME` ist. Alternativ können Sie mithilfe der Kinesis-Konsole einen Videostream erstellen, indem Sie die Schritte in der Dokumentation zu Kinesis Video Streams ausführen. Notieren Sie sich den AWS-Ressourcennamen (ARN)	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des erstellten Streams. Sie benötigen ihn später.	

Ausführen eines Beispiels

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Video in den Stream hoch.	Öffnen Sie im Projektordner für die `frame-splitter-code` Beispielanwendung die `ProcessingTaskTest.java` Datei im `src/test/java/amazon/awscdk/examples/splitter` Ordner. Ersetzen Sie die `streamName` Variablen `profileName` und durch die Werte, die Sie in den vorherigen Schritten verwendet haben. Um das Beispielvideo in den Kinesis-Videostream hochzuladen, den Sie im vorherigen Schritt erstellt haben, führen Sie aus: `amazon.awscdk.examples.splitter.ProcessingTaskTest#testExample test` Alternativ können Sie Ihr Video mit einer der in der Dokumentation zu Kinesis	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Video Streams beschriebenen Methoden hochladen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initiieren Sie die Videoverarbeitung.	Nachdem Sie nun ein Video in den Kinesis-Videostrom hochgeladen haben, können Sie mit der Verarbeitung beginnen. Um die Verarbeitungslogik zu initiieren, müssen Sie eine Nachricht mit Details an die SQS-Warteschlange senden, die das AWS-CDK während der Bereitstellung erstellt hat. Um eine Nachricht mit der AWS CLI zu senden, führen Sie Folgendes aus:
	`aws sqs --profile "$AWS_PROFILE_NAME" send-message --queue-url QUEUE_URL --message-body MESSAGE`
	wobei den Namen des AWS-Profils aus Ihren AWS-Anmeldeinformationen `$AWS_PROFILE_NAME` enthält (diesen Parameter entfernen, um das Standardprofil zu verwenden), der `QueueUrl`Wert aus der AWS-CDK-Ausgabe `MESSAGE` und eine JSON-Zeichenfolge im folgenden Format `QUEUE_URL` ist:
	`{ "streamARN": "STREAM_ARN", "bucket": "BUCKET_N`
		Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AME", "s3Directory": "test-output" }` wobei der ARN des Videostreams `STREAM_ARN` ist, den Sie in einem früheren Schritt erstellt haben, und der Bucket-Wert aus der AWS-CDK-Ausgabe `BUCKET_NAME` ist. Das Senden dieser Nachricht initiiert die Videoverarbeitung. Alternativ können Sie eine Nachricht über die Amazon SQS-Konsole senden, wie in der Amazon SQS-Dokumentation beschrieben.	
Sehen Sie sich Bilder der Videoframes an.	Sie können die resultierenden Bilder im S3-Ausgabe-Bucket sehen `s3://BUCKET_NAME/test-output`, wobei der Bucket-Wert aus der AWS-CDK-Ausgabe `BUCKET_NAME` ist.	Entwickler, DevOps Techniker

Zugehörige Ressourcen

- AWS-CDK-Dokumentation
- AWS-CDK-API-Referenz
- AWS-CDK-Einführungsworkshop
- Dokumentation zu Amazon Kinesis Video Streams
- Beispiel: Identifizieren von Objekten in Videostreams mit SageMaker
- Beispiel: Analysieren und Rendern von Kinesis-Videostreams-Fragmenten

- Analysieren Sie Live-Videos in Echtzeit mit Amazon Kinesis Video Streams und Amazon SageMaker (Blogbeitrag von AWS Machine Learning)
- Erste Schritte mit AWS Fargate

Zusätzliche Informationen

Auswählen einer IDE

Wir empfehlen Ihnen, Ihre bevorzugte Java-IDE zu verwenden, um dieses Projekt zu erstellen und zu erkunden.

Bereinigen

Nachdem Sie dieses Beispiel ausgeführt haben, entfernen Sie alle bereitgestellten Ressourcen, um zusätzliche AWS-Infrastrukturkosten zu vermeiden.

Um die Infrastruktur und den Videostream zu entfernen, verwenden Sie diese beiden Befehle in der AWS CLI:

```
cdk destroy --profile "$AWS_PROFILE_NAME" --all
```

```
aws kinesisvideo --profile "$AWS_PROFILE_NAME" delete-stream --stream-arn "$STREAM_ARN"
```

Alternativ können Sie die Ressourcen manuell entfernen, indem Sie die AWS- CloudFormation Konsole verwenden, um den AWS- CloudFormation Stack zu entfernen, und die Kinesis-Konsole, um den Kinesis-Videostream zu entfernen. Beachten Sie, dass den S3-Ausgabe-Bucket oder die Images in Amazon Elastic Container Registry (Amazon ECR)-Repositorys () `cdk destroy` nicht entfernt`aws-cdk/assets`. Sie müssen sie manuell entfernen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen von SAP RHEL-Pacemaker-Clustern mithilfe von AWS-Services

Erstellt von Bolsh Thoria (AWS), Randy Deutsch (AWS) und RAVEENDRA Voore (AWS)

Umgebung: Produktion	Technologien: Cloudnativ; Infrastruktur; Betriebssysteme	Workload: SAP
AWS-Services: Amazon CloudWatch; Amazon SNS ; Amazon CloudWatch Logs		

Übersicht

Dieses Muster beschreibt die Schritte zur Überwachung und Konfiguration von Warnungen für einen Red Hat Enterprise Linux (RHEL) Pacemaker-Cluster für SAP-Anwendungen und SAP HANA-Datenbankservices mithilfe von Amazon CloudWatch und Amazon Simple Notification Service (Amazon SNS).

Mit der Konfiguration können Sie die Clusterressourcen von SAP SCS oder ASCS, Enqueue Replication Server (ERS) und SAP HANA überwachen, wenn sie sich in einem „gestoppten“ Zustand befinden, mithilfe von CloudWatch Protokollstreams, Metrikfiltern und Alarmen. Amazon SNS sendet eine E-Mail über den Status des gestoppten Clusters an die Infrastruktur oder das SAP-Basis-Team.

Sie können die AWS Ressourcen für dieses Muster mithilfe von AWS CloudFormation Skripten oder den AWS Servicekonsolen erstellen. Bei diesem Muster wird davon ausgegangen, dass Sie die Konsolen verwenden. Es werden keine CloudFormation Skripts bereitgestellt oder die Infrastrukturbereitstellung für CloudWatch und Amazon SNS abgedeckt. Schrittweiser-Befehle werden verwendet, um die Cluster-Warnungskonfiguration festzulegen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Amazon SNS ist für das Senden von E-Mail- oder mobilen Benachrichtigungen eingerichtet.

- Ein SAP ASCS/ERS für ABAP oder SCS/ERS für Java und ein SAP HANA Database RHEL Pacemaker-Cluster. Detaillierte Informationen finden Sie hier:
  - Einrichtung des SAP-HANA-Clusters
  - Einrichtung des SAP-Netweaver-ABAP/Java-Clusters

Einschränkungen

- Diese Lösung funktioniert derzeit für Pacemaker-basierte RHEL-Cluster der Version 7.3 und höher. Es wurde nicht auf SUSE-Betriebssystemen getestet.

Produktversionen

- RHEL 7.3 und höher

Architektur

Zieltechnologie-Stack

- RHEL-Pacemaker-Warnungsereignis-gesteuerter Agent
- Amazon Elastic Compute Cloud (Amazon EC2)
- CloudWatch Alarm
- CloudWatch Protokollgruppe und Metrikfilter
- Amazon SNS

Zielarchitektur

Das folgende Diagramm veranschaulicht die Komponenten und Workflows für diese Lösung.

Automatisierung und Skalierung

- Sie können die Erstellung von AWS Ressourcen mithilfe von CloudFormation Skripts automatisieren. Sie können auch zusätzliche Metrikfilter verwenden, um mehrere Cluster zu skalieren und abzudecken.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie ausführen, AWS in Echtzeit zu überwachen.
- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.

Tools

- CloudWatch Agent (unified) ist ein Tool, das Metriken auf Systemebene, Protokolle und Ablaufverfolgungen von EC2-Instances sammelt und benutzerdefinierte Metriken aus Ihren Anwendungen abruft.
- Der Pacemaker-Warnagent (für RHEL 7.3 und höher) ist ein Tool, das eine Aktion auslöst, wenn eine Änderung in einem Pacemaker-Cluster stattfindet, z. B. wenn eine Ressource beendet oder neu gestartet wird.

Bewährte Methoden

- Bewährte Methoden für die Verwendung von SAP-Workloads in AWSfinden Sie im SAP Lens für das AWS Well-Architected Framework.
- Berücksichtigen Sie die Kosten für die Einrichtung der CloudWatch Überwachung für SAP-HANA-Cluster. Weitere Informationen finden Sie in der CloudWatch -Dokumentation.
- Erwägen Sie, einen Pager oder Ticketing-Mechanismus für Amazon SNS-Warnungen zu verwenden.
- Suchen Sie immer nach RHEL-Hochverfügbarkeitsversionen (HA) des RPM-Pakets für pcs , Pacemaker und den FencingAWS-Agenten.

Polen

Einrichten von Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home. 2. Wählen Sie auf dem Amazon-SNS-Dashboard unter Common actions die Option Create Topic. 3. Wählen Sie im Dialogfeld Neues Thema erstellen für Typ die Option Standard aus. 4. Geben Sie unter Themenname einen Namen für das Thema ein (z. B. `my-topic`). 5. Wählen Sie Thema erstellen aus. Dadurch wird ein SNS-Thema mit einer Ressourcenrichtlinie erstellt, mit der Sie Benachrichtigungen veröffentlichen können. 6. Kopieren Sie den Themen-ARN (z. B. `arn:aws:sns:us-east-1:11112`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`2223333:my-topic`). Sie werden diesen ARN in einem späteren Schritt verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Zugriffsr ichtlinie für das SNS-Thema.	1. Wählen Sie in der Amazon SNS-Konsole im Navigatio nsbereich Themen und dann das von Ihnen erstellte Thema aus. 2. Wählen Sie Bearbeiten und gehen Sie zum Abschnitt Zugriffsrichtlinie. 3. Stellen Sie sicher, dass die Zugriffsrichtlinie CloudWatc h als einen der Service-Prinzipale enthält, die zu diesem Thema veröffent lichen dürfen. Beispiels weise: `{ "Sid": "Allow AWS CloudWatch to Publish to this SNS topic", "Effect": "Allow", "Principal": { "Service": [ "cloudwatch.amazonaws.com" ] }, "Action": "SNS:Publish", "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic" }`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Änderungen speichern aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das SNS-Thema.	1. Wählen Sie in der Amazon SNS-Konsole im Navigationsbereich Abonnements, Abonnement erstellen aus. 2. Fügen Sie für Themen-ARN den ARN ein, den Sie in der ersten Aufgabe erstellt haben. 3. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. 4. Geben Sie für Endpunkt eine E-Mail-Adresse für die Person oder das Team ein, die für den SAP-Pacemaker-Cluster verantwortlich ist und Benachrichtigungen erhalten soll. Dies kann beispielsweise die E-Mail-Adresse für die -Verteilerliste von SAP Basis oder Infrastrukturteam sein. 5. Wählen Sie Create subscription (Abonnement erstellen) aus. 6. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht von AWS Notifications und bestätigen Sie Ihr Abonnement.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihr Webbrowser zeigt eine Bestätigungsantwort vom Amazon SNS an.	

Bestätigen Sie die Einrichtung des Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Cluster-Status.	Verwenden Sie den Befehl pcs status, um zu bestätigen, dass die Ressourcen online sind.	SAP-Basis-Administrator

Konfigurieren von Pacemaker-Warnungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie den Pacemaker-Warnagenten auf der primären Cluster-Instance.	Melden Sie sich bei der EC2-Instance im pimary-Cluster an und führen Sie die folgenden Befehle aus:
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample`
	`touch /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
		SAP-Basis-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pcs alert create id=alert_file description="Log events to a file." path=/var/lib/pacemaker/alert_file.sh` `pcs alert recipient add alert_file id=my-alert_logfile value=/var/log/pcmk_alert_file.log`	

Konfigurieren Sie den Pacemaker-Warnagenten auf der sekundären Cluster-Instance.	Melden Sie sich bei der EC2-Instance des sekundären Clusters im sekundären Cluster an und führen Sie die folgenden Befehle aus:
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
		SAP-Basis-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass die RHEL-Warnressource erstellt wurde.	Verwenden Sie den folgenden Befehl, um zu bestätigen, dass die Warnressource erstellt wurde:
	`pcs alert`
	Die Ausgabe des Befehls sieht wie folgt aus:
	`[root@xxxxxxx ~]# pcs alert`
	`Alerts:`
	` Alert: alert_file (path=/var/lib/pacemaker/alert_file.sh)`
	`  Description: Log events to a file.`
	`  Recipients:`
	`   Recipient: my-alert_logfile (value=/var/log/pcmk_alert_file.log)`
		SAP-Basis-Administrator

Konfigurieren des CloudWatch Agenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den CloudWatch Agenten.	Es gibt mehrere Möglichkeiten, den CloudWatch Agenten auf einer EC2-Instance zu installieren. So verwenden Sie die Befehlszeile: 1. Laden Sie das CloudWatch Agentenpaket herunter:	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`wget https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-region/redhat/amd64/latest/amazon-cloudwatch-agent.rpm`
	
	wobei die `<region>` ist, AWS-Region in der sich die EC2-Instance befindet (z. B. `us-west-2`).
	2. Optional) Überprüfen Sie die Paketsignatur. Anweisungen finden Sie unter Überprüfen der Signatur des CloudWatch Agentenpakets in der -CloudWatch Dokumentation.
	3. Installieren Sie das -Paket auf der ersten Instance:
	
	`sudo rpm -U ./amazon-cloudwatch-agent.rpm`
	
	4. Wiederholen Sie diesen Vorgang für die sekundäre Instance.
	
	Weitere Informationen finden Sie in der CloudWatch -Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der EC2-Instance eine IAM-Rolle an.	Damit der CloudWatch Agent Daten von den Instances senden kann, müssen Sie die IAM-CloudWatchAgentServerRoleRolle an jede Instance anfügen. Oder Sie können Ihrer vorhandenen IAM-Rolle eine Richtlinie für den CloudWatch Agenten hinzufügen. Weitere Informationen finden Sie in der CloudWatch -Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den CloudWatch Agenten so, dass er die Protokolldatei des Pacemaker-Warnagenten auf der primären Cluster-Instance überwacht.	1. Konfigurieren Sie die primäre Cluster-Instance, indem Sie den Befehl ausführen: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard` 2. Wählen Sie 1 für Linux und dann die Optionen für Ihre Überwachungsstrategie aus. 3. Wählen Sie für die Frage „Möchten Sie Protokoll dateien überwachen“ Ja aus und geben Sie den Pfad der Pacemaker-Protokolldatei aus dem pcs-Warnbefehl an. In unserem Fall ist es `var/log/pcmk_alert_file.log`. 4. Geben Sie den Namen der Protokollgruppe und des Protokollstreams an. Wenn Sie keinen Protokollstream angeben, wird die AWS Instance-ID als Standard verwendet. 5. Wiederholen Sie die Schritte 1-4 für die sekundäre Cluster-Instance.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den CloudWatch Agenten auf den primären und sekundären Cluster-Instances.	Um den Agenten zu starten, führen Sie den folgenden Befehl auf den EC2-Instances im primären und sekundären Cluster aus: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json`	AWS-Administrator

Einrichten von - CloudWatch Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie CloudWatch Protokollgruppen ein.	1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/ 2. Wählen Sie im Navigationsbereich Protokollgruppen, Protokollgruppe erstellen aus. 3. Geben Sie einen Namen für die Protokollgruppe ein und wählen Sie dann Protokollgruppe erstellen aus. Der CloudWatch Agent überträgt die Pacemaker-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Warndatei als Protokollstream an die CloudWatch Protokoll gruppe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie CloudWatch Metrikfilter ein.	Metrikfilter helfen Ihnen bei der Suche nach einem Muster wie `stop <cluster-resource-name>` in den CloudWatch Protokoll streams. Wenn dieses Muster identifiziert wird, aktualisiert der Metrikfilter eine benutzerd efinierte Metrik. 1. Wählen Sie in der CloudWatch -Konsole im Navigationsbereich Protokollgruppen aus. 2. Wählen Sie den Namen der Protokollgruppe aus, die Sie in der vorherigen Aufgabe erstellt haben. 3. Wählen Sie Aktionen, Metrikfilter erstellen aus. 4. Geben Sie für Filtermus ter das zu verwenden de Filtermuster ein, z. B. `stop ABC_scs`, um das Stoppereignis für eine SAP-SCS-Clusterressource mit dem Namen abzugleic henABC_scs. Weitere Informati onen finden Sie unter Filtermustersyntax in der - CloudWatch Dokumenta tion.	AWS-Administrator, SAP-Basis-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. (Optional) Um das Filtermuster zu testen, geben Sie unter Test Pattern (Muster testen) ein oder mehrere Protokollereignisse ein, die zum Testen des Musters verwendet werden sollen. Jedes Protokollereignis muss in einer separaten Zeile angegeben werden, da Zeilenumbrüche verwendet werden, um Protokollereignisse im Feld Protokollereignismeldungen zu trennen. 6. Wählen Sie Next (Weiter) aus und geben Sie einen Namen für den Filter ein. 7. Geben Sie unter Metrikdetails für Metrik-Namespace einen Namen für den CloudWatch Namespace ein, in dem die Metrik veröffentlicht werden soll (z. B. `sapcluster_monitoring`). Wenn dieser Namespace noch nicht vorhanden ist, wählen Sie Neu erstellen aus. 8. Geben Sie unter Metriknam e einen Namen für die neue Metrik ein (z. B. `sapcluster_<sid>` , wobei der SAP-Syste	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	midentifikationsname <sid> ist). 9. Geben Sie für Metrikwert 1 ein. Alternativ können Sie ein Token wie eingeben$size. Dadurch wird die Metrik für jedes Protokollereignis, das ein size-Feld enthält, um den Wert der Zahl in der size erhöht. 10. Geben Sie für Standardwert 0 ein. 11. Wählen Sie Metrikfilter erstellen aus. Wenn der Metrikfilter das Muster in Schritt 4 identifiziert, aktualisiert er den Wert der CloudWatch benutzerdefinierten Metrik sapcluster_abc auf 1. Der CloudWatch Alarm SAP-Cluster-QA1-ABC überwacht die Metrik sapcluster_abc und sendet eine SNS-Benachrichtigung, wenn sich der Wert der Metrik auf 1 ändert. Dies weist darauf hin, dass die Cluster-Ressource gestoppt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wurde und Maßnahmen ergriffen werden müssen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen CloudWatch Metrikalarm für die Metrik SAP ASCS/SCS und ERS ein.	So erstellen Sie einen Alarm basierend auf einer einzelnen Metrik: 1. Wählen Sie in der - CloudWatch Konsole im Navigationsbereich Alarme, Alle Alarme aus. 2. Wählen Sie Create alarm (Alarm erstellen) aus. 3. Wählen Sie Select Metric (Metrik auswählen) aus. 4. Suchen Sie nach der benutzerdefinierte n Metrik`sapcluste r_monitoring` , die in der vorherigen Aufgabe erstellt wurde. 5. Wählen Sie den Metriknam en für SAP SCS (z. B. `sapcluster_<abc>`), der auch in der vorherigen Aufgabe erstellt wurde. 6. Legen Sie auf der Registerk arte Grafische Metriken Folgendes fest: • Wählen Sie für Statistic (Statistik) Maximum aus. • Wählen Sie als Zeitraum die Option 1 Minute aus. • Wählen Sie für Schwellen werttyp die Option Statisch aus und legen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Schwellenwert für `sapcluster_<sid>` auf einen Wert fest, der größer oder gleich 1 ist. 7. Wählen Sie Weiter aus. 8. Wählen Sie für Benachrichtigung das SNS-Thema aus, das Sie im ersten Epos erstellt haben. 9. Geben Sie für Name und Beschreibung den Alarmnamen und eine kurze Beschreibung ein und wählen Sie dann Weiter aus. 10. Wählen Sie Alarm erstellen aus.	
Richten Sie einen CloudWatch Metrikalarm für die SAP HANA-Metrik ein.	Wiederholen Sie die Schritte zum Einrichten eines CloudWatch Metrikalarms aus der vorherigen Aufgabe mit diesen Änderungen: • Wählen Sie für Schritt 5 den Metriknamen für SAP HANA aus (z. B. `sapcluster_db_<abc>`). • Legen Sie für Schritt 6 den Schwellenwert für `sapcluster_<sid>` auf einen Wert größer als 0 fest.	AWS-Administrator

Zugehörige Ressourcen

- Auslösen von Skripts für Cluster-Ereignisse (RHEL-Dokumentation)
- Erstellen der CloudWatch Agentenkonfigurationsdatei mit dem Assistenten (CloudWatch Dokumentation)
- Installieren und Ausführen des CloudWatch Agenten auf Ihren Servern (CloudWatch Dokumentation)
- Erstellen eines CloudWatch Alarms basierend auf einem statischen Schwellenwert (CloudWatch Dokumentation)
- Manuelle Bereitstellung von SAP HANA in AWS mit Hochverfügbarkeitsclustern (SAP-Dokumentation auf der -AWSWebsite)
- SAP- NetWeaver Leitfäden (SAP-Dokumentation auf der -AWSWebsite)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erfolgreiches Importieren eines S3-Buckets als AWS-CloudFormation Stack

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Cloudnativ; Speicher und Backup	AWS-Services: Amazon S3; AWS CloudFormation

Übersicht

Wenn Sie Amazon Web Services (AWS)-Ressourcen wie Amazon Simple Storage Service (Amazon S3)-Buckets verwenden und einen Infrastructure as Code (IaC)-Ansatz verwenden möchten, können Sie Ihre Ressourcen in AWS importieren CloudFormation und als Stack verwalten.

Dieses Muster enthält Schritte zum erfolgreichen Importieren eines S3-Buckets als AWS-CloudFormation Stack. Mit dem Ansatz dieses Musters können Sie mögliche Fehler vermeiden, die auftreten können, wenn Sie Ihren S3-Bucket in einer einzigen Aktion importieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener S3-Bucket und eine S3-Bucket-Richtlinie. Weitere Informationen dazu finden Sie unter Welche S3-Bucket-Richtlinie sollte ich verwenden, um die AWS Config-Regel s3-einzuhaltenbucket-ssl-requests-only? im AWS Knowledge Center.
- Ein vorhandener AWS Key Management Service (AWS KMS)-Schlüssel und sein Alias. Weitere Informationen dazu finden Sie unter Arbeiten mit Aliassen in der AWS KMS-Dokumentation.
- Die `CloudFormation-template-S3-bucket` AWS- CloudFormation Beispielvorlage (angefügt), die auf Ihren lokalen Computer heruntergeladen wurde.

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer erstellt eine AWS- CloudFormation Vorlage im JSON- oder YAML-Format.
2. Die Vorlage erstellt einen AWS- CloudFormation Stack zum Importieren des S3-Buckets.
3. Der AWS- CloudFormation Stack verwaltet den S3-Bucket, den Sie in der Vorlage angegeben haben.

Technologie-Stack

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- AWS KMS
- Amazon S3

Tools

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der vorhersehbaren und wiederholten Erstellung und Bereitstellung von AWS-Infrastrukturbereitstellungen.
- AWS Identity and Access Management (IAM) – IAM ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services.
- AWS KMS – AWS Key Management Service (AWS KMS) ist ein Verschlüsselungs- und Schlüsselverwaltungsservice, der für die Cloud skaliert ist.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.

Polen

Importieren eines S3-Buckets mit CMK-basierter Verschlüsselung als AWS- CloudFormation Stack

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Vorlage zum Importieren des S3-Buckets und des CMK.	Erstellen Sie auf Ihrem lokalen Computer mithilfe der folgenden Beispielvorlage eine Vorlage zum Importieren Ihres S3-Buckets und Ihres CMK:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	AWSTemplateFormatVersion: 2010-09-09
	
	Parameters:
	
	  bucketName:
	
	    Type: String
	
	Resources:
	
	  S3Bucket:
	
	    Type: 'AWS::S3::Bucket'
	
	    DeletionPolicy: Retain
	
	    Properties:
	
	      BucketName: !Ref bucketName
	
	      BucketEncryption:
	
	        ServerSideEncryptionConfiguration:
	
	          - ServerSideEncryptionByDefault:
	
	              SSEAlgorithm: 'aws:kms'
	
	              KMSMasterKeyID: !GetAtt
	
	                - KMSS3Encryption	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- Arn
	
	KMSS3Encryption:
	
	Type: 'AWS::KMS
	::Key'
	
	DeletionPolicy:
	Retain
	
	Properties:
	
	Enabled: true
	
	KeyPolicy: !Sub
	|-
	
	{
	
	"Id": "key-
	consolepolicy-3",
	
	"Version":
	"2012-10-17",
	
	"Statemen
	t": [
	
	{
	
	"Sid": "Enable IAM User
	Permissions",
	
	"Effect": "Allow",
	
	"Principal": {</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"AWS": ["arn:aws:iam::${AWS::AccountId}:root"]
	},
	"Action": "kms:*",
	"Resource": "*"
	}
	}
	]
	}
	EnableKeyRotation: true</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS-CloudFormation Konsole, wählen Sie Stack anzeigen, wählen Sie Stack erstellen und wählen Sie dann Mit vorhandenen Ressourcen (Ressourcen importieren) aus. 2. Wählen Sie Vorlagendatei hochladen und laden Sie dann die Vorlagendatei hoch, die Sie zuvor erstellt haben. 3. Geben Sie einen Namen für Ihren Stack ein und konfigurieren Sie die verbleibenden Optionen entsprechend Ihren Anforderungen. 4. Wählen Sie Stack erstellen und warten Sie, bis sich der Status des Stacks in ändert`IMPORT_COMPLETE` .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den KMS-Schlüssel-Alias.	1. Wählen Sie in der AWS-CloudFormation Konsole Stacks aus, wählen Sie den Namen des Stacks aus, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und dann In Designer anzeigen aus.
	2. Fügen Sie dem `Resource` Abschnitt Ihrer Vorlage den folgenden Codeausschnitt hinzu, wählen Sie dann Stack erstellen und schließen Sie den Assistenten ab:
	
	`KMSS3EncryptionAlias:`
	
	`  Type: 'AWS::KMS::Alias'`
	
	`  DeletionPolicy: Retain`
	
	`  Properties:`
	
	`  AliasName: alias/S3BucketKey`
	
	`  TargetKeyId: !Ref KMSS3Encryption`
	
	Weitere Informationen dazu finden Sie unter AWS-CloudFormation Stack-Upd
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ates in der AWS- CloudForm ation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie den Stack so, dass er die S3-Bucket-Richtlinie enthält.	1. Wählen Sie in der AWS-CloudFormation Konsole Stacks aus, wählen Sie den Namen des Stacks aus, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und wählen Sie dann In Designer anzeigen aus.
	2. Fügen Sie dem `Resource` Abschnitt der Vorlage den folgenden Codeaussc hnitt hinzu, wählen Sie dann Stack erstellen und schließen Sie den Assistenten ab:
	`S3BucketPolicy:`
	`  Type: 'AWS::S3::BucketPolicy'`
	`  Properties:`
	`  Bucket: !Ref S3Bucket`
	`  PolicyDocument: !Sub |-`
	`  {`
	`  "Version": "2008-10-17",`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"Id": "restricthttp",
	"Statement": [
	{
	"Sid": "denyhttp",
	"Effect": "Deny",
	"Principal": {
	"AWS": "*"
	},
	"Action": "s3:*",
	"Resource": ["arn:aws:s3:::${S3Bucket}","arn:aws:s3:::${S3Bucket}/*"],
	"Condition": {
	"Bool": {
	"aws:SecureTransport": "false"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>}
	
	}
	
	}
	
	]
	
	}</pre>
	Hinweis: Diese S3-Bucket-Richtlinie enthält eine Deny-Anweisung, die API-Aufrufe einschränkt, die nicht sicher sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Schlüsselrichtlinie.	1. Wählen Sie in der AWS-CloudFormation Konsole Stacks aus, wählen Sie den Namen des Stacks aus, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und wählen Sie dann In Designer anzeigen aus. 2. Ändern Sie die KMS-Ressource der Vorlage so, dass sie die Schlüsselrichtlinie enthält, die es Administratoren ermöglicht, den CMK zu verwalten. 3. Wählen Sie Stack erstellen, wählen Sie Weiter und schließen Sie dann den Assistenten entsprechend Ihren Anforderungen ab. Weitere Informationen dazu finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS und Schlüsseladministratoren die Verwaltung des CMK erlauben in der AWS KMS-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Tags auf Ressourcenebene hinzu.	1. Wählen Sie in der AWS-CloudFormation Konsole Stacks aus, wählen Sie den Namen des Stacks aus, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und wählen Sie dann In Designer anzeigen aus.
	2. Fügen Sie dem `Properties` Abschnitt Amazon S3-Ressourcen der Vorlage den folgenden Codeausschnitt hinzu, wählen Sie dann Stack erstellen und schließen Sie den Assistenten ab:
	`Tags:`
	`  - Key: createdBy`
	`  Value: Cloudformation`
		AWS DevOps

Zugehörige Ressourcen

- Integrieren vorhandener Ressourcen in die AWS CloudFormation -Verwaltung
- AWS re:Invent 2017: Detaillierter Einblick in AWS CloudFormation (Video)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Mehr Muster

- Zugreifen auf einen Bastion-Host mithilfe von Session Manager und Amazon EC2 Instance Connect
- Zuordnen eines AWS- CodeCommit Repositorys in einem AWS-Konto zu SageMaker Studio in einem anderen Konto
- Automatisieren des Hinzufügens oder Aktualisierens von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie das Training und die Bereitstellung von Amazon Lookout for Vision zur Erkennung von Anomalien
- Automatisieren der Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation
- Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisches Erstellen eines RFC in AMS mit Python
- ???
- Erstellen Sie einen Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Verketten von AWS-Services mithilfe eines Serverless-Ansatzes
- EC2-Instances beim Start auf obligatorische Tags überprüfen
- Konfiguration von Veritas NetBackup für VMware Cloud on AWS
- Herstellen einer Verbindung mit einer Amazon EC2-Instance mithilfe von Session Manager
- ???
- ???
- Erstellen von Alarmen für benutzerdefinierte Metriken mithilfe der Amazon CloudWatch - Anomalieerkennung
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2-Instances
- Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte
- Automatisches Erstellen von Tag-basierten CloudWatch Amazon-Dashboards
- Bereitstellen einer geclusterten Anwendung in Amazon ECS mithilfe von AWS Copilot
- Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront
- Bereitstellen und Debuggen von Amazon-EKS-Clustern

- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform
- Bereitstellen von Containern mithilfe von Elastic Beanstalk
- Bereitstellen von Lambda-Funktionen mit Container-Images
- Dokumentieren Sie institutionelles Wissen anhand von Spracheingaben mithilfe von Amazon Bedrock und Amazon Transcribe
- Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen
- Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität
- Entdecken Sie die Full-Stack-Entwicklung von cloudnativen Webanwendungen mit Green Boost
- Exportieren von Amazon RDS for SQL Server-Tabellen in einen S3-Bucket mithilfe von AWS DMS
- Generieren Sie personalisierte und neu eingestufte Empfehlungen mit Amazon Personalize
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Amazon SNS-Benachrichtigungen abrufen, wenn sich der Schlüsselstatus eines AWS KMS-Schlüssels ändert
- ???
- Identifizieren und warnen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS-Schlüssel verschlüsselt sind
- Implementieren Sie das Serverless-Saga-Muster mithilfe von AWS Step Functions
- Verbessern Sie die betriebliche Leistung, indem Sie Amazon DevOps Guru über mehrere AWS-Regionen, Konten und OUs hinweg mit dem AWS-CDK aktivieren
- Aufnehmen und Migrieren von EC2-Windows-Instances in ein AWS Managed Services-Konto
- Verwalten von AWS Service Catalog-Produkten in mehreren AWS-Konten und AWS-Regionen
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie DNS-Datensätze in großen Mengen in eine privat gehostete Zone von Amazon Route 53
- Migrieren von Oracle 8i oder 9i zu Amazon RDS für Oracle mit SharePlex und AWS DMS
- Überwachen Sie ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand
- Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung
- Überwachen von ElastiCache Clustern für Sicherheitsgruppen
- Replizieren von Mainframe-Datenbanken in AWS mithilfe von Precisely Connect

- Richten Sie die CloudFormation AWS-Drift-Erkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein
- Strukturieren eines Python-Projekts in hexaffinaler Architektur mit AWS Lambda
- Mandanten-Onboarding in SaaS-Architektur für das Silomodell mit C# und AWS CDK
- Aktualisieren von AWS CLI-Anmeldeinformationen von AWS IAM Identity Center mithilfe von PowerShell
- Verwenden von Terraform zum automatischen Aktivieren von Amazon GuardDuty für eine Organisation
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen

Container und Microservices

Themen

- Generieren Sie eine statische ausgehende IP-Adresse mithilfe einer Lambda-Funktion, Amazon VPC und einer serverlosen Architektur
- Installieren des SSM-Agenten auf Amazon-EKS-Worker-Knoten mithilfe von Kubernetes DaemonSet
- Installieren Sie den SSM-Agenten und - CloudWatch Agenten auf Amazon-EKS-Worker-Knoten mit preBootstrapCommands
- Von AWS App2Container generierte Docker-Images optimieren
- Platzieren Sie Kubernetes-Pods auf Amazon EKS mithilfe von Knotenaffinität, Taints und Toleranzen
- Replizieren Sie gefilterte Amazon ECR-Container-Images über Konten oder Regionen hinweg
- Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern
- Ausführen von Amazon-ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere
- Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 EC2-Linux-Instance aus
- Ausführen von nachrichtengesteuerten Workloads in großem Umfang mithilfe von AWS Fargate
- Führen Sie zustandsbehaftete Workloads mit persistenter Datenspeicherung aus, indem Sie Amazon EFS auf Amazon EKS mit AWS Fargate verwenden
- Mehr Muster

Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu

Erstellt von Kirankumar Chandrashekar (AWS)

Umwelt: Produktion	Technologien: Container und Mikroservices; Netzwerke ; Sicherheit, Identität, Compliance; Web- und mobile Apps	Arbeitslast: Alle anderen Workloads
AWS-Services: Amazon EC2; Amazon EC2 Auto Scaling; Amazon EC2 Container Registry; Amazon EFS; Amazon RDS; Amazon VPC; Amazon ECS; Elastic Load Balancing (ELB); AWS Lambda		

Übersicht

Dieses Muster beschreibt, wie Sie eine Docker-Container-Anwendung privat auf Amazon Elastic Container Service (Amazon ECS) hinter einem Network Load Balancer hosten und mithilfe von AWS auf die Anwendung zugreifen. PrivateLink Sie können dann ein privates Netzwerk verwenden, um sicher auf Dienste in der Amazon Web Services (AWS) Cloud zuzugreifen. Amazon Relational Database Service (Amazon RDS) hostet die relationale Datenbank für die Anwendung, die auf Amazon ECS mit hoher Verfügbarkeit (HA) ausgeführt wird. Amazon Elastic File System (Amazon EFS) wird verwendet, wenn die Anwendung persistenten Speicher benötigt.

Der Amazon ECS-Service, auf dem die Docker-Anwendungen ausgeführt werden, mit einem Network Load Balancer am Frontend kann mit einem Virtual Private Cloud (VPC) -Endpunkt für den Zugriff über AWS verknüpft werden. PrivateLink Dieser VPC-Endpunktdienst kann dann mit anderen VPCs gemeinsam genutzt werden, indem deren VPC-Endpunkte verwendet werden.

Sie können auch AWS Fargate anstelle einer Amazon EC2 Auto Scaling Scaling-Gruppe verwenden. Weitere Informationen finden Sie unter Privaten Zugriff auf Containeranwendungen auf Amazon ECS mithilfe von AWS Fargate PrivateLink, AWS und einem Network Load Balancer.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows
- Eine Anwendung, die auf Docker läuft

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon RDS
- Amazon-Simple-Storage-Service (Amazon-S3)
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer

- VPC

Automatisierung und Skalierung

- Sie können AWS verwenden CloudFormation, um dieses Muster mithilfe von Infrastructure as Code zu erstellen.

Tools

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud.
- Amazon EC2 Auto Scaling — Amazon EC2 Auto Scaling hilft Ihnen sicherzustellen, dass Ihnen die richtige Anzahl von Amazon EC2 EC2-Instances zur Verfügung steht, um die Last für Ihre Anwendung zu bewältigen.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Stoppen und Verwalten von Containern in einem Cluster vereinfacht.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter AWS-Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- AWS Lambda — Lambda ist ein Rechenservice zum Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.
- AWS Secrets Manager — Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Kennwörtern, zu ersetzen, indem es einen API-Aufruf an Secrets Manager bereitstellt, um das Geheimnis programmgesteuert abzurufen.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.

- Elastic Load Balancing — Elastic Load Balancing verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele, wie Amazon EC2 EC2-Instances, Container und IP-Adressen, in mehreren Availability Zones.
- Docker — Docker hilft Entwicklern dabei, jede Anwendung als leichten, portablen und autarken Container zu packen, zu versenden und auszuführen.

Epen

Netzwerkkomponenten erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. Wählen Sie Create VPC und dann VPC and more aus. 2. Geben Sie einen Namen für Ihre VPC ein und wählen Sie einen geeigneten CIDR-Blockbereich aus. 3. Geben Sie zwei Availability Zones, zwei öffentliche Subnetze und vier private Subnetze an. Zwei private Subnetze sind für Amazon ECS-Aufgaben und zwei private Subnetze für Amazon RDS-Datenbanken vorgesehen. 4. Geben Sie ein NAT-Gateway für jede Availability Zone an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie VPC erstellen aus.	

Erstellen Sie die Load Balancer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	1. Öffnen Sie die Amazon EC2 EC2-Konsole und wählen Sie die AWS-Region aus, die Ihre VPC enthält. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Network Load Balancer und dann Create aus. 4. Konfigurieren Sie auf der Seite Load Balancer konfigurieren Ihren Network Load Balancer und Listener. Wichtig: Stellen Sie sicher, dass Sie das Schema Ihres Network Load Balancers als Intern auswählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instance oder IP als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrie ren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Load Balancer.	1. Wählen Sie auf der Amazon EC2 EC2-Konsole dieselbe Region aus, in der sich Ihre VPC befindet. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Application Load Balancer und dann Create. 4. Konfigurieren Sie Ihren Application Load Balancer und seinen Listener. Wichtig: Stellen Sie sicher, dass Sie das Schema Ihres Application Load Balancers als Intern auswählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren Instance oder IP als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrieren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen.	Cloud-Administrator

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	1. Öffnen Sie die Amazon EFS-Konsole und wählen Sie Create file system aus. 2. Geben Sie im Dialogfeld Dateisystem erstellen einen Namen für Ihr Dateisyst em ein und wählen Sie Ihre VPC aus. 3. Wählen Sie Erstellen, um das Dateisystem zu erstellen. 4. Richten Sie Ihr Amazon EFS-Dateisystem ein und konfigurieren Sie es.	Cloud-Administrator
Mounten Sie Ziele für die Subnetze.	1. Kehren Sie zur Amazon EFS-Konsole zurück und wählen Sie Dateisysteme. Auf der Seite Dateisyst eme werden die Amazon EFS-Dateisysteme in Ihrem Konto angezeigt. 2. Wählen Sie das Dateisyst em aus, das Sie erstellt haben, und wählen Sie Verwalten, um die Availabil ity Zones anzuzeigen. Um ein Mount-Ziel hinzuzufü gen, wählen Sie Mount-Zie l hinzufügen und fügen Sie die vier privaten Subnetze	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hinzu, die Sie erstellt haben.	
Stellen Sie sicher, dass die Subnetze als Ziele bereitgestellt sind.	1. Wählen Sie in der Amazon EFS-Konsole Dateisysteme aus. 2. Wählen Sie Netzwerk aus, um die Liste der vorhandenen Mount-Ziele anzuzeigen. Stellen Sie sicher, dass diese die vier Subnetze enthalten, die Sie erstellt haben.	Cloud-Administrator

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie bei Bedarf einen S3-Bucket, um die statischen Ressourcen Ihrer Anwendung zu speichern.	Cloud-Administrator

Ein Secrets Manager Manager-Geheimnis erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS-KMS-Schlüssel, um das Secrets Manager Manager-Geheimnis zu verschlüsseln.	Öffnen Sie die AWS Key Management Service (AWS KMS) -Konsole und erstellen Sie einen KMS-Schlüssel.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Secrets Manager Manager-Geheimnis, um das Amazon RDS-Passwort zu speichern.	1. Öffnen Sie die AWS Secrets Manager Manager-Konsole und erstellen Sie ein neues Geheimnis, indem Sie Neues Geheimnis speichern wählen. 2. Wählen Sie den KMS-Schlüssel aus, den Sie erstellt haben, und speichern Sie Ihr neues Geheimnis.	Cloud-Administrator

Eine Amazon RDS-Instance erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DB-Subnetzgruppe.	1. Öffnen Sie die Amazon RDS-Konsole und wählen Sie Subnetzgruppen. 2. Wählen Sie Create DB Subnet Group und geben Sie einen Namen und eine Beschreibung für Ihre DB-Subnetzgruppe ein. 3. Wählen Sie die VPC aus, die Sie zuvor erstellt haben, und wählen Sie die Availability Zones und Subnetze aus. Wählen Sie die Option Erstellen aus.	Cloud-Administrator
Erstellen Sie eine Amazon RDS-Instance.	Erstellen und konfigurieren Sie eine Amazon RDS-Instance in den privaten Subnetzen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	. Stellen Sie sicher, dass Multi-AZ für HA aktiviert ist.	
Laden Sie Daten in die Amazon RDS-Instance.	Laden Sie die für Ihre Anwendung erforderlichen relationalen Daten in Ihre Amazon RDS-Instance. Dieser Prozess hängt von den Anforderungen Ihrer Anwendung sowie davon ab, wie Ihr Datenbankschema definiert und entworfen ist.	Cloud-Administrator, DBA

Erstellen Sie die Amazon ECS-Komponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen ECS-Cluster.	1. Öffnen Sie die Amazon ECS-Konsole und wählen Sie Clusters. 2. Wählen Sie Cluster erstellen und richten Sie einen ECS-Cluster gemäß Ihren erforderlichen Spezifikationen ein.	Cloud-Administrator
Erstellen Sie die Docker-Images.	Erstellen Sie die Docker-Images, indem Sie den Anweisungen im Abschnitt Verwandte Ressourcen folgen.	Cloud-Administrator
Erstellen Sie Amazon ECR-Repositorys.	1. Wählen Sie auf der Amazon ECR-Konsole Repositories aus.	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Create Repository und geben Sie einen eindeutigen Namen für Ihr Repository ein. 3. Konfigurieren Sie das Repository gemäß Ihren Spezifikationen, einschlie ßlich AWS-KMS-Verschlüss elung, falls erforderlich.	
Authentifizieren Sie Ihren Docker-Client für das Amazon ECR-Repository.	Um Ihren Docker-Client für das Amazon ECR-Repository zu authentifizieren, führen Sie den `aws ecr get-login -password` Befehl „in der AWS-CLI aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Docker-Images in das Amazon ECR-Repository.	1. Identifizieren Sie das Docker-Image, das Sie pushen möchten, und führen Sie den `docker images` Befehl in der AWS-CLI aus. 2. Kennzeichnen Sie Ihr Bild mit der Amazon ECR-Registrierung, dem Repository und der optionalen Kombination aus Image-Tagnamen. 3. Übertragen Sie das Docker-Image, indem Sie den `docker push` Befehl ausführen. 4. Wiederholen Sie diese Schritte für alle erforderlichen Bilder.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon ECS-Aufgabendefinition.	Eine Aufgabendefinition ist erforderlich, um Docker-Container in Amazon ECS auszuführen. 1. Kehren Sie zur Amazon ECS-Konsole zurück, wählen Sie Aufgabend efinitionen und dann Neue Aufgabendefinition erstellen . 2. Wählen Sie auf der Seite „Kompatibilitäten auswählen “ den Starttyp aus, den Ihre Aufgabe verwenden soll, und klicken Sie auf Nächster Schritt. Hilfe beim Einrichten Ihrer Aufgabendefinition finden Sie unter „Eine Aufgabend efinition erstellen“ im Abschnitt Verwandte Ressourcen. Wichtig: Stellen Sie sicher, dass Sie die Docker-Images bereitstellen, die Sie an Amazon ECR übertragen haben.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-ECS-Service.	Erstellen Sie einen Amazon ECS-Service mithilfe des ECS-Clusters, den Sie zuvor erstellt haben. Stellen Sie sicher, dass Sie Amazon EC2 als Starttyp und die im vorherigen Schritt erstellte Aufgabendefinition sowie die Zielgruppe des Application Load Balancer auswählen.	Cloud-Administrator

Eine Amazon EC2 Auto Scaling Scaling-Gruppe erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Startkonf iguration	Öffnen Sie die Amazon EC2 EC2-Konsole und erstellen Sie eine Startkonfiguration. Stellen Sie sicher, dass die Benutzerd aten den Code enthalten, der es den EC2-Instances ermöglicht, dem gewünschten ECS-Cluster beizutreten. Ein Beispiel für den erforderlichen Code finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator
Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-G ruppe.	Kehren Sie zur Amazon EC2 EC2-Konsole zurück und wählen Sie unter Auto Scaling die Option Auto Scaling Scaling-Gruppen aus. Richten Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein. Stellen Sie sicher, dass Sie die privaten Subnetze auswählen und die Konfigura tion starten, die Sie zuvor erstellt haben.	

AWS einrichten PrivateLink

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den PrivateLink AWS-Endpunkt ein.	1. Erstellen Sie auf der Amazon VPC-Konsole einen PrivateLink AWS-Endpunkt. 2. Ordnen Sie diesen Endpunkt dem Network Load Balancer zu, der die auf Amazon ECS gehostete Anwendung privat für Kunden verfügbar macht. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator

Erstellen eines VPC-Endpunkts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt.	Erstellen Sie einen VPC-Endpunkt für den PrivateLink AWS-Endpunkt, den Sie zuvor erstellt haben. Der vollquali	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	fizierte Domainname (FQDN) des VPC-Endpunkts zeigt auf den PrivateLink AWS-Endpunkt-FQDN. Dadurch wird eine elastic network interface zum VPC-Endpunktdienst erstellt, auf die die DNS-Endpunkte zugreifen können.	

So erstellen Sie die Lambda-Funktion:

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	Erstellen Sie auf der AWS Lambda Lambda-Konsole eine Lambda-Funktion, um die IP-Adressen des Application Load Balancer als Ziele für den Network Load Balancer zu aktualisieren. Weitere Informationen dazu finden Sie im Blogbeitrag „Statische IP-Adressen für Application Load Balancers verwenden “ im Abschnitt Verwandte Ressourcen.	App-Developer

Zugehörige Ressourcen

Erstellen Sie die Load Balancer:

- Einen Network Load Balancer erstellen
- Erstellen Sie einen Application Load Balancer

Erstellen Sie ein Amazon EFS-Dateisystem:

- Erstellen Sie ein Amazon EFS-Dateisystem
- Bereitstellungsziele in Amazon EFS erstellen

Erstellen Sie einen S3-Bucket:

- Erstellen Sie einen S3-Bucket

Erstellen Sie ein Secrets Manager Manager-Geheimnis:

- Schlüssel in AWS KMS erstellen
- Erstellen Sie ein Geheimnis in AWS Secrets Manager

Erstellen Sie eine Amazon RDS-Instance:

- Eine Amazon RDS-DB-Instance erstellen

Erstellen Sie die Amazon ECS-Komponenten:

- Erstellen Sie einen Amazon ECS-Cluster
- Erstellen Sie ein Docker-Image
- Erstellen Sie ein Amazon ECR-Repository
- Authentifizieren Sie Docker mit dem Amazon ECR-Repository
- Ein Bild in ein Amazon ECR-Repository übertragen
- Amazon ECS-Aufgabendefinition erstellen
- Einen Amazon ECS-Service erstellen

Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe:

- Erstellen Sie eine Startkonfiguration
- Erstellen einer Auto-Scaling-Gruppe mithilfe einer Startkonfiguration
- Bootstrap-Container-Instances mit Amazon EC2 EC2-Benutzerdaten

AWS einrichten PrivateLink:

- VPC-Endpunktdienste (AWS PrivateLink)

Erstellen Sie einen VPC-Endpunkt:

- Schnittstelle VPC-Endpunkte (AWS) PrivateLink

Erstellen Sie die Lambda-Funktion:

- Erstellen Sie eine Lambda-Funktion

Andere Ressourcen:

- Verwendung statischer IP-Adressen für Application Load Balancer
- Sicherer Zugriff auf Services über AWS PrivateLink

Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden

Erstellt von Kirankumar Chandrashekar (AWS)

Umwelt: Produktion	Technologien: Container und Mikroservices; Netzwerke ; Sicherheit, Identität, Compliance; Web- und mobile Apps	Arbeitslast: Alle anderen Workloads
AWS-Services: Amazon EC2 Container Registry; Amazon ECS; Amazon EFS; Amazon RDS; Amazon VPC; Elastic Load Balancing (ELB); AWS Lambda		

Übersicht

Dieses Muster beschreibt, wie Sie eine Docker-Container-Anwendung privat in der Amazon Web Services (AWS) -Cloud hosten, indem Sie Amazon Elastic Container Service (Amazon ECS) mit einem AWS Fargate-Starttyp hinter einem Network Load Balancer verwenden und mithilfe von AWS auf die Anwendung zugreifen. PrivateLink Amazon Relational Database Service (Amazon RDS) hostet die relationale Datenbank für die Anwendung, die auf Amazon ECS mit hoher Verfügbarkeit (HA) ausgeführt wird. Sie können Amazon Elastic File System (Amazon EFS) verwenden, wenn die Anwendung persistenten Speicher benötigt.

Dieses Muster verwendet einen Fargate-Starttyp für den Amazon ECS-Service, auf dem die Docker-Anwendungen ausgeführt werden, mit einem Network Load Balancer am Frontend. Es kann dann mit einem Virtual Private Cloud (VPC) -Endpunkt für den Zugriff über AWS PrivateLink verknüpft werden. Dieser VPC-Endpunktdienst kann dann mit anderen VPCs gemeinsam genutzt werden, indem deren VPC-Endpunkte verwendet werden.

Sie können Fargate mit Amazon ECS verwenden, um Container auszuführen, ohne Server oder Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Sie können anstelle von Fargate auch eine Amazon EC2 Auto Scaling Scaling-Gruppe verwenden. Weitere Informationen finden Sie unter Privaten Zugriff auf Containeranwendungen auf Amazon ECS mithilfe von AWS PrivateLink und einem Network Load Balancer.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows
- Eine Anwendung, die auf Docker läuft

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon EFS
- Amazon RDS
- Amazon-Simple-Storage-Service (Amazon-S3)
- AWS Fargate
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer

- Network Load Balancer
- VPC

Automatisierung und Skalierung

- Sie können AWS verwenden CloudFormation, um dieses Muster mithilfe von Infrastructure as Code zu erstellen.

Tools

- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Stoppen und Verwalten von Containern in einem Cluster vereinfacht.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter AWS-Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- AWS Fargate — AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen, ohne Server oder Cluster von Amazon EC2 EC2-Instances verwalten zu müssen.
- AWS Lambda — Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.
- AWS Secrets Manager — Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.

- Elastic Load Balancing — Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele, wie EC2-Instances, Container und IP-Adressen, in mehreren Availability Zones.
- Docker — Docker hilft Entwicklern dabei, jede Anwendung als leichten, portablen und autarken Container einfach zu packen, zu versenden und auszuführen.

Epen

Netzwerkkomponenten erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. Wählen Sie Create VPC und dann VPC and more aus. 2. Geben Sie einen Namen für Ihre VPC ein und wählen Sie einen geeigneten CIDR-Blockbereich aus. 3. Geben Sie zwei Availability Zones, zwei öffentliche Subnetze und vier private Subnetze an. Zwei private Subnetze sind für Amazon ECS-Aufgaben und zwei private Subnetze für Amazon RDS-Datenbanken vorgesehen. 4. Geben Sie ein NAT-Gateway für jede Availability Zone an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie VPC erstellen aus.	

Erstellen Sie die Load Balancer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	1. Öffnen Sie die Amazon EC2 EC2-Konsole und wählen Sie die AWS-Region aus, die Ihre VPC enthält. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Network Load Balancer und dann Create aus. 4. Konfigurieren Sie auf der Seite Load Balancer konfigurieren Ihren Network Load Balancer und Listener. Wichtig: Stellen Sie sicher, dass Sie das Schema Ihres Network Load Balancers als Intern auswählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren IP	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrieren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt Verwandte Ressourcen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Load Balancer.	1. Wählen Sie auf der Amazon EC2 EC2-Konsole dieselbe Region aus, in der sich Ihre VPC befindet. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Application Load Balancer und dann Create aus. 4. Konfigurieren Sie Ihren Application Load Balancer und seinen Listener. Wichtig: Stellen Sie sicher, dass Sie das Schema Ihres Application Load Balancers als Intern auswählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren IP als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrieren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen.	Cloud-Administrator

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	1. Öffnen Sie die Amazon EFS-Konsole und wählen Sie Create file system aus. 2. Geben Sie im Dialogfeld Dateisystem erstellen einen Namen für Ihr Dateisyst em ein und wählen Sie Ihre VPC aus. 3. Wählen Sie Erstellen, um das Dateisystem zu erstellen. 4. Richten Sie Ihr Amazon EFS-Dateisystem ein und konfigurieren Sie es.	Cloud-Administrator
Mounten Sie Ziele für die Subnetze.	1. Kehren Sie zur Amazon EFS-Konsole zurück und wählen Sie Dateisysteme. Auf der Seite Dateisyst eme werden die Amazon EFS-Dateisysteme in Ihrem Konto angezeigt. 2. Wählen Sie das Dateisyst em aus, das Sie erstellt haben, und wählen Sie Verwalten, um die Availabil ity Zone anzuzeigen. 3. Um ein Mount-Ziel hinzuzufügen, wählen Sie Mount-Ziel hinzufügen und fügen Sie die vier privaten	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Subnetze hinzu, die Sie erstellt haben.	
Stellen Sie sicher, dass die Subnetze als Ziele bereitgestellt sind.	1. Wählen Sie in der Amazon EFS-Konsole Dateisysteme aus. 2. Wählen Sie Netzwerk aus, um die Liste der vorhandenen Mount-Ziele anzuzeigen. Stellen Sie sicher, dass diese die vier Subnetze enthalten, die Sie erstellt haben.	Cloud-Administrator

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie bei Bedarf einen S3-Bucket, um die statischen Ressourcen Ihrer Anwendung zu speichern.	Cloud-Administrator

Erstellen Sie ein Secrets Manager Manager-Geheimnis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS-KMS-Schlüssel, um das Secrets Manager Manager-Geheimnis zu verschlüsseln.	Öffnen Sie die AWS Key Management Service (AWS KMS) -Konsole und erstellen Sie einen KMS-Schlüssel.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Secrets Manager Manager-Geheimnis, um das Amazon RDS-Passwort zu speichern.	1. Öffnen Sie die AWS Secrets Manager Manager-Konsole und erstellen Sie ein neues Geheimnis, indem Sie Neues Geheimnis speichern wählen. 2. Wählen Sie den KMS-Schlüssel aus, den Sie erstellt haben, und speichern Sie Ihr neues Geheimnis.	Cloud-Administrator

Eine Amazon RDS-Instance erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DB-Subnetzgruppe.	1. Öffnen Sie die Amazon RDS-Konsole und wählen Sie Subnetzgruppen aus. 2. Wählen Sie Create DB Subnet Group und geben Sie einen Namen und eine Beschreibung für Ihre DB-Subnetzgruppe ein. 3. Wählen Sie die VPC aus, die Sie zuvor erstellt haben, und wählen Sie die Availability Zones und Subnetze aus. Wählen Sie die Option Erstellen aus.	Cloud-Administrator
Erstellen Sie eine Amazon RDS-Instance.	Erstellen und konfigurieren Sie eine Amazon RDS-Instance in den privaten Subnetzen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	. Stellen Sie sicher, dass Multi-AZ für Hochverfügbarkeit (HA) aktiviert ist.	
Laden Sie Daten in die Amazon RDS-Instance.	Laden Sie die für Ihre Anwendung erforderlichen relationalen Daten in Ihre Amazon RDS-Instance. Dieser Prozess hängt von den Anforderungen Ihrer Anwendung sowie davon ab, wie Ihr Datenbankschema definiert und entworfen ist.	DBA

Erstellen Sie die Amazon ECS-Komponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen ECS-Cluster.	1. Öffnen Sie die Amazon ECS-Konsole und wählen Sie Clusters. 2. Wählen Sie Cluster erstellen und richten Sie einen ECS-Cluster gemäß Ihren erforderlichen Spezifikationen ein.	Cloud-Administrator
Erstellen Sie die Docker-Images.	Erstellen Sie die Docker-Images, indem Sie den Anweisungen im Abschnitt Verwandte Ressourcen folgen.	Cloud-Administrator
Erstellen Sie ein Amazon-ECR-Repository.	1. Öffnen Sie die Amazon ECR-Konsole und wählen Sie Repositories.	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Create Repository und geben Sie einen eindeutigen Namen für Ihr Repository ein. 3. Konfigurieren Sie das Repository gemäß Ihren Spezifikationen, einschlie ßlich AWS-KMS-Verschlüss elung, falls erforderlich.	
Übertragen Sie die Docker-Images in das Amazon ECR-Repository.	1. Identifizieren Sie das Docker-Image, das Sie pushen möchten, und führen Sie den `docker images` Befehl in der AWS-CLI aus. 2. Kennzeichnen Sie Ihr Bild mit der Amazon ECR-Regis trierung, dem Repositor y und der optionalen Kombination aus Image-Tagnamen. 3. Übertragen Sie das Docker-Image, indem Sie den `docker push` Befehl ausführen. 4. Wiederholen Sie diese Schritte für alle erforderl ichen Bilder.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon ECS-Aufgabendefinition.	Eine Aufgabendefinition ist erforderlich, um Docker-Container in Amazon ECS auszuführen. 1. Kehren Sie zur Amazon ECS-Konsole zurück, wählen Sie Aufgabend efinitionen und dann Neue Aufgabendefinition erstellen . 2. Wählen Sie auf der Seite „Kompatibilitäten auswählen “ den Starttyp aus, den Ihre Aufgabe verwenden soll, und klicken Sie auf Nächster Schritt. Hilfe beim Einrichten Ihrer Aufgabendefinition finden Sie unter „Eine Aufgabend efinition erstellen“ im Abschnitt Verwandte Ressourcen. Wichtig: Stellen Sie sicher, dass Sie die Docker-Images bereitstellen, die Sie an Amazon ECR übertragen haben.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen ECS-Service und wählen Sie Fargate als Starttyp.	1. Erstellen Sie einen Amazon ECS-Service mithilfe des ECS-Clusters, den Sie zuvor erstellt haben. Stellen Sie sicher, dass Sie Fargate als Starttyp wählen. 2. Wählen Sie die im vorherigen Schritt erstellte Aufgabendefinition und wählen Sie die Zielgrupp e des Application Load Balancer aus.	Cloud-Administrator

AWS einrichten PrivateLink

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den PrivateLink AWS-Endpunkt ein.	1. Öffnen Sie die Amazon VPC-Konsole und erstellen Sie einen PrivateLink AWS-Endpunkt. 2. Ordnen Sie diesen Endpunkt dem Network Load Balancer zu, der die auf Amazon ECS gehostete Anwendung privat für Kunden verfügbar macht. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator

Erstellen eines VPC-Endpunkts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt.	Erstellen Sie einen VPC-Endpunkt für den PrivateLink AWS-Endpunkt, den Sie zuvor erstellt haben. Der vollquali fizierte Domainname (FQDN) des VPC-Endpunkts zeigt auf den PrivateLink AWS-Endpu nkt-FQDN. Dadurch wird eine elastic network interface zum VPC-Endpunktdienst erstellt, auf die die Domain Name Service-Endpunkte zugreifen können.	Cloud-Administrator

So erstellen Sie die Lambda-Funktion:

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	Öffnen Sie die Lambda-Ko nsole und erstellen Sie eine Lambda-Funktion, um die IP-Adressen des Application Load Balancer als Ziele für den Network Load Balancer zu aktualisieren. Weitere Informationen dazu finden Sie im Blogbeitrag „Statisch e IP-Adressen für Application Load Balancers verwenden “ im Abschnitt Verwandte Ressourcen.	App-Developer

Zugehörige Ressourcen

Erstellen Sie die Load Balancer:

- Einen Network Load Balancer erstellen
- Erstellen Sie einen Application Load Balancer

Erstellen Sie ein Amazon EFS-Dateisystem:

- Erstellen Sie ein Amazon EFS-Dateisystem
- Bereitstellungsziele in Amazon EFS erstellen

Erstellen Sie einen S3-Bucket:

- Erstellen Sie einen S3-Bucket

Erstellen Sie ein Secrets Manager Manager-Geheimnis:

- Schlüssel in AWS KMS erstellen
- Erstellen Sie ein Geheimnis in AWS Secrets Manager

Erstellen Sie eine Amazon RDS-Instance:

- Eine Amazon RDS-DB-Instance erstellen

Erstellen Sie die Amazon ECS-Komponenten:

- Erstellen Sie einen Amazon ECS-Cluster
- Erstellen Sie ein Docker-Image
- Erstellen Sie ein Amazon ECR-Repository
- Authentifizieren Sie Docker mit dem Amazon ECR-Repository
- Ein Bild in ein Amazon ECR-Repository übertragen
- Amazon ECS-Aufgabendefinition erstellen
- Erstellen Sie einen Amazon ECS-Service

Richten Sie AWS ein PrivateLink:

- VPC-Endpunktdienste (AWS PrivateLink)

Erstellen Sie einen VPC-Endpunkt:

- Schnittstelle VPC-Endpunkte (AWS) PrivateLink

Erstellen Sie die Lambda-Funktion:

- Erstellen Sie eine Lambda-Funktion

Andere Ressourcen:

- Verwendung statischer IP-Adressen für Application Load Balancer
- Sicherer Zugriff auf Services über AWS PrivateLink

Greifen Sie mit AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon EKS zu

Erstellt von Kirankumar Chandrashekar (AWS)

Umwelt: Produktion	Technologien: Container und Mikroservices DevOps; Modernisierung; Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon EKS; Amazon VPC		

Übersicht

Dieses Muster beschreibt, wie Sie eine Docker-Container-Anwendung privat auf Amazon Elastic Kubernetes Service (Amazon EKS) hinter einem Network Load Balancer hosten und mithilfe von AWS auf die Anwendung zugreifen. PrivateLink Sie können dann ein privates Netzwerk verwenden, um sicher auf Dienste in der Amazon Web Services (AWS) Cloud zuzugreifen.

Der Amazon EKS-Cluster, auf dem die Docker-Anwendungen ausgeführt werden, mit einem Network Load Balancer am Frontend kann mit einem Virtual Private Cloud (VPC) -Endpunkt für den Zugriff über AWS verknüpft werden. PrivateLink Dieser VPC-Endpunktdienst kann dann mit anderen VPCs gemeinsam genutzt werden, indem deren VPC-Endpunkte verwendet werden.

Das in diesem Muster beschriebene Setup ist eine sichere Methode, um den Anwendungszugriff zwischen VPCs und AWS-Konten gemeinsam zu nutzen. Es sind keine speziellen Konnektivitäts- oder Routing-Konfigurationen erforderlich, da die Verbindung zwischen den Kunden- und Anbieterkonten auf dem globalen AWS-Backbone erfolgt und nicht das öffentliche Internet durchquert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows.
- Eine Anwendung, die auf Docker läuft.

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows.
- Ein vorhandener Amazon EKS-Cluster mit markierten privaten Subnetzen, der für das Hosten von Anwendungen konfiguriert ist. Weitere Informationen finden Sie unter Subnet-Tagging in der Amazon EKS-Dokumentation.
- Kubectl, installiert und konfiguriert für den Zugriff auf Ressourcen in Ihrem Amazon EKS-Cluster. Weitere Informationen finden Sie unter Installation von kubectl in der Amazon EKS-Dokumentation.

Architektur

Technologie-Stack

- Amazon EKS
- AWS PrivateLink
- Network Load Balancer

Automatisierung und Skalierung

- Kubernetes-Manifeste können in einem Git-basierten Repository (z. B. auf AWS CodeCommit) verfolgt und verwaltet und mithilfe von Continuous Integration and Continuous Delivery (CI/CD) in AWS bereitgestellt werden. CodePipeline
- Sie können AWS verwenden CloudFormation , um dieses Muster mithilfe von Infrastructure as Code (IaC) zu erstellen.

Tools

- AWS CLI — AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Elastic Load Balancing — Elastic Load Balancing verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele, wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen, in einer oder mehreren Availability Zones.

- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.
- Kubectl — Kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.

Epen

Stellen Sie die Kubernetes-Bereitstellungs- und Service-Manifestdateien bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Manifestdatei für die Kubernetes-Bereitstellung.	Erstellen Sie eine Bereitstellungsmanifestdatei, indem Sie die folgende Beispieldatei Ihren Anforderungen entsprechend ändern.
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: sample-app`
	`spec:`
	`  replicas: 3`
	`  selector:`
	`  matchLabels:`
	`  app: nginx`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: nginx`
	`  spec:`
	`  containers:`
	`  - name: nginx`
	`  image:`
	`public.ecr.aws/z9d2n7e1/nginx:1.19.5`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>ports:
	  - name: http
	  container
	Port: 80</pre>
	Hinweis: Dies ist eine NGINX-Beispielkonfigurationsdatei, die mithilfe des NGINX-Docker-Images bereitgestellt wird. Weitere Informationen finden Sie in der Docker-Dokumentation unter So verwenden Sie das offizielle NGINX-Docker-Image.	

Stellen Sie die Kubernetes-Bereitstellungsmanifestdatei bereit.	Führen Sie den folgenden Befehl aus, um die Bereitstellungsmanifestdatei auf Ihren Amazon EKS-Cluster anzuwenden: `kubectl apply –f <your_deployment_file_name>`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Manifestdatei des Kubernetes-Dienstes.	Erstellen Sie eine Dienstmanifestdatei, indem Sie die folgende Beispieldatei Ihren Anforderungen entsprechend ändern.
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: sample-service`
	`  annotations:`
	`  service.beta.kubernetes.io/aws-load-balancer-type: nlb`
	`  service.beta.kubernetes.io/aws-load-balancer-internal: "true"`
	`spec:`
	`  ports:`
	`  - port: 80`
	`  targetPort: 80`
	`  protocol: TCP`
	`  type: LoadBalancer`
	`  selector:`
	`  app: nginx`
	
	Wichtig: Stellen Sie sicher, dass Sie Folgendes angegeben haben`annotations`, um einen internen Network Load Balancer zu definieren:
	
	`service.beta.kubernetes.io/aws-load-balancer-type: nlb`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`service.beta.kubernetes.io/aws-load-balancer-internal: "true"`	
Stellen Sie die Manifestdatei des Kubernetes-Dienstes bereit.	Führen Sie den folgenden Befehl aus, um die Service-Manifest-Datei auf Ihren Amazon EKS-Cluster anzuwenden: `kubectl apply -f <your_service_file_name>`	DevOps Ingenieur

Erstellen Sie die Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich den Namen des Network Load Balancers.	Führen Sie den folgenden Befehl aus, um den Namen des Network Load Balancer abzurufen: `kubectl get svc sample-service -o wide` Notieren Sie sich den Namen des Network Load Balancers, der für die Erstellung eines PrivateLink AWS-Endpunkts erforderlich ist.	DevOps Ingenieur
Erstellen Sie einen PrivateLink AWS-Endpunkt.	Melden Sie sich bei der AWS-Managementkonsole	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an, öffnen Sie die Amazon VPC-Konsole und erstellen Sie dann einen PrivateLink AWS-Endpunkt. Ordnen Sie diesen Endpunkt dem Network Load Balancer zu, damit die Anwendung privat für Kunden verfügbar ist. Weitere Informationen finden Sie unter VPC Endpoint Services (AWS PrivateLink) in der Amazon VPC-Dokumentation. Wichtig: Wenn das Verbraucherkonto Zugriff auf die Anwendung benötigt, muss die AWS-Konto-ID des Verbraucherkontos zur Liste der zulässigen Prinzipale für die PrivateLink AWS-Endpunktkonfiguration hinzugefügt werden. Weitere Informationen finden Sie unter Hinzufügen und Entfernen von Berechtigungen für Ihren Endpunkt-Service in der Amazon VPC-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt.	Wählen Sie in der Amazon VPC-Konsole Endpoint Services und dann Create Endpoint Service aus. Erstellen Sie einen VPC-Endpunkt für den PrivateLink AWS-Endpunkt. Der vollqualifizierte Domainname (FQDN) des VPC-Endpunkts verweist auf den FQDN für den AWS-Endpunkt. PrivateLink Dadurch wird eine elastic network interface zum VPC-Endpunktdienst erstellt, auf die die DNS-Endpunkte zugreifen können.	Cloud-Administrator

Zugehörige Ressourcen

- Verwenden Sie das offizielle NGINX Docker-Image
- Netzwerklastenausgleich auf Amazon EKS
- VPC-Endpunktdienste (AWS PrivateLink) erstellen
- Hinzufügen und Entfernen von Berechtigungen für Ihren Endpunkt-Service

Aktivieren von mTLS in AWS App Mesh mit AWS Private CA in Amazon EKS

Erstellt von Omar Kahil (AWS), Emman Saliu (AWS) und Bolhammad Shahzad (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices	AWS-Services: AWS App Mesh; Amazon EKS; AWS Certificate Manager (ACM)

Übersicht

Dieses Muster zeigt, wie Sie Mutual Transport Layer Security (mTLS) auf Amazon Web Services (AWS) mithilfe von Zertifikaten der AWS Private Certificate Authority (AWS Private CA) in AWS App Mesh implementieren. Es verwendet die Envoy Secret Discovery Service (SDS) API über das Secure Production Identity Framework for Every (SPIFFE). SPIFFE ist ein Open-Source-Projekt der Cloud Native Computing Foundation (CNCF) mit umfassender Community-Unterstützung, das ein differenziertes und dynamisches Workload-Identitätsmanagement bietet. Um SPIFFE-Standards zu implementieren, verwenden Sie die SPIRE SPIFFE-Laufzeitumgebung.

Die Verwendung von mTLS in App Mesh bietet bidirektionale Peer-Authentifizierung, da sie eine Sicherheitsebene über TLS hinzufügt und es Diensten im Mesh ermöglicht, den Client zu überprüfen, der die Verbindung herstellt. Der Client in der Client-Server-Beziehung stellt während der Sitzungsaushandlung auch ein X.509-Zertifikat bereit. Der Server verwendet dieses Zertifikat, um den Client zu identifizieren und zu authentifizieren. Auf diese Weise können Sie überprüfen, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurde und ob es sich um ein gültiges Zertifikat handelt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster mit selbstverwalteten oder verwalteten Knotengruppen
- App-Mesh-Controller, der auf dem Cluster mit aktiviertem SDS bereitgestellt wird
- Ein privates Zertifikat von AWS Certificate Manager (ACM), das von AWS Private CA ausgestellt wurde

Einschränkungen

- SPIRE kann nicht auf AWS Fargate installiert werden, da der SPIRE Agent als Kubernetes ausgeführt werden muss DaemonSet.

Produktversionen

- AWS App Mesh Controller-Diagramm 1.3.0 oder höher

Architektur

Das folgende Diagramm zeigt den EKS-Cluster mit App Mesh in der VPC. Der SPIRE-Server in einem Worker-Knoten kommuniziert mit den SPIRE Agents in anderen Worker-Knoten und mit AWS Private CA. Envoy wird für die mTLS-Kommunikation zwischen den Worker-Knoten des SPIRE Agent verwendet.

Die Abbildung zeigt die folgenden Schritte:

1. Das Zertifikat wird ausgestellt.
2. Fordern Sie die Zertifikatsignierung und das Zertifikat an.

Tools

AWS-Services

- AWS Private CA – AWS Private Certificate Authority (AWS Private CA) ermöglicht die Erstellung von Private Certificate Authority (CA)-Hierarchien, einschließlich Stamm- und untergeordneter CAs, ohne die Investitionen und Wartungskosten für den Betrieb einer On-Premises-CA.
- AWS App Mesh – AWS App Mesh ist ein Service-Mesh, das die Überwachung und Steuerung von Services vereinfacht. App Mesh standardisiert die Kommunikation Ihrer Services und bietet Ihnen konsistente Transparenz und Netzwerkverkehrskontrollen für jeden Service in einer Anwendung.
- Amazon EKS – Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren, betreiben und warten zu müssen.

Andere Tools

- Helm – Helm ist ein Paketmanager für Kubernetes, mit dem Sie Anwendungen auf Ihrem Kubernetes-Cluster installieren und verwalten können. Dieses Muster verwendet Helm, um AWS App Mesh Controller bereitzustellen.
- AWS App Mesh Controller-Diagramm – Das AWS App Mesh Controller-Diagramm wird von diesem Muster verwendet, um AWS App Mesh in Amazon EKS zu aktivieren.

Polen

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie App Mesh mit Amazon EKS ein.	Befolgen Sie die grundlegenden Bereitstellungsschritte, die im Repository bereitgestellt werden.	DevOps Techniker
Installieren Sie SPIRE.	Installieren Sie SPIRE auf dem EKS-Cluster mithilfe von microSD_setup.yaml.	DevOps Techniker
Installieren Sie das AWS Private CA-Zertifikat.	Erstellen und installieren Sie ein Zertifikat für Ihre private Stammzertifizierungsstelle, indem Sie den Anweisungen in der AWS-Dokumentation folgen.	DevOps Techniker
Erteilen Sie Berechtigungen für die Cluster-Knoten-Instance-Rolle.	Um Richtlinien an die Cluster-Knoten-Instance-Rolle anzuhängen, verwenden Sie den Code, der sich im Abschnitt Zusätzliche Informationen befindet.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das SPIRE-Plugin für AWS Private CA hinzu.	Um das Plugin zur SPIRE-Serverkonfiguration hinzuzufügen, verwenden Sie den Code, der sich im Abschnitt Zusätzliche Informationen befindet. Ersetzen Sie den `certificate_authority_arn` Amazon-Ressourcennamen (ARN) durch Ihren privaten CA-ARN. Der verwendete Signaturalgorithmus muss mit dem Signaturalgorithmus auf der privaten CA übereinstimmen. Ersetzen Sie `your_region` durch Ihre AWS-Region. Weitere Informationen zum Plugin finden Sie unter Server-Plugin: UpstreamAuthority "aws_pca"	DevOps Techniker
Aktualisieren Sie bundle.cert.	Nachdem Sie den SPIRE-Server erstellt haben, wird eine `-spire-bundle.yaml` Datei erstellt. Ändern Sie den `bundle.crt` Wert in der `spire-bundle.yaml` Datei von der privaten Zertifizierungsstelle in das öffentliche Zertifikat.	DevOps Techniker

Bereitstellen und Registrieren der Workloads

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie Knoten- und Workload-Einträge bei SPIRE.	Um Knoten und Workload (Services) bei SPIRE Server zu registrieren, verwenden Sie den Code im Repository .	DevOps Techniker
Erstellen Sie ein Mesh in App Mesh mit aktiviertem mTLS.	Erstellen Sie ein neues Mesh in App Mesh mit allen Komponenten für Ihre Microservices-Anwendung (z. B. virtueller Service, virtueller Router und virtuelle Knoten).	DevOps Techniker
Überprüfen Sie die registrierten Einträge.	Sie können die registrierten Einträge für Ihre Knoten und Workloads überprüfen, indem Sie den folgenden Befehl ausführen. `kubectl exec -n spire spire-server-0 -- /opt/spire/bin/spire-server entry show` Dadurch werden die Einträge für die SPIRE-Agenten angezeigt.	DevOps Techniker

Überprüfen des mTLS-Datenverkehrs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den mTLS-Datenverkehr.	1. Senden Sie vom Frontend-Service aus einen HTTP-	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Header an den Backend-Service und überprüfen Sie eine erfolgreiche Antwort mit den Services, die in SPIRE registriert sind.
	2. Für die gegenseitige TLS-Authentifizierung können Sie die `ssl.handshake` Statistik überprüfen, indem Sie den folgenden Befehl ausführen.
	`kubectl exec -it $POD -n $NAMESPACE -c envoy -- curl http://localhost:9901/stats | grep ssl.handshake`
	Nachdem Sie den vorherigen Befehl ausgeführt haben, sollten Sie die Listener-`ssl.handshake` Anzahl sehen, die dem folgenden Beispiel ähnelt:
	`listener.0.0.0.0_15000.ssl.handshake: 2`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass Zertifikate von AWS Private CA ausgestellt werden.	Sie können überprüfen, ob die Plugins korrekt konfiguriert wurden und Zertifikate von Ihrer privaten Upstream-Zertifizierungsstelle ausgestellt werden, indem Sie die Protokolle auf Ihrem SPIRE-Server anzeigen. Führen Sie den folgenden Befehl aus. `kubectl logs spire-server-0 -n spire` Zeigen Sie dann die Protokolle an, die erstellt werden. Dieser Code geht davon aus, dass Ihr Server benannt ist `spire-server-0` und in Ihrem Audio-Namespace gehostet wird. Sie sollten sehen, dass die Plugins erfolgreich geladen wurden und eine Verbindung zu Ihrer privaten Upstream-Zertifizierungsstelle hergestellt wurde.	DevOps Techniker

Zugehörige Ressourcen

- Verwenden von mTLS mit SPIFFE/SPIRE in AWS App Mesh auf Amazon EKS
- Aktivieren von mTLS in AWS App Mesh mit SPIFFE/SPIRE in einer Amazon-EKS-Umgebung mit mehreren Konten
- In diesem Muster verwendete exemplarische Vorgehensweise
- Server-Plugin: UpstreamAuthority "aws_pca"

- Schnellstart für Kubernetes

Zusätzliche Informationen

Anfügen von Berechtigungen an die Cluster-Knoten-Instance-Rolle

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ACMPCASigning",
            "Effect": "Allow",
            "Action": [
                "acm-pca:DescribeCertificateAuthority",
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm:ExportCertificate"
            ],
            "Resource": "*"
        }
    ]
}
AWS Managed Policy: "AWSAppMeshEnvoyAccess"
```

Hinzufügen des SPIRE-Plugins für ACM

```
Add the SPIRE plugin for ACM
Change certificate_authority_arn to your PCA ARN. The signing algorithm used must be
 the same as the signing algorithm on the PCA. Change your_region to the appropriate
 AWS Region.
UpstreamAuthority "aws_pca" {
    plugin_data {
        region = "your_region"
        certificate_authority_arn = "arn:aws:acm-pca:...."
        signing_algorithm = "your_signing_algorithm"
    }
}
```

Automatisieren von Backups für Amazon RDS for PostgreSQL-DB-Instances mithilfe von AWS Batch

Erstellt von Kirankumar Chandrashekar (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices; Datenbanken; DevOps	Workload: Alle anderen Workloads
AWS-Services: Amazon RDS; AWS Batch; Amazon CloudWatch; AWS Lambda ;Amazon S3		

Übersicht

Das Sichern Ihrer PostgreSQL-Datenbanken ist eine wichtige Aufgabe und kann in der Regel mit dem Dienstprogramm pg_dump abgeschlossen werden, das standardmäßig den COPY-Befehl verwendet, um ein Schema und einen Datenabbild einer PostgreSQL-Datenbank zu erstellen. Dieser Prozess kann sich jedoch wiederholen, wenn Sie regelmäßige Backups für mehrere PostgreSQL-Datenbanken benötigen. Wenn Ihre PostgreSQL-Datenbanken in der Cloud gehostet werden, können Sie auch die automatisierte Backup-Funktion von Amazon Relational Database Service (Amazon RDS) für PostgreSQL nutzen. Dieses Muster beschreibt, wie Sie regelmäßige Backups für DB-Instances von Amazon RDS für PostgreSQL mit dem Dienstprogramm pg_dump automatisieren.

Hinweis: In den Anweisungen wird davon ausgegangen, dass Sie Amazon RDS verwenden. Sie können diesen Ansatz jedoch auch für PostgreSQL-Datenbanken verwenden, die außerhalb von Amazon RDS gehostet werden. Um Backups erstellen zu können, muss die AWS Lambda-Funktion auf Ihre Datenbanken zugreifen können.

Ein zeitbasiertes Amazon Events- CloudWatch Ereignis initiiert eine Lambda-Funktion, die nach bestimmten Backup-Tags sucht, die auf die Metadaten der PostgreSQL-DB-Instances in Amazon RDS angewendet werden. PostgreSQL Wenn die PostgreSQL-DB-Instances das Tag bkp:AutomatedDBDump = Active und andere erforderliche Backup-Tags haben, sendet die Lambda-Funktion einzelne Aufträge für jedes Datenbank-Backup an AWS Batch .

AWS Batch verarbeitet diese Aufträge und lädt die Sicherungsdaten in einen Amazon Simple Storage Service (Amazon S3)-Bucket hoch. Dieses Muster verwendet eine Docker-Datei und eine entrypoint.sh-Datei, um ein Docker-Container-Image zu erstellen, das für Backups im AWS Batch-Auftrag verwendet wird. Nachdem der Backup-Prozess abgeschlossen ist, zeichnet AWS Batch die Backup-Details in einer Bestandstabelle auf Amazon DynamoDB auf. Als zusätzlicher Schutz initiiert ein CloudWatch Ereignisereignis eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung, wenn ein Auftrag in AWS Batch fehlschlägt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine vorhandene verwaltete oder nicht verwaltete Datenverarbeitungsumgebung. Weitere Informationen finden Sie unter Verwaltete und nicht verwaltete Datenverarbeitungsumgebungen in der AWS Batch-Dokumentation.
- AWS Command Line Interface (CLI) Version 2 Docker-Image , installiert und konfiguriert.
- Bestehende DB-Instances von Amazon RDS für PostgreSQL.
- Ein vorhandener S3-Bucket.
- Docker , installiert und konfiguriert unter Linux, macOS oder Windows.
- Vertrautheit mit der Codierung in Lambda.

Architektur

Technologie-Stack

- Amazon CloudWatch -Ereignisse
- Amazon DynamoDB
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon RDS
- Amazon SNS
- Amazon S3
- AWS Batch

- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- Docker

Tools

- Amazon CloudWatch Events – CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.
- Amazon DynamoDB – DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Amazon ECR – Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter AWS-Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon RDS – Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud vereinfacht.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten bereitstellt.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.
- AWS Batch – AWS Batch hilft Ihnen, Batch-Computing-Workloads in der AWS Cloud auszuführen.
- AWS KMS – AWS Key Management Service (AWS KMS) ist ein verwalteter Service, der es Ihnen erleichtert, die Verschlüsselungsschlüssel zu erstellen und zu steuern, die zur Verschlüsselung Ihrer Daten verwendet werden.
- AWS Lambda – Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen.
- AWS Secrets Manager – Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- Docker – Docker hilft Entwicklern dabei, jede Anwendung einfach als leichter, portabler und selbstzureichender Container zu packen, zu versenden und auszuführen.

Auf Ihre PostgreSQL-DB-Instances in Amazon RDS müssen Tags auf ihre Metadaten angewendet werden. Die Lambda-Funktion sucht nach Tags, um DB-Instances zu identifizieren, die gesichert werden sollen, und die folgenden Tags werden normalerweise verwendet.

Markierung	Beschreibung
bkp:AutomatedDBDump = Aktiv	Identifiziert eine Amazon RDS-DB-Instance als Kandidat für Backups.
bkp:AutomatedBackupSecret = <secret_name>	Identifiziert das Secrets-Manager-Secret, das die Amazon-RDS-Anmeldeinformationen enthält.
bkp:AutomatedDBDumpS3Bucket = <s3_bucket_name>	Identifiziert den S3-Bucket, an den Sicherungen gesendet werden sollen.
bkp:AutomatedDBDumpFrequency bkp:AutomatedDBDumpTime	Identifizieren Sie die Häufigkeit und Uhrzeit, zu der Datenbanken gesichert werden sollen.
bkp:pgdumpcommand = <pgdump_command>	Identifiziert die Datenbanken, für die die Backups erstellt werden müssen.

Polen

Erstellen einer Bestandstabelle in DynamoDB

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle in DynamoDB .	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon DynamoDB-Konsole und erstellen Sie eine Tabelle. Hilfe zu dieser und anderen Artikeln finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator, Datenbankadministrator
Bestätigen Sie, dass die Tabelle erstellt wurde.	Führen Sie den Befehl `aws dynamodb describe-table --table-name`	Cloud-Administrator, Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<table-name> | grep TableStatus` aus. Wenn die Tabelle vorhanden ist, gibt der Befehl das `"TableStatus": "ACTIVE",` Ergebnis zurück.	

Erstellen eines SNS-Themas für fehlgeschlagene Auftragsereignisse in AWS Batch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Öffnen Sie die Amazon SNS-Konsole, wählen Sie Themen und erstellen Sie ein SNS-Thema mit dem Namen `JobFailedAlert` . Abonnieren Sie eine aktive E-Mail-Adresse für das Thema und überprüfen Sie Ihren E-Mail-Posteingang, um die SNS-Abonnement-E-Mail von AWS Notifications zu bestätigen.	Cloud-Administrator
Erstellen Sie eine fehlgeschlagene Auftragsereignisregel für AWS Batch .	Öffnen Sie die Amazon-CloudWatch Konsole, wählen Sie Ereignisse und dann Regel erstellen aus. Wählen Sie Erweiterte Optionen anzeigen und dann Bearbeiten aus. Ersetzen Sie unter Muster erstellen, das Ereignisse für die Verarbeitung durch Ihre Ziele auswählt den vorhandenen Text durch	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Code „Auftragsereignis fehlgeschlagen“ aus dem Abschnitt Zusätzliche Informationen. Dieser Code definiert eine CloudWatch Ereignisregel, die ausgelöst wird, wenn AWS Batch ein `Failed` Ereignis hat.	
Fügen Sie ein Ereignisregelziel hinzu.	Wählen Sie unter Ziele die Option Ziele hinzufügen und wählen Sie das `JobFailed Alert` SNS-Thema aus. Konfigurieren Sie die verbleibenden Details und erstellen Sie die Cloudwatch Events-Regel.	Cloud-Administrator

Erstellen eines Docker-Images und Übertragen in ein Amazon ECR-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Öffnen Sie die Amazon ECR-Konsole und wählen Sie die AWS-Region aus, in der Sie Ihr Repository erstellen möchten. Wählen Sie Repositorys und dann Repository erstellen aus. Konfigurieren Sie das Repository entsprechend Ihren Anforderungen.	Cloud-Administrator
Schreiben Sie eine Docker-Datei.	Melden Sie sich bei Docker an und verwenden Sie die Datei „Beispiel-Dockerfile“	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und „Beispiel-entrypoint.sh“ aus dem Abschnitt Zusätzlic he Informationen, um ein Dockerfile zu erstellen.	
Erstellen Sie ein Docker-Im age und übertragen Sie es in das Amazon-ECR-Repository.	Erstellen Sie die Docker-Da tei in ein Docker-Image und übertragen Sie sie in das Amazon ECR-Repository. Hilfe zu dieser Geschicht e finden Sie im Abschnitt Verwandte Ressourcen.	DevOps Techniker

Erstellen der AWS Batch-Komponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Batch-Auftragsdefinition.	Öffnen Sie die AWS Batch-Konsole und erstellen Sie eine Auftragsdefinition, die den Uniform Resource Identifie r (URI) des Amazon ECR-Repositorys als Eigenschaft enthält`Image`.	Cloud-Administrator
Konfigurieren Sie die AWS Batch-Auftragswarteschlange.	Wählen Sie in der AWS Batch-Konsole Auftragswarteschla ngen und dann Warteschlange erstellen aus. Erstellen Sie eine Auftragswarteschlange, in der Aufträge gespeichert werden, bis AWS Batch sie auf den Ressourcen in Ihrer Datenverarbeitungsumgebung ausführt. Wichtig: Stellen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie sicher, dass Sie Logik für AWS Batch schreiben, um die Backup-Details in der DynamoDB-Bestandstabelle aufzuzeichnen.	

Erstellen und Planen einer Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion, um nach Tags zu suchen.	Erstellen Sie eine Lambda-Funktion, die auf Ihren PostgreSQL-DB-Instances nach Tags sucht und Backup-Kandidaten identifiziert. Stellen Sie sicher, dass Ihre Lambda-Funktion das `bkp:AutomatedDBDump = Active` Tag und alle anderen erforderlichen Tags identifizieren kann. Wichtig: Die Lambda-Funktion muss auch in der Lage sein, Aufträge zur AWS Batch-Auftragswarteschlange hinzuzufügen.	DevOps Techniker
Erstellen Sie ein CloudWatch zeitbasiertes Ereignis.	Öffnen Sie die Amazon-CloudWatch Konsole und erstellen Sie ein CloudWatch Ereignis, das einen Cron-Ausdruck verwendet, um Ihre Lambda-Funktion regelmäßig auszuführen. Wichtig:	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Alle geplanten Ereignisse verwenden die UTC-Zeitzone.	

Testen der Backup-Automatisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-KMS-Schlüssel.	Öffnen Sie die Amazon KMS-Konsole und erstellen Sie einen KMS-Schlüssel, mit dem die in AWS Secrets Manager gespeicherten Amazon RDS-Anmeldeinformationen verschlüsselt werden können.	Cloud-Administrator
Erstellen Sie ein AWS Secrets Manager-Secret.	Öffnen Sie die AWS Secrets Manager-Konsole und speichern Sie Ihre Datenbank anmeldeinformationen von Amazon RDS für PostgreSQL als Secret.	Cloud-Administrator
Fügen Sie den PostgreSQ L-DB-Instances die erforderl ichen Tags hinzu.	Öffnen Sie die Amazon-RD S-Konsole und fügen Sie den PostgreSQL-DB-Inst ances, die Sie automatis ch sichern möchten, Tags hinzu. Sie können die Tags aus der Tabelle im Abschnitt Tools verwenden. Wenn Sie Backups aus mehreren PostgreSQL-Datenbanken innerhalb derselben Amazon-RDS-Instance benötigen, verwenden Sie `-d test:-`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`d test1` als Wert für das `bkp:pgdumpcommand` Tag. Wichtig: `test` und `test1` sind Datenbanknamen. Stellen Sie sicher, dass nach dem Doppelpunkt (:) kein Leerzeichen vorhanden ist.	
Überprüfen Sie die Backup-Automatisierung.	Um die Backup-Automatisierung zu überprüfen, können Sie entweder die Lambda-Funktion aufrufen oder warten, bis der Backup-Zeitplan beginnt. Überprüfen Sie nach Abschluss des Backup-Vorgangs, ob die DynamoDB-Bestandstabelle einen gültigen Backup-Eintrag für Ihre PostgreSQL-DB-Instances enthält. Wenn sie übereinstimmen, ist der Backup-Automatisierungsprozess erfolgreich.	Cloud-Administrator

Zugehörige Ressourcen

Erstellen einer Bestandstabelle in DynamoDB

- Erstellen einer Amazon-DynamoDB-Tabelle

Erstellen eines SNS-Themas für fehlgeschlagene Auftragsereignisse in AWS Batch

- Erstellen eines Amazon SNS-Themas

- Senden von SNS-Warnungen für fehlgeschlagene Auftragsereignisse in AWS Batch

Erstellen eines Docker-Images und Übertragen in ein Amazon ECR-Repository

- Erstellen eines Amazon-ECR-Repositorys
- Schreiben einer Docker-Datei, Erstellen eines Docker-Images und Verschieben in Amazon ECR

Erstellen der AWS Batch-Komponenten

- Erstellen einer AWS Batch-Auftragsdefinition
- Konfigurieren Ihrer Datenverarbeitungsumgebung und AWS Batch-Auftragswarteschlange
- Erstellen einer Auftragswarteschlange in AWS Batch

Erstellen einer Lambda-Funktion

- Erstellen einer Lambda-Funktion und Schreiben von Code
- Verwenden von Lambda mit DynamoDB

Erstellen eines CloudWatch Ereignisses

- Erstellen eines zeitbasierten CloudWatch Ereignisses
- Verwenden von Cron-Ausdrücken in Cloudwatch Events

Testen der Backup-Automatisierung

- Erstellen eines Amazon-KMS-Schlüssels
- Erstellen eines Secrets-Manager-Secrets

- Hinzufügen von Tags zu einer Amazon-RDS-Instance

Zusätzliche Informationen

Fehlgeschlagenes Auftragsereignis:

```
{
  "detail-type": [
    "Batch Job State Change"
  ],
  "source": [
    "aws.batch"
  ],
  "detail": {
    "status": [
      "FAILED"
    ]
  }
}
```

Beispiel-Dockerfile:

```
FROM alpine:latest
RUN apk --update add py-pip postgresql-client jq bash && \
pip install awscli && \
rm -rf /var/cache/apk/*
ADD entrypoint.sh /usr/bin/
RUN chmod +x /usr/bin/entrypoint.sh
ENTRYPOINT ["entrypoint.sh"]
```

Beispieldatei entrypoint.sh:

```
 #!/bin/bash
set -e
DATETIME=`date +"%Y-%m-%d_%H_%M"`
FILENAME=RDS_PostGres_dump_${RDS_INSTANCE_NAME}
FILE=${FILENAME}_${DATETIME}

aws configure --profile new-profile set role_arn arn:aws:iam::${TargetAccountId}:role/
${TargetAccountRoleName}
aws configure --profile new-profile set credential_source EcsContainer
```

```
echo "Central Account access provider IAM role is: "
aws sts get-caller-identity

echo "Target Customer Account access provider IAM role is: "
aws sts get-caller-identity --profile new-profile

securestring=$(aws secretsmanager get-secret-value --secret-id $SECRETID --output json
 --query 'SecretString' --region=$REGION --profile new-profile)

if [[ ${securestring} ]]; then
    echo "successfully accessed secrets manager and got the credentials"
    export PGPASSWORD=$(echo $securestring | jq --raw-output | jq -r '.DB_PASSWORD')
    PGSQL_USER=$(echo $securestring | jq --raw-output | jq -r '.DB_USERNAME')
    echo "Executing pg_dump for the PostGres endpoint ${PGSQL_HOST}"
    # pg_dump -h $PGSQL_HOST -U $PGSQL_USER -n dms_sample | gzip -9 -c  | aws s3 cp -
 --region=$REGION  --profile new-profile s3://$BUCKET/$FILE
    # in="-n public:-n private"
    IFS=':' list=($EXECUTE_COMMAND);
    for command in "${list[@]}";
      do
        echo $command;
        pg_dump -h $PGSQL_HOST -U $PGSQL_USER ${command} | gzip -9 -c  | aws s3 cp - --
region=$REGION --profile new-profile s3://${BUCKET}/${FILE}-${command}".sql.gz"
        echo $?;
        if  [[ $? -ne 0 ]]; then
            echo "Error occurred in database backup process. Exiting now....."
            exit 1
        else
            echo "Postgresql dump was successfully taken for the RDS endpoint
 ${PGSQL_HOST} and is uploaded to the following S3 location s3://${BUCKET}/${FILE}-
${command}.sql.gz"
            #write the details into the inventory table in central account
            echo "Writing to DynamoDB inventory table"
            aws dynamodb put-item --table-name ${RDS_POSTGRES_DUMP_INVENTORY_TABLE} --
region=$REGION --item '{ "accountId": { "S": "'"${TargetAccountId}"'" }, "dumpFileUrl":
 {"S": "'"s3://${BUCKET}/${FILE}-${command}.sql.gz"'" }, "DumpAvailableTime": {"S":
 "'"`date +"%Y-%m-%d::%H::%M::%S"` UTC"'"}}'
            echo $?
            if  [[ $? -ne 0 ]]; then
                echo "Error occurred while putting item to DynamoDb Inventory Table.
 Exiting now....."
                exit 1
            else
```

```
                echo "Successfully written to DynamoDb Inventory Table
 ${RDS_POSTGRES_DUMP_INVENTORY_TABLE}"
            fi
        fi
      done;
else
    echo "Something went wrong {$?}"
    exit 1
fi

exec "$@"
```

Automatisieren der Bereitstellung des Node Termination Handler in Amazon EKS mithilfe einer CI/CD-Pipeline

Erstellt von Sandip Gangapadhyay (AWS), John Var (AWS), Pragtideep Singh (AWS), Sandeep Gawande (AWS) und Viyoma Sachdeva (AWS)

Code-Repository: Bereitstellen von NTH in EKS	Umgebung: Produktion	Technologien: Container und Microservices; DevOps
AWS-Services: AWS CodePipeline; Amazon EKS; AWS CodeBuild		

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie AWS Node Termination Handler , ein Open-Source-Projekt, verwenden, um das Herunterfahren von Amazon Elastic Compute Cloud (Amazon EC2)-Instances innerhalb von Kubernetes ordnungsgemäß durchzuführen. AWS Node Termination Handler hilft sicherzustellen, dass die Kubernetes-Steuerebene angemessen auf Ereignisse reagiert, die dazu führen können, dass Ihre EC2-Instance nicht verfügbar ist. Zu diesen Ereignissen gehören die folgenden:

- Geplante Wartung der EC2-Instance
- Unterbrechungen der Amazon EC2 Spot Instance
- Auto Scaling-Gruppenskalierung
- Neuausgleich von Auto Scaling-Gruppen über Availability Zones hinweg
- EC2-Instance-Beendigung über die API oder die AWS-Managementkonsole

Wenn ein Ereignis nicht behandelt wird, wird Ihr Anwendungscode möglicherweise nicht ordnungsgemäß beendet. Es kann auch länger dauern, bis die volle Verfügbarkeit wiederhergestellt ist, oder es kann versehentlich Arbeit an Knoten planen, die ausfallen. Die `aws-node-termination-handler` (NTH) kann in zwei verschiedenen Modi betrieben werden: Instance Metadata Service (IMDS) oder Warteschlangenprozessor. Weitere Informationen zu den beiden Modi finden Sie in der Readme-Datei .

Dieses Muster automatisiert die Bereitstellung von NTH mithilfe des Warteschlangenprozessors über eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD).

Hinweis: Wenn Sie EKS-verwaltete Knotengruppen verwenden, benötigen Sie die nicht`aws-node-termination-handler`.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Webbrowser, der für die Verwendung mit der AWS-Managementkonsole unterstützt wird. Sehen Sie sich die Liste der unterstützten Browser an.
- AWS Cloud Development Kit (AWS CDK) installiert.
- `kubectl`, das Kubernetes-Befehlszeilen-Tool, installiert.
- `eksctl`, die AWS-Befehlszeilenschnittstelle (AWS CLI) für Amazon Elastic Kubernetes Service (Amazon EKS), installiert .
- Ein laufender EKS-Cluster mit Version 1.20 oder höher.
- Eine selbstverwaltete Knotengruppe, die dem EKS-Cluster zugeordnet ist. Führen Sie den folgenden Befehl aus, um einen Amazon-EKS-Cluster mit einer selbstverwalteten Knotengruppe zu erstellen.

```
eksctl create cluster --managed=false --region <region> --name <cluster_name>
```

  Weitere Informationen zu finden Sie `eksctl`in der eksctl-Dokumentation.
- AWS Identity and Access Management (IAM) OpenID Connect (OIDC)-Anbieter für Ihren Cluster. Weitere Informationen finden Sie unter Erstellen eines IAM-OIDC-Anbieters für Ihren Cluster.

Einschränkungen

- Sie müssen eine AWS-Region verwenden, die den Amazon EKS-Service unterstützt.

Produktversionen

- Kubernetes Version 1.20 oder höher
- `eksctl` -Version 0.107.0 oder höher

- AWS-CDK-Version 2.27.0 oder höher

Architektur

Zieltechnologie-Stack

- Eine Virtual Private Cloud (VPC)
- Ein EKS-Cluster
- Amazon Simple Queue Service (Amazon SQS)
- IAM
- Kubernetes

Zielarchitektur

Das folgende Diagramm zeigt die allgemeine Ansicht der end-to-end Schritte beim Starten der Knotenbeendigung.

Der im Diagramm gezeigte Workflow besteht aus den folgenden allgemeinen Schritten:

1. Das Ereignis zum Beenden der EC2-Instance mit automatischer Skalierung wird an die SQS-Warteschlange gesendet.
2. Der NTH-Pod überwacht auf neue Nachrichten in der SQS-Warteschlange.
3. Der NTH-Pod empfängt die neue Nachricht und führt Folgendes aus:
   - Sperrt den Knoten, sodass der neue Pod nicht auf dem Knoten ausgeführt wird.
   - Entleert den Knoten, sodass der vorhandene Pod evakuiert wird
   - Sendet ein Lebenszyklus-Hook-Signal an die Auto Scaling-Gruppe, damit der Knoten beendet werden kann.

Automatisierung und Skalierung

- Code wird von AWS CDK verwaltet und bereitgestellt, unterstützt von CloudFormation verschachtelten AWS-Stacks.
- Die Amazon-EKS-Steuerebene wird über mehrere Availability Zones hinweg ausgeführt, um eine hohe Verfügbarkeit zu gewährleisten.

- Für die automatische Skalierung unterstützt Amazon EKS den Kubernetes Cluster Autoscaler und Karpenter .

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- Amazon EC2 Auto Scaling unterstützt Sie bei der Aufrechterhaltung der Anwendungsverfügbarkeit und ermöglicht Ihnen das automatische Hinzufügen oder Entfernen von Amazon EC2-Instances gemäß den von Ihnen definierten Bedingungen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Andere Tools

- kubectl ist ein Kubernetes-Befehlszeilen-Tool zum Ausführen von Befehlen für Kubernetes-Cluster. Sie können kubectl verwenden, um Anwendungen bereitzustellen, Clusterressourcen zu überprüfen und zu verwalten und Protokolle anzuzeigen.

Code

Der Code für dieses Muster ist im deploy-nth-to-eks Repo auf GitHub.com verfügbar. Das Code-Repo enthält die folgenden Dateien und Ordner.

- `nth folder` – Das Helm-Diagramm, die Werte der Dateien und die Skripts zum Scannen und Bereitstellen der AWS- CloudFormation Vorlage für Node Termination Handler.
- `config/config.json` – Die Konfigurationsparameterdatei für die Anwendung. Diese Datei enthält alle Parameter, die für die Bereitstellung von CDK erforderlich sind.
- `cdk` – AWS-CDK-Quellcode.
- `setup.sh` – Das Skript, das zum Bereitstellen der AWS-CDK-Anwendung verwendet wird, um die erforderliche CI/CD-Pipeline und andere erforderliche Ressourcen zu erstellen.
- `uninstall.sh` – Das Skript, das zum Bereinigen der Ressourcen verwendet wird.

Um den Beispielcode zu verwenden, folgen Sie den Anweisungen im Abschnitt „Epics“.

Bewährte Methoden

Bewährte Methoden zur Automatisierung des AWS Node Termination Handler finden Sie im Folgenden:

- Bewährte Methoden für EKS
- Node Termination Handler – Konfiguration

Sekunden

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo.	Um das Repo mithilfe von SSH (Secure Shell) zu klonen, führen Sie den folgenden Befehl aus. `git clone git@github.com:aws-samples/deploy-nth-to-eks.git`	App-Entwickler, AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Um das Repo mithilfe von HTTPS zu klonen, führen Sie den folgenden Befehl aus.
	`git clone https://github.com/aws-samples/deploy-nth-to-eks.git`
	Durch das Klonen des Repositorys wird ein Ordner mit dem Namen erstelltdeploy-nth-to-eks.
	Wechseln Sie zu diesem Verzeichnis.
	`cd deploy-nth-to-eks`	

Legen Sie die kubeconfig-Datei fest.	Legen Sie Ihre AWS-Anmeldeinformationen in Ihrem Terminal fest und bestätigen Sie, dass Sie über die Rechte verfügen, die Clusterrolle zu übernehmen. Sie können den folgenden Beispielcode verwenden. `aws eks update-kubeconfig --name <Cluster_Name> --region <region>--role-arn <Role_ARN>`	AWS DevOps, DevOps Techniker, App-Entwickler

Bereitstellen der CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Parameter ein.	Richten Sie in der `config/config.json` Datei die folgenden erforderlichen Parameter ein. • `pipelineName` : Der Name der CI/CD-Pipeline, die von AWS CDK erstellt werden soll (z. B. `deploy-nth-to-eks-pipeline`). AWS CodePipeline erstellt eine Pipeline mit diesem Namen. • `repositoryName` : Das zu erstellende AWS CodeCommit -Repo (z. B. `deploy-nth-to-eks-repo`). AWS CDK erstellt dieses Repo und legt es als Quelle für die CI/CD-Pipeline fest. Hinweis: Diese Lösung erstellt dieses CodeCommit Repo und die Verzweigung (im folgenden Verzweigungsparameter bereitgestellt). • `branch`: Der Verzweigungsname im Repo (z. B. `main`). Ein Commit an diesen Zweig initiiert die CI/CD-Pipeline.	App-Entwickler, AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `cfn_scan_script` : Der Pfad des Skripts, das zum Scannen der AWS-CloudFormation Vorlage auf NTH () verwendet wird`scan.sh`. Dieses Skript ist im `nth` Ordner vorhanden, der Teil des AWS- CodeCommit Repo sein wird. • `cfn_deploy_scrip t`: Der Pfad des Skripts, das zur Bereitstellung der AWS-CloudFormation Vorlage für NTH () verwendet wird`installApp.sh` . • `stackName` : Der Name des CloudFormation Stacks, der bereitgestellt werden soll. • `eksClusterName` : Der Name des vorhandenen EKS-Clusters. • `eksClusterRole` : Die IAM-Rolle, die für den Zugriff auf den EKS-Clust er für alle Kubernetes-API-Aufrufe verwendet wird (z. B. `clusteradmin`). Normalerweise wird diese Rolle in hinzugefügt`aws-authConfigMap` . • `create_cluster_rol e` : Um die `eksCluste`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rRole` IAM-Rolle zu erstellen, geben Sie Ja ein. Wenn Sie eine vorhandene Clusterrolle im `eksCluste rRole` Parameter angeben möchten, geben Sie keine ein. • `create_iam_oidc_pr ovider` : Um den IAM-OIDC-Anbieter für Ihren Cluster zu erstellen, geben Sie Ja ein. Wenn bereits ein IAM-OIDC-Anbieter vorhanden ist, geben Sie keine ein. Weitere Informati onen finden Sie unter Erstellen eines IAM-OIDC-Anbieters für Ihren Cluster. • `AsgGroupName` : Eine durch Komma getrennte Liste von Auto Scaling-G ruppennamen, die Teil des EKS-Clusters sind (z. B. `ASG_Group_1,ASG_Gr oup_2`). • `region`: Der Name der AWS-Region, in der sich der Cluster befindet (z. B. `us-east-2`). • `install_cdk` : Wenn AWS CDK derzeit nicht auf dem Computer installiert ist, geben Sie Ja ein. Führen Sie den `cdk --version`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Befehl aus, um zu überprüfen, ob die installierte AWS-CDK-Version 2.27.0 oder höher ist. Geben Sie in diesem Fall keine ein. Wenn Sie Ja eingeben, führt das Skript setup.sh den `sudo npm install -g cdk@2.27.0` Befehl aus, um AWS CDK auf dem Computer zu installieren. Das Skript erfordert Sudo-Berechtigungen. Geben Sie daher das Kontopasswort an, wenn Sie dazu aufgefordert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CI/CD-Pipeline, um NTH bereitzustellen.	Führen Sie das Skript setup.sh aus. `./setup.sh` Das Skript stellt die AWS-CDK-Anwendung bereit, die das CodeCommit Repo mit Beispielcode, Pipeline und CodeBuild Projekten basierend auf den Benutzereingabeparametern in `config/config.json` der Datei erstellt. Dieses Skript fragt nach dem Passwort, wenn es npm-Pakete mit dem sudo-Befehl installiert.	App-Entwickler, AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CI/CD-Pipeline.	Öffnen Sie die AWS-Managementkonsole und überprüfen Sie die folgenden Ressourcen, die im Stack erstellt wurden. • CodeCommit -Repo mit dem Inhalt des `nth` Ordners • AWS- CodeBuild Projekt `cfn-scan`, das die CloudFormation Vorlage auf Schwachstellen scannt. • CodeBuild Projekt `Nth-Deploy` , das die AWS-CloudFormation Vorlage und die entsprechenden NTH-Helm-Diagramme über die AWS- CodePipeline Pipeline bereitstellt. • Eine CodePipeline Pipeline zur Bereitstellung von NTH. Nachdem die Pipeline erfolgreich ausgeführt wurde, `aws-node-termination-handler` wird die Helm-Version im EKS-Cluster installiert. Außerdem `aws-node-termination-handler` wird ein Pod mit dem Namen im `kube-system` Namespace im Cluster ausgeführt.	App-Entwickler, AWS DevOps, DevOps Techniker

Testen der NTH-Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Simulieren Sie ein Abskalier ungsereignis für Auto Scaling-Gruppen.	Gehen Sie wie folgt vor, um ein Abskalierungsereignis für die automatische Skalierung zu simulieren: 1. Öffnen Sie in der AWS-Konsole die EC2-Konso le und wählen Sie Auto Scaling-Gruppen aus. 2. Wählen Sie die Auto Scaling-Gruppe aus, die denselben Namen wie die in angegebene hat `config/config.json` , und wählen Sie Bearbeiten aus. 3. Verringern Sie die gewünschte und minimale Kapazität um 1. 4. Wählen Sie Aktualisieren.	
Überprüfen Sie die Protokolle.	Während des Abskalier ungsereignisses sperrt und leert der NTH-Pod den entsprechenden Worker-Kn oten (die EC2-Instance, die im Rahmen des Abskalier ungsereignisses beendet wird). Um die Protokolle zu überprüfen, verwenden Sie den Code im Abschnitt Zusätzliche Informationen.	App-Entwickler, AWS DevOps, DevOps Techniker

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie alle AWS-Ressourcen.	Führen Sie den folgenden Befehl aus, um die durch dieses Muster erstellten Ressourcen zu bereinigen. `./uninstall.sh` Dadurch werden alle in diesem Muster erstellten Ressourcen durch Löschen des CloudFormation Stacks bereinigt.	DevOps Techniker

Fehlerbehebung

Problem	Lösung
Die npm-Registrierung ist nicht korrekt festgelegt.	Während der Installation dieser Lösung installiert das Skript npm install, um alle erforderlichen Pakete herunterzuladen. Wenn während der Installation die Meldung „Modul kann nicht gefunden werden“ angezeigt wird, ist die npm-Registrierung möglicherweise nicht korrekt festgelegt. Führen Sie den folgenden Befehl aus, um die aktuelle Registrierungseinstellung anzuzeigen. `npm config get registry` Führen Sie den folgenden Befehl aus`https://registry.npmjs.org/` , um die Registrierung mit festzulegen.

Problem	Lösung
	`npm config set registry https://registry.npmjs.org`
Verzögern Sie die Zustellung von SQS-Nachrichten.	Wenn Sie im Rahmen Ihrer Fehlerbehebung die SQS-Nachrichtenzustellung an den NTH-Pod verzögern möchten, können Sie den Parameter für die SQS-Zustellungsverzögerung anpassen. Weitere Informationen finden Sie unter Amazon SQS-Verzögerungswarteschlangen.

Zugehörige Ressourcen

- Quellcode des AWS Node Termination Handler
- EC2-Workshop
- AWS CodePipeline
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Cloud Development Kit
- AWS CloudFormation

Zusätzliche Informationen

1. Suchen Sie den Namen des NTH-Pods.

```
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
```

2. Überprüfen Sie die Protokolle. Ein Beispielprotokoll sieht wie folgt aus. Es zeigt, dass der Knoten vor dem Senden des Lebenszyklus-Hook-Vervollständigungssignals der Auto Scaling-Gruppe gesperrt und geleert wurde.

```
kubectl -n kube-system logs aws-node-termination-handler-65445555-kbqc7
```

```
022/07/17 20:20:43 INF Adding new event to the event store
 event={"AutoScalingGroupName":"eksctl-my-cluster-target-nodegroup-
ng-10d99c89-NodeGroup-ZME36IGAP7O1","Description":"ASG Lifecycle Termination
 event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n","EndTime":"0001-01-01T00:00:00Z","EventID":"asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564","InProgress":fal
east-2.compute.internal","NodeProcessed":false,"Pods":null,"ProviderID":"aws:///us-
east-2c/i-0409f2a9d3085b80e","StartTime":"2022-07-17T20:20:42.702Z","State":""}
2022/07/17 20:20:44 INF Requesting instance drain event-id=asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564
 instance-id=i-0409f2a9d3085b80e kind=SQS_TERMINATE node-name=ip-192-168-75-60.us-
east-2.compute.internal provider-id=aws:///us-east-2c/i-0409f2a9d3085b80e
2022/07/17 20:20:44 INF Pods on node node_name=ip-192-168-75-60.us-
east-2.compute.internal pod_names=["aws-node-qchsw","aws-node-termination-
handler-65445555-kbqc7","kube-proxy-mz5x5"]
2022/07/17 20:20:44 INF Draining the node
2022/07/17 20:20:44 ??? WARNING: ignoring DaemonSet-managed Pods: kube-system/aws-node-
qchsw, kube-system/kube-proxy-mz5x5
2022/07/17 20:20:44 INF Node successfully cordoned and drained
 node_name=ip-192-168-75-60.us-east-2.compute.internal reason="ASG Lifecycle
 Termination event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n"
2022/07/17 20:20:44 INF Completed ASG Lifecycle Hook (NTH-K8S-TERM-HOOK) for instance
 i-0409f2a9d3085b80e
```

Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline

Erstellt von MAHESH RAGHUNANDANAN (AWS), Bol Radtke (AWS) und Jomcypachen (AWS)

Code-Repository: aws-cicd-java-eks	Umgebung: Produktion	Technologien: Container und Microservices; Cloudnativ; DevOpsModernisierung
Workload: Alle anderen Workloads	AWS-Services: AWS CloudFormation; AWS CodeCommit; AWS CodePipeline; Amazon EC2 Container Registry ; Amazon EKS	

Übersicht

Dieses Muster beschreibt, wie Sie eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery) erstellen, die automatisch eine Java-Anwendung mit empfohlenen DevSecOps Methoden erstellt und auf einem Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster in der Amazon Web Services (AWS) Cloud bereitstellt. Dieses Muster verwendet eine Grußanwendung, die mit einem Spring Boot Java-Framework entwickelt wurde und Apache Maven verwendet.

Sie können den Ansatz dieses Musters verwenden, um den Code für eine Java-Anwendung zu erstellen, die Anwendungsartefakte als Docker-Image zu verpacken, das Image sicher zu scannen und das Image als Workload-Container auf Amazon EKS hochzuladen. Der Ansatz dieses Musters ist nützlich, wenn Sie von einer eng gekoppelten monolithischen Architektur zu einer Microservices-Architektur migrieren möchten. Der Ansatz hilft Ihnen auch dabei, den gesamten Lebenszyklus einer Java-Anwendung zu überwachen und zu verwalten, was ein höheres Automatisierungsniveau gewährleistet und Fehler oder Fehler vermeidet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- AWS Command Line Interface (AWS CLI) Version 2, installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI Version 2 in der AWS CLI-Dokumentation.
- AWS CLI Version 2 muss mit derselben IAM-Rolle konfiguriert sein, die den Amazon EKS-Cluster erstellt, da nur diese Rolle berechtigt ist, weitere IAM`aws-auth`-Rollen zum hinzuzufügen`ConfigMap`. Informationen und Schritte zur Konfiguration der AWS CLI finden Sie unter Konfigurationsgrundlagen in der AWS CLI-Dokumentation.
- AWS Identity and Access Management (IAM)-Rollen und -Berechtigungen mit vollständigem Zugriff auf AWS CloudFormation. Weitere Informationen dazu finden Sie unter Zugriffskontrolle mit IAM in der AWS- CloudFormation Dokumentation.
- Ein vorhandener Amazon-EKS-Cluster mit Details zum IAM-Rollennamen und zum Amazon-Ressourcennamen (ARN) der IAM-Rolle von Worker-Knoten im EKS-Cluster.
- Kubernetes Cluster Autoscaler, installiert und konfiguriert in Ihrem Amazon-EKS-Cluster. Weitere Informationen finden Sie unter Cluster Autoscaler in der Amazon-EKS-Dokumentation.
- Zugriff auf Code im GitHub Repository.

Wichtiger Hinweis

AWS Security Hub ist als Teil der AWS- CloudFormation Vorlagen aktiviert, die sich im Code befinden. Standardmäßig wird nach der Aktivierung von Security Hub eine 30-tägige kostenlose Testversion bereitgestellt, nach der Kosten für diesen AWS-Service anfallen. Weitere Informationen zu Preisen finden Sie unter AWS Security Hub – Preise.

Produktversionen

- Helm-Version 3.4.2 oder höher
- Apache Maven Version 3.6.3 oder höher
- BridgeCrew Checkov-Version 2.2 oder höher
- Bol Security Trivy Version 0.37 oder höher

Architektur

Technologie-Stack

- AWS CodeBuild
- AWS CodeCommit

- Amazon CodeGuru
- AWS CodePipeline
- Amazon Elastic Container Registry
- Amazon Elastic Kubernetes Service
- Amazon EventBridge
- AWS Security Hub
- Amazon Simple Notification Service (Amazon SNS)

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Der Entwickler aktualisiert den Java-Anwendungscode im Basiszweig des CodeCommit Repositorys, der eine Pull-Anforderung (PR) erstellt.
2. Sobald die PR eingereicht wurde, überprüft Amazon CodeGuru Reviewer den Code automatisch, analysiert ihn auf der Grundlage bewährter Methoden für Java und gibt dem Entwickler Empfehlungen.
3. Nachdem das PR mit dem Basiszweig zusammengeführt wurde, wird ein Amazon- EventBridge Ereignis erstellt.
4. Das EventBridge Ereignis initiiert die CodePipeline Pipeline, die startet.
5. CodePipeline führt die CodeSecurity Scan-Stufe aus (kontinuierliche Sicherheit).
6. CodeBuild startet den Sicherheitsscanprozess, bei dem die Helm-Dateien der Dockerfile- und Kubernetes-Bereitstellung mit Checkov gescannt werden und der Anwendungsquellcode auf der Grundlage inkrementeller Codeänderungen gescannt wird. Der Scan des Anwendungsquellcodes wird vom CodeGuru Reviewer Command Line Interface (CLI) Wrapper durchgeführt.
7. Wenn die Phase des Sicherheitsscans erfolgreich ist, wird die Build-Phase (fortlaufende Integration) initiiert.
8. In der Build-Phase CodeBuild erstellt das Artefakt, packt das Artefakt in ein Docker-Image, scannt das Image mithilfe von Security Trivy auf Sicherheitsschwachstellen und speichert das Image in Amazon ECR.
9. Die in Schritt 8 erkannten Schwachstellen werden zur weiteren Analyse durch Entwickler oder Techniker in Security Hub hochgeladen. Security Hub bietet einen Überblick und Empfehlungen zur Behebung der Schwachstellen.

10 E-Mail-Benachrichtigungen über verschiedene Phasen innerhalb der CodePipeline Pipeline werden über Amazon SNS gesendet.

11 Nachdem die kontinuierlichen Integrationsphasen abgeschlossen sind, CodePipeline gibt die Bereitstellungsphase ein (fortlaufende Bereitstellung).

12 Das Docker-Image wird in Amazon EKS als Container-Workload (Pod) mithilfe von Helm-Diagrammen bereitgestellt.

13 Der Anwendungs-Pod ist mit Amazon CodeGuru Profiler Agent konfiguriert, der die Profilerstellungsdaten der Anwendung (CPU, Heap-Nutzung und Latenz) an Amazon CodeGuru Profiler sendet, was Entwicklern hilft, das Verhalten der Anwendung zu verstehen.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- Amazon CodeGuru Profiler sammelt Laufzeitleistungsdaten aus Ihren Live-Anwendungen und bietet Empfehlungen, mit denen Sie die Leistung Ihrer Anwendung optimieren können.
- Amazon CodeGuru Reviewer verwendet Programmanalysen und Machine Learning, um potenzielle Fehler zu erkennen, die für Entwickler schwer zu finden sind, und bietet Vorschläge zur Verbesserung Ihres Java- und Python-Codes.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.

- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS-Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere -Services

- Helm ist ein Open-Source-Paketmanager für Kubernetes.
- Apache Maven ist ein Tool für die Verwaltung und Untersuchung von Softwareprojekten.
- BridgeCrew Checkov ist ein Tool zur statischen Codeanalyse zum Scannen von Infrastructure as Code (IaC)-Dateien auf Fehlkonfigurationen, die zu Sicherheits- oder Compliance-Problemen führen können.
- Security Trivy ist ein umfassender Schutz vor Schwachstellen in Container-Images, Dateisystemen und Git-Repositorys sowie Konfigurationsproblemen.

Code

Der Code für dieses Muster ist im GitHub aws-codepipeline-devsecops-amazoneksRepository verfügbar.

Bewährte Methoden

- Das Prinzip der geringsten Berechtigung wurde für IAM-Entitäten in allen Phasen dieser Lösung befolgt. Wenn Sie die Lösung um zusätzliche AWS-Services oder Tools von Drittanbietern erweitern möchten, empfehlen wir, dem Prinzip der geringsten Berechtigung zu folgen.

- Wenn Sie mehrere Java-Anwendungen haben, empfehlen wir, für jede Anwendung separate CI/CD-Pipelines zu erstellen.
- Wenn Sie eine monolithe Anwendung haben, empfehlen wir, die Anwendung so weit wie möglich in Microservices aufzuteilen. Microservices sind flexibler, erleichtern die Bereitstellung von Anwendungen als Container und bieten einen besseren Einblick in den gesamten Aufbau und die Bereitstellung der Anwendung.

Sekunden

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Führen Sie den folgenden Befehl aus, um das Repository zu klonen. `git clone https://github.com/aws-samples/aws-codepipeline-devsecops-amazoneks`	App-Entwickler, DevOps Techniker
Erstellen Sie einen S3-Bucket und laden Sie den Code hoch.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3-Konsole und erstellen Sie dann einen S3-Bucket in der AWS-Region, in der Sie diese Lösung bereitstellen möchten. Weitere Informationen finden Sie unter Erstellen eines Buckets in der Amazon S3-Dokumentation. 2. Erstellen Sie im S3-Bucket einen Ordner mit dem Namen `code`.	AWS DevOps, DevOps Engineering, Cloud-Administrator, DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Navigieren Sie zu dem Ort, an dem Sie das Repository geklont haben. Um eine komprimierte Version des gesamten Codes mit der ZIP-Erweiterung (`cicdstack.zip`) zu erstellen und die ZIP-Datei zu validieren, führen Sie die folgenden Befehle der Reihe nach aus.
	
	Hinweis: Wenn der `python` Befehl fehlschlägt und besagt, dass Python nicht gefunden wurde, verwenden Sie `python3` stattdessen .
	
	`cd aws-codepipeline-devsecops-amazoneks`
	`python -m zipfile -c cicdstack.zip *`
	`python -m zipfile -t cicdstack.zip`
	
	4. Laden Sie die `cicdstack.zip` Datei in den Codeordner hoch, den Sie zuvor im S3-Bucket erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS-CloudFormation Stack.	1. Öffnen Sie die AWS-CloudFormation Konsole und wählen Sie Stack erstellen aus. 2. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen, laden Sie die `cf_templates/codecommit_ecr.yaml` Datei hoch und wählen Sie dann Weiter aus. 3. Geben Sie unter Stack-Details angeben den Stack-Namen ein und geben Sie dann die folgenden Eingabeparameterwerte an: • CodeCommitRepositoryBranchName: Der Branch-Name, in dem sich Ihr Code befinden wird (Standardeinstellung ist Haupt-) • CodeCommitRepositoryName: Der Name des zu erstellenden CodeCommit Repo. • CodeCommitRepositoryS3Bucket : Der Name des S3-Buckets, in dem Sie den Codeordner erstellt haben	AWS DevOps, DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• CodeCommitRepositoryS3BucketObjKey: `code/cicdstack.zip` • ECR RepositoryName: Der Name des zu erstellenden Amazon-ECR-Repo 4. Wählen Sie Weiter, verwenden Sie die Standardeinstellungen für die Optionen Stack konfigurieren und wählen Sie dann Weiter aus. 5. Überprüfen Sie im Abschnitt Überprüfen die Vorlage und die Stack-Details und wählen Sie dann Stack erstellen aus. Der Stack wird dann erstellt, einschließlich der CodeCommit und Amazon-ECR-Repositorys. 6. Notieren Sie sich die Namen der CodeCommit und Amazon-ECR-Repositorys, die für die Einrichtung der Java-CI/CD-Pipeline erforderlich sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die CloudFormation Stack-Bereitstellung.	1. Überprüfen Sie unter Stacks in der - CloudFormation Konsole den Status des CloudFormation Stacks, den Sie bereitgestellt haben. Der Status des Stacks sollte CREATE COMPLETE lauten. 2. Überprüfen Sie außerdem über die Konsole, ob CodeCommit und Amazon ECR bereitgestellt wurden und bereit sind.	DevOps Techniker
Löschen Sie den S3-Bucket.	Leeren und löschen Sie den S3-Bucket, den Sie zuvor erstellt haben. Weitere Informationen finden Sie unter Löschen eines Buckets in der Amazon S3-Dokumentation.	AWS DevOps, DevOps

Konfigurieren der Helm-Diagramme

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Helm-Diagramme Ihrer Java-Anwendung.	1. Navigieren Sie an dem Speicherort, an dem Sie das GitHub Repository geklont haben, zum Ordner `helm_charts/aws-proserve-java-greeting` . In diesem Ordner enthält die `-values.dev.yaml`	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Datei Informationen zur Kubernetes-Ressour cenkonfiguration, die Sie für Ihre Container-Bereitst ellungen in Amazon EKS ändern können. Aktualisi eren Sie den Docker-Re pository-Parameter, indem Sie Ihre AWS-Konto-ID, AWS-Region und den Amazon ECR-Repository-Namen angeben.
	
	`image:`
	`  repository:`
	`  <account-id>.dkr.e`
	`cr.<region>.amazon`
	`aws.com/<app-ecr-r`
	`epo-name>`
	
	2. Der Servicetyp des Java-Pods ist auf festgeleg `tLoadBalancer` .
	
	`service:`
	`  type: LoadBalancer`
	`  port: 80`
	`  targetPort: 8080`
	`  path: /hello`
	`  initialDelaySecond`
	`s: 60`
	`  periodSeconds: 30`
	
	Um einen anderen Service zu verwenden (z. B. `NodePort`), können Sie die Parameter ändern. Weitere	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Informationen finden Sie in der Kubernetes-Dokumentation.
	3. Sie können den Kubernetes Horizontal Pod Autoscaler aktivieren, indem Sie den `autoscaling` Parameter in ändern`enabled: true`.
	`autoscaling:`
	`enabled: true`
	`minReplicas: 1`
	`maxReplicas: 100`
	`targetCPUUtilizationPercentage: 80`
	`# targetMemoryUtilizationPercentage: 80`
	Sie können verschiedene Funktionen für die Kubernetes-Workloads aktivieren, indem Sie die Werte in der `-values.<ENV>.yaml` Datei ändern, wobei Ihre Entwicklungs-, Produktions-, UAT- oder QA-Umgebung `<ENV>` ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Validieren Sie Helm-Diagramme auf Syntaxfehler.	1. Überprüfen Sie auf dem Terminal, ob Helm v3 auf Ihrer lokalen Workstation installiert ist, indem Sie den folgenden Befehl ausführen.
	`helm --version`
	Wenn Helm v3 nicht installiert ist, installieren Sie es .
	2. Navigieren Sie im Terminal zum Helm-Charts-Verzeichnis (`helm_charts/aws-proserve-java-greeting`) und führen Sie den folgenden Befehl aus.
	`helm lint . -f values.dev.yaml`
	Dadurch werden die Helm-Diagramme auf Syntaxfehler überprüft.
		DevOps Techniker

Einrichten der Java CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CI/CD-Pipeline.	1. Öffnen Sie die AWS-CloudFormation Konsole und wählen Sie Stack erstellen aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen , die `cf_templates/build_deployment.yaml` Vorlage hochladen und dann Weiter aus. 3. Geben Sie unter Stack-Details angeben den Stack-Namen an und geben Sie dann die folgenden Werte für die Eingabeparameter an: • CodeBranchName: Verzweigungsname des CodeCommit Repositorys, in dem sich Ihr Code befindet • EKS ClusterName: Name Ihres EKS-Clusters (nicht die `EKSCluster` -ID) • EKS CodeBuild AppName: Name des App-Helm-Charts (`aws-proserve-java-greeting`) • EKS WorkerNodeRoleARN: ARN der IAM-Rolle der Amazon-EKS-Worker-Knoten • EKS WorkerNodeRoleName: Name der IAM-Rolle, die den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-EKS-Worker-Knoten zugewiesen ist • EcrDockerRepository: Name des Amazon-ECR-Repo, in dem die Docker-Images Ihres Codes gespeichert werden • EmailRecipient: E-Mail-Adresse, an die Build-Benachrichtigungen gesendet werden müssen • EnvType: Umgebung (z. B. dev, test oder prod) • SourceRepoName: Name des CodeCommit Repositorys, in dem sich Ihr Code befindet 4. Wählen Sie Weiter aus. Verwenden Sie die Standardeinstellungen unter Stack-Optionen konfiguri eren und wählen Sie dann Weiter aus. 5. Überprüfen Sie im Abschnitt Review die AWS-CloudFormation Vorlage und die Stack-Details und wählen Sie dann Next aus. 6. Wählen Sie Stack erstellen aus. 7. Während der CloudForm ation Stack-Bereitstellung erhält der Besitzer der E-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mail-Adresse, die Sie in den Parametern angegeben haben, eine Nachricht zum Abonnieren eines SNS-Themas. Um Amazon SNS zu abonnieren, muss der Eigentümer den Link in der Nachricht auswählen. 8. Nachdem der Stack erstellt wurde, öffnen Sie die Registerkarte Outputs des Stacks und notieren Sie dann den ARN-Wert für den `EksCodeBuildkubeRoleARN` Ausgabeschlüssel. Dieser IAM-ARN-Wert wird später benötigt, um der CodeBuild IAM-Rolle Berechtigungen zum Bereitstellen von Workloads im Amazon-EKS-Cluster zu erteilen.	

Aktivieren der Integration zwischen Security Hub und Security

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Security-Integration.	Dieser Schritt ist erforderlich, um die von Trivy gemeldeten Docker-Image-Schwachstellen ergebnisse in Security Hub hochzuladen. Da AWS keine Security Hub CloudFormation -Integrationen unterstützt,	AWS-Administrator, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	muss dieser Vorgang manuell durchgeführt werden. 1. Öffnen Sie die AWS Security Hub-Konsole und navigieren Sie zu Integrationen. 2. Suchen Sie nach Security und wählen Sie Security: Security aus. 3. Wählen Sie Ergebnisse akzeptieren aus.	

Konfigurieren von CodeBuild zum Ausführen von Helm- oder kubectl-Befehlen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erlauben Sie CodeBuild , Helm- oder kubectl-Befehle im Amazon-EKS-Cluster auszuführen.	Damit für die Verwendung CodeBuild von Helm- oder -`kubectl`Befehlen mit dem EKS-Cluster `aws-auth` authentifiziert werden kann, müssen Sie die IAM-Rollen zur hinzufügen`ConfigMap` . Fügen Sie in diesem Fall den ARN der IAM-Rolle hinzu. Dabei handelt es sich um die IAM-Rolle`EksCodeBuildkubeRoleARN` , die für den CodeBuild Service erstellt wurde, um auf den EKS-Cluster zuzugreifen und Workloads darauf bereitzustellen. Dies ist eine einmalige Aktivität.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Wichtig: Das folgende Verfahren muss vor der Genehmigungsphase der Bereitstellung in abgeschlossen sein CodePipeline.
	
	1. Öffnen Sie das `cf_templates/kube_aws_auth_configmap_patch.sh` Shell-Skript in Ihrer Amazon Linux- oder macOS-Umgebung.
	2. Authentifizieren Sie sich beim Amazon-EKS-Cluster, indem Sie den folgenden Befehl ausführen.
	
	`aws eks --region <aws-region> update-kubeconfig --name <eks-cluster-name>`
	
	3. Führen Sie das Shell-Skript mit dem folgenden Befehl aus und ersetzen Sie durch `<rolearn-eks-codebuild-kubectl>` den ARN-Wert von `EksCodeBuildkubeRoleARN`, den Sie zuvor aufgezeichnet haben.
	
	`bash cf_templates/kube_aws_auth_configmap_patch.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<rolearn-eks-codebuild-kubectl>` Die `aws_auth` `ConfigMap` ist konfiguriert und der Zugriff wird gewährt.	

Validieren der CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die CI/CD-Pipeline automatisch initiiert wird.	1. Die CodeSecurity Scan-Phase in der Pipeline schlägt normalerweise fehl, wenn Checkov Schwachstellen in den Dockerfile- oder Helm-Diagrammen erkennt. Der Zweck dieses Beispiels besteht jedoch darin, einen Prozess zur Identifizierung potenzieller Sicherheitsschwachstellen einzurichten, anstatt ihn über die CI/CD-Pipeline zu reparieren, in der Regel ein DevSecOps Prozess. In der Datei verwendet der `checkov` Befehl das `---soft-fail` Flag`buildspec/buildspec_secscan.yaml` , um Pipeline-Fehler zu vermeiden.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- echo -e "\n Running Dockerfile Scan"
	- checkov -f code/app/Dockerfile --framework dockerfile --soft-fail --summary-position bottom
	- echo -e "\n Running Scan of Helm Chart files"
	- cp -pv helm_charts/$EKS_CODEBUILD_APP_NAME/values.dev.yaml helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml
	- checkov -d helm_charts/$EKS_CODEBUILD_APP_NAME --framework helm --soft-fail --summary-position bottom
	- rm -rfv helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml</pre> Damit die Pipeline fehlschlägt, wenn Schwachstellen für die Dockerfile- und Helm-Diagramme gemeldet werden, muss die `--soft-fail` Option aus dem `checkov` Befehl entfernt werden. Entwickler oder	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Techniker können dann die Schwachstellen beheben und die Änderungen im CodeCommit Quellcode-Repository festschreiben. 2. Ähnlich wie CodeSecurity Scan verwendet die Build-Phase Bol Security Trivy, um HOHE und CRITIC Docker-Image-Schwachstellen zu identifizieren, bevor die Anwendung an Amazon ECR übertragen wird. In diesem Beispiel machen wir die Pipeline für Docker-Image-Schwachstellen nicht fehlschlagen. In der Datei enthält `buildspec/buildspec.yml` der `trivy` Befehl das -Flag `--exit-code` mit dem Wert `0`, weshalb die Pipeline nicht fehlschlägt, wenn HOHE oder CRITIC Docker-Image-Schwachstellen gemeldet werden. `- AWS_REGION=$AWS_DEFAULT_REGION AWS_ACCOUNT_ID=$AWS_ACCOUNT_ID trivy -d image --no-progress --ignore-unfixed --exit-code 0 --severity HIGH,CRITICAL --`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`format template -- template "@securit yhub/asff.tpl" -o securityhub/report .asff $AWS_ACCO UNT_ID.dkr.ecr.$AW S_DEFAULT_REGION.a mazonaws.com/$IMAG E_REPO_NAME:$CODEB UILD_RESOLVED_SOUR CE_VERSION` Damit die Pipeline fehlschlägt, wenn `HIGH, CRTICAL` Schwachstellen gemeldet werden, ändern Sie den Wert von `--exit-code` in 1. Entwickler oder Techniker können dann die Schwachstellen beheben und die Änderungen im CodeCommit Quellcode-Repository festschreiben. 3. Von Security Trivy gemeldete Docker-Image-Schwachstellen werden in Security Hub hochgeladen. Navigieren Sie in der AWS Security Hub-Konsole zu Erkenntnisse. Filtern Sie die Ergebnisse mit Datensatz status = Aktiv und Produkt = Sicherheit. Dadurch werden die Docker-Image-Schwachstellen in Security	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hub aufgeführt. Es kann 15 Minuten bis 1 Stunde dauern, bis Schwachstellen im Security Hub auftreten. Weitere Informationen zum Starten der Pipeline mithilfe von CodePipelinefinden Sie unter Starten einer Pipeline in CodePipeline, Manuelles Starten einer Pipeline und Starten einer Pipeline nach einem Zeitplan in der AWS-CodePipeline Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Genehmigen Sie die Bereitstellung.	1. Nachdem die Erstellungsphase abgeschlossen ist, gibt es ein Genehmigungs-Gate für die Bereitstellung. Der Prüfer oder ein Release Manager sollte den Build überprüfen und ihn, falls alle Anforderungen erfüllt sind, genehmigen. Dies ist der empfohlene Ansatz für Teams, die die kontinuierliche Bereitstellung für die Anwendungsbereitstellung verwenden. 2. Nach der Genehmigung initiiert die Pipeline die Bereitstellungsphase. 3. Nachdem die Bereitstellungsphase erfolgreich war, stellt das CodeBuild Protokoll für diese Phase die URL der Anwendung bereit. Verwenden Sie die URL, um die Bereitschaft der Anwendung zu überprüfen.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Anwendung sprofilerstellung.	Nachdem die Bereitstellung abgeschlossen ist und der Anwendungs-Pod in Amazon EKS bereitgestellt wird, versucht der in der Anwendung konfigurierte Amazon- CodeGuru Profiler-Agent, Profilerstellungsdaten der Anwendung (CPU, Heap-Zusammenfassung, Latenz und Engpässe) an Amazon CodeGuru Profiler zu senden. Für die erste Bereitstellung einer Anwendung benötigt Amazon CodeGuru Profiler etwa 15 Minuten, um die Profilerstellungsdaten zu visualisieren.	AWS DevOps

Zugehörige Ressourcen

- AWS- CodePipeline Dokumentation
- Scannen von Bildern mit Trivy in einem AWS CodePipeline (Blogbeitrag)
- Verbessern Ihrer Java-Anwendungen mit Amazon CodeGuru Profiler (Blogbeitrag)
- AWS Security Finding Format (ASFF)-Syntax
- Amazon- EventBridge Ereignismuster
- Helm-Upgrade

Zusätzliche Informationen

CodeGuru Profiler sollte in Bezug auf die Funktionalität nicht mit dem AWS X-Ray-Service verwechselt werden. CodeGuru Profiler wird bevorzugt, um die teuersten Codezeilen zu identifizieren,

die zu Engpässen oder Sicherheitsproblemen führen können, und sie zu beheben, bevor sie zu einem potenziellen Risiko werden. Der AWS X-Ray-Service dient der Überwachung der Anwendungsleistung.

In diesem Muster sind Ereignisregeln dem Standard-Event-Bus zugeordnet. Bei Bedarf können Sie das Muster erweitern, um einen benutzerdefinierten Event Bus zu verwenden.

Dieses Muster verwendet CodeGuru Reviewer als statisches Tool für Anwendungssicherheitstests (SAST) für Anwendungscode. Sie können diese Pipeline auch für andere Tools wie SonarQube oder Checkmarx verwenden. Die entsprechenden Scan-Setup-Anweisungen eines dieser Tools können in hinzugefügt werden `buildspec/buildspec_secscan.yaml`und ersetzen die Scan-Anweisungen von CodeGuru.

Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2-Instances

Erstellt von Durga Prasad Cheepuri (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Mikroservices; Cloud-nativ; Verwaltung und Verwaltung; Speicher und Backup; Web- und mobile Apps	AWS-Dienste: Amazon ECS; Amazon EFS

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zum Erstellen einer Amazon Elastic Container Service (Amazon ECS) -Aufgabendefinition, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der Amazon Web Services (AWS) -Cloud ausgeführt wird, während Amazon Elastic File System (Amazon EFS) zum Mounten eines Dateisystems auf diesen EC2-Instances verwendet wird. Amazon ECS-Aufgaben, die Amazon EFS verwenden, mounten automatisch die Dateisysteme, die Sie in der Aufgabendefinition angeben, und stellen diese Dateisysteme den Containern der Aufgabe in allen Availability Zones in einer AWS-Region zur Verfügung.

Um Ihre Anforderungen an persistenten Speicher und gemeinsam genutzten Speicher zu erfüllen, können Sie Amazon ECS und Amazon EFS zusammen verwenden. Sie können Amazon EFS beispielsweise verwenden, um persistente Benutzerdaten und Anwendungsdaten für Ihre Anwendungen mit aktiven und Standby-ECS-Containerpaaren zu speichern, die in verschiedenen Availability Zones laufen, um eine hohe Verfügbarkeit zu gewährleisten. Sie können Amazon EFS auch verwenden, um gemeinsam genutzte Daten zu speichern, auf die parallel von ECS-Containern und verteilten Job-Workloads zugegriffen werden kann.

Um Amazon EFS mit Amazon ECS zu verwenden, können Sie einer Aufgabendefinition eine oder mehrere Volume-Definitionen hinzufügen. Eine Volume-Definition umfasst eine Amazon EFS-Dateisystem-ID, eine Zugriffspunkt-ID und eine Konfiguration für die AWS Identity and Access Management (IAM) -Autorisierung oder die Transport Layer Security (TLS) -Verschlüsselung bei der Übertragung. Sie können Containerdefinitionen innerhalb von Aufgabendefinitionen verwenden, um die Aufgabendefinitionsvolumes anzugeben, die bei der Ausführung des Containers bereitgestellt

werden. Wenn eine Aufgabe ausgeführt wird, die ein Amazon EFS-Dateisystem verwendet, stellt Amazon ECS sicher, dass das Dateisystem bereitgestellt ist und für die Container verfügbar ist, die Zugriff darauf benötigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Virtual Private Cloud (VPC) mit einem Virtual Private Network (VPN) -Endpunkt oder einem Router
- (Empfohlen) Amazon ECS-Container-Agent 1.38.0 oder höher aus Gründen der Kompatibilität mit Amazon EFS-Zugriffspunkten und IAM-Autorisierungsfunktionen (Weitere Informationen finden Sie im AWS-Blogbeitrag Neu für Amazon EFS — IAM-Autorisierung und Zugriffspunkte.)

Einschränkungen

- Amazon ECS-Container-Agent-Versionen vor 1.35.0 unterstützen keine Amazon EFS-Dateisysteme für Aufgaben, die den EC2-Starttyp verwenden.

Architektur

Das folgende Diagramm zeigt ein Beispiel für eine Anwendung, die Amazon ECS verwendet, um eine Aufgabendefinition zu erstellen und ein Amazon EFS-Dateisystem auf EC2-Instances in ECS-Containern zu mounten.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen Sie ein Amazon EFS-Dateisystem.
2. Erstellen Sie eine Aufgabendefinition mit einem Container.
3. Konfigurieren Sie die Container-Instances für das Mounten des Amazon EFS-Dateisystems. Die Aufgabendefinition verweist auf die Volume-Mounts, sodass die Container-Instance das Amazon EFS-Dateisystem verwenden kann. ECS-Aufgaben haben Zugriff auf dasselbe Amazon EFS-Dateisystem, unabhängig davon, auf welcher Container-Instance diese Aufgaben erstellt werden.
4. Erstellen Sie einen Amazon ECS-Service mit drei Instanzen der Aufgabendefinition.

Technologie-Stack

- Amazon EC2
- Amazon ECS
- Amazon EFS

Tools

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können Amazon EC2 verwenden, um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können horizontal oder horizontal skalieren.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Um mehr Kontrolle über Ihre Infrastruktur zu erhalten, können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von EC2-Instances ausführen, die Sie verwalten.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS-CLI-Befehle, die Funktionen implementieren, die denen entsprechen, die von der browserbasierten AWS-Managementkonsole bereitgestellt werden, von einer Befehlszeile aus ausführen.

Epen

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie mithilfe der AWS-Managementkonsole ein Amazon EFS-Dateisystem.	1. Erstellen Sie ein Amazon EFS-Dateisystem und wählen Sie die VPC aus,	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Ihre Container enthält. Hinweis: Wenn Sie eine andere VPC verwenden, richten Sie eine VPC-Peering-Verbindung ein. 2. Notieren Sie sich die File system ID (Dateisystem-ID).	

Erstellen Sie eine Amazon ECS-Aufgabendefinition, indem Sie entweder ein Amazon EFS-Dateisystem oder die AWS-CLI CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabendefinition mit einem Amazon EFS-Dateisystem.	Erstellen Sie eine Aufgabendefinition mithilfe der neuen Amazon ECS-Konsole oder der klassischen Amazon ECS-Konsole mit den folgenden Konfigurationen: • Wenn Sie die neue Konsole verwenden, wählen Sie Amazon EC2 EC2-Instances für die App-Umgebung. Wenn Sie die klassische Konsole verwenden, wählen Sie EC2 als Starttyp. • Fügen Sie ein Volume hinzu. Geben Sie einen Namen für das Volume ein, wählen Sie EFS als Volumetyp und wählen Sie dann die Dateisystem-ID, die Sie zuvor notiert	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	haben. Wählen Sie für das Stammverzeichnis den Amazon EFS-Datei systempfad, den Sie auf dem Amazon ECS-Conta iner-Host hosten möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie mit der AWS-CLI eine Aufgabendefinition.	1. Führen Sie den folgenden Befehl aus, um eine JSON-Vorlage mit Platzhaltern für Eingabeparameter für Ihre Aufgabendefinition zu erstellen:
	`aws ecs register-task-definition --generate-cli-skeleton`
	2. Führen Sie den folgenden Befehl aus, um die Aufgabendefinition mit der JSON-Vorlage zu erstellen:
	`aws ecs register-task-definition --cli-input-json file://<path_to_your_json_file>`
	3. Geben Sie die Eingabeparameter in Ihre JSON-Vorlage ein, die auf der `task_definition_parameters.json` Datei (angehängt) basieren. Hinweis: Weitere Informationen zu Eingabeparametern finden Sie unter Aufgabendefinitionsparameter (Amazon ECS-Dokumentation) und
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	register-task-definition(AWS CLI Command Reference).	

Zugehörige Ressourcen

- Amazon ECS-Aufgabendefinitionen
- Amazon EFS-Volumes

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Bereitstellen von Java-Microservices auf Amazon ECS mithilfe von AWS Fargate

Erstellt von Vijay Thompson (AWS) und Sandeep Bondugula (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Container	Ziel: Amazon ECS
R-Typ: N/A	Technologien: Container und Mikroservices; Web- und mobile Apps	AWS-Dienste: Amazon ECS

Übersicht

Dieses Muster bietet Anleitungen für die Bereitstellung containerisierter Java-Mikroservices auf Amazon Elastic Container Service (Amazon ECS) mithilfe von AWS Fargate. Das Muster verwendet Amazon Elastic Container Registry (Amazon ECR) nicht für die Containerverwaltung. Stattdessen werden Docker-Images von einem Docker-Hub abgerufen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Java-Microservices-Anwendung auf einem Docker-Hub
- Ein öffentliches Docker-Repository
- Ein aktives AWS-Konto
- Vertrautheit mit AWS-Services, einschließlich Amazon ECS und Fargate
- Docker-, Java- und Spring Boot-Framework
- Amazon Relational Database Service (Amazon RDS) ist betriebsbereit (optional)
- Eine virtuelle private Cloud (VPC), wenn für die Anwendung Amazon RDS erforderlich ist (optional)

Architektur

Quelltechnologie-Stack

- Java-Mikroservices (z. B. in Spring Boot implementiert) und auf Docker bereitgestellt

Quellarchitektur

Zieltechnologie-Stack

- Ein Amazon ECS-Cluster, der jeden Microservice mithilfe von Fargate hostet
- Ein VPC-Netzwerk zum Hosten des Amazon ECS-Clusters und der zugehörigen Sicherheitsgruppen
- Eine Cluster-/Aufgabendefinition für jeden Microservice, der Container mithilfe von Fargate hochfährt

Zielarchitektur

Tools

Tools

- Amazon ECS macht es überflüssig, Ihre eigene Container-Orchestrierungssoftware zu installieren und zu betreiben, einen Cluster von virtuellen Maschinen zu verwalten und zu skalieren oder Container auf diesen virtuellen Maschinen zu planen.
- Mit AWS Fargate können Sie Container ausführen, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Docker ist eine Softwareplattform, mit der Sie Anwendungen schnell erstellen, testen und bereitstellen können. Docker packt Software in standardisierte Einheiten, sogenannte Container, die alles enthalten, was die Software zum Ausführen benötigt, einschließlich Bibliotheken, Systemtools, Code und Laufzeit.

Docker-Code

Das folgende Dockerfile gibt die verwendete Version des Java Development Kit (JDK) an, in der die Java-Archivdatei (JAR) vorhanden ist, die Portnummer, die verfügbar gemacht wird, und den Einstiegspunkt für die Anwendung.

```
FROM openjdk:11
ADD target/Spring-docker.jar Spring-docker.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Epen

Neue Aufgabendefinitionen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabend efinition.	Für die Ausführung eines Docker-Containers in Amazon ECS ist eine Aufgabend efinition erforderlich. Öffnen Sie die Amazon ECS-Konso le unter https://console.a ws.amazon.com/ecs/, wählen Sie Aufgabendefinitionen und erstellen Sie dann eine neue Aufgabendefinition. Weitere Informationen finden Sie in der Amazon ECS-Dokumentation.	AWS-Systemadministrator, App-Entwickler
Wählen Sie den Starttyp.	Wählen Sie Fargate als Starttyp.	AWS-Systemadministrator, App-Entwickler
Konfigurieren Sie die Aufgabe.	Definieren Sie einen Aufgabennamen und konfiguri eren Sie die Anwendung mit der entsprechenden Menge an Aufgabenspeicher und CPU.	AWS-Systemadministrator, App-Entwickler
Definieren Sie den Container.	Geben Sie den Namen des Containers an. Geben Sie für das Image den Namen der Docker-Site, den Repositor y-Namen und den Tag-	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen des Docker-Images ein ()`docker.io/sample-repo/sample-application:sample-tag-name` . Legen Sie Speicherlimits für die Anwendung und Portzuordnungen (`8080, 80`) für die zulässigen Ports fest.	
Erstellen Sie die Aufgabe.	Wenn die Aufgaben- und Containerkonfigurationen vorhanden sind, erstellen Sie die Aufgabe. Detaillierte Anweisungen finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	AWS-Systemadministrator, App-Entwickler

Konfigurieren Sie den Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen Cluster.	Wählen Sie als Clustertyp nur Networking aus, konfigurieren Sie den Namen und erstellen Sie dann den Cluster oder verwenden Sie einen vorhandenen Cluster, falls verfügbar. Weitere Informationen finden Sie in der Amazon ECS-Dokumentation.	AWS-Systemadministrator, App-Entwickler

Aufgabe konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabe.	Wählen Sie im Cluster die Option Neue Aufgabe ausführen aus.	AWS-Systemadministrator, App-Entwickler
Wählen Sie den Starttyp.	Wählen Sie Fargate als Starttyp.	AWS-Systemadministrator, App-Entwickler
Wählen Sie Aufgabendefinition , Revision und Plattform version.	Wählen Sie die Aufgabe, die Sie ausführen möchten, die Version der Aufgabendefinition und die Plattformversion aus.	AWS-Systemadministrator, App-Entwickler
Wählen Sie den -Cluster.	Wählen Sie den Cluster aus, von dem aus Sie die Aufgabe ausführen möchten.	AWS-Systemadministrator, App-Entwickler
Geben Sie die Anzahl der Aufgaben an.	Konfigurieren Sie die Anzahl der Aufgaben, die ausgeführ t werden sollen. Wenn Sie mit zwei oder mehr Aufgaben starten, ist ein Load Balancer erforderlich, um den Datenverkehr auf die Aufgaben zu verteilen.	AWS-Systemadministrator, App-Entwickler
Geben Sie die Aufgabeng ruppe an.	(Optional) Geben Sie einen Aufgabengruppennamen an, um eine Gruppe verwandter Aufgaben als Aufgabengruppe zu identifizieren.	AWS-Systemadministrator, App-Entwickler
Konfigurieren Sie die Cluster-VPC, die Subnetze und die Sicherheitsgruppen.	Konfigurieren Sie die Cluster-VPC und die Subnetze, in denen Sie die Anwendung	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereitstellen möchten. Erstellen oder aktualisieren Sie Sicherheitsgruppen (HTTP, HTTPS und Port 8080), um den Zugriff auf eingehende und ausgehende Verbindungen zu ermöglichen.	
Konfigurieren Sie öffentliche IP-Einstellungen.	Aktivieren oder deaktivie ren Sie die öffentliche IP, je nachdem, ob Sie eine öffentlic he IP-Adresse für Fargate-A ufgaben verwenden möchten. Die empfohlene Standardo ption ist Aktiviert.	AWS-Systemadministrator, App-Entwickler
Überprüfen Sie die Einstellu ngen und erstellen Sie die Aufgabe	Überprüfen Sie Ihre Einstellu ngen und wählen Sie dann Task ausführen.	AWS-Systemadministrator, App-Entwickler

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Anwendung s-URL.	Wenn der Aufgabenstatus auf Wird ausgeführt aktualisi ert wurde, wählen Sie die Aufgabe aus. Kopieren Sie im Bereich Netzwerk die öffentlic he IP.	AWS-Systemadministrator, App-Entwickler
Testen Sie Ihre Anwendung.	Geben Sie in Ihrem Browser die öffentliche IP ein, um die Anwendung zu testen.	AWS-Systemadministrator, App-Entwickler

Zugehörige Ressourcen

- Docker-Grundlagen für Amazon ECS (Amazon ECS-Dokumentation)
- Amazon ECS auf AWS Fargate (Amazon ECS-Dokumentation)
- Eine Aufgabendefinition erstellen (Amazon ECS-Dokumentation)
- Einen Cluster erstellen (Amazon ECS-Dokumentation)
- Konfiguration grundlegender Serviceparameter (Amazon ECS-Dokumentation)
- Konfiguration eines Netzwerks (Amazon ECS-Dokumentation)
- Bereitstellung von Java-Microservices auf Amazon ECS (Blogbeitrag)

Stellen Sie mit Amazon ECR und AWS Fargate Java-Microservices auf Amazon ECS bereit

Erstellt von Vijay Thompson (AWS) und Sandeep Bondugula (AWS)

Umgebung: PoC oder Pilot	Quelle: Container	Ziel: Amazon ECS
R-Typ: N/A	Technologien: Container und Mikroservices; Web- und mobile Apps	AWS-Dienste: Amazon ECS

Übersicht

Dieses Muster führt Sie durch die Schritte zur Bereitstellung von Java-Microservices als containerisierte Anwendungen in Amazon Elastic Container Service (Amazon ECS). Das Muster verwendet außerdem Amazon Elastic Container Registry (Amazon ECR) für die Verwaltung Ihres Containers und AWS Fargate für den Betrieb Ihres Containers.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Java-Microservices-Anwendung, die lokal auf Docker ausgeführt wird
- Ein aktives AWS-Konto
- Vertrautheit mit Amazon ECR, Amazon ECS, AWS Fargate und AWS Command Line Interface (AWS CLI)
- Vertrautheit mit Java- und Docker-Software

Produktversionen

- AWS CLI Version 1.7 oder höher

Architektur

Quelltechnologie-Stack

- Java-Microservices (z. B. mit Spring Boot entwickelt) und lokal bereitgestellt
- Docker

Quellarchitektur

Zieltechnologie-Stack

- Amazon ECR
- Amazon ECS
- AWS Fargate

Zielarchitektur

Tools

Tools

- Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Registry, die es Entwicklern erleichtert, Docker-Container-Images zu speichern, zu verwalten und bereitzustellen. Amazon ECR ist in Amazon ECS integriert, um Ihren development-to-production Arbeitsablauf zu vereinfachen. Amazon ECR hostet Ihre Images in einer hochverfügbaren und skalierbaren Architektur, sodass Sie Container für Ihre Anwendungen zuverlässig bereitstellen können. Die Integration mit AWS Identity and Access Management (IAM) ermöglicht die Kontrolle jedes Repositorys auf Ressourcenebene.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, leistungsstarker Container-Orchestrierungsservice, der Docker-Container unterstützt und es Ihnen ermöglicht, containerisierte Anwendungen auf AWS einfach auszuführen und zu skalieren. Mit Amazon ECS müssen Sie keine eigene Container-Orchestrierungssoftware installieren und betreiben, einen Cluster von virtuellen Maschinen verwalten und skalieren oder Container auf diesen virtuellen Maschinen planen.
- AWS Fargate ist eine Rechen-Engine für Amazon ECS, mit der Sie Container ausführen können, ohne Server oder Cluster verwalten zu müssen. Mit AWS Fargate müssen Sie keine Cluster von virtuellen Maschinen mehr bereitstellen, konfigurieren und skalieren, um Container auszuführen.

Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Cluster skaliert werden oder das Cluster-Packing optimiert werden.

- Docker ist eine Plattform, mit der Sie Anwendungen in Paketen, sogenannten Containern, erstellen, testen und bereitstellen können.

Code

Im Folgenden wird die verwendete Version des Java Development Kit (JDK) DockerFile angegeben, in der die Java-Archivdatei (JAR) vorhanden ist, die Portnummer, die verfügbar gemacht wird, und der Einstiegspunkt für die Anwendung.

```
FROM openjdk:8
 ADD target/Spring-docker.jar Spring-docker.jar
 EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Epen

Erstellen Sie ein Amazon ECR-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein -Repository.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon ECR-Konsole unter https://console.aws.amazon.com/ecr/repositories. Erstellen Sie ein privates Repository. Anweisungen finden Sie in der Amazon ECR-Dokumentation unter Erstellen eines privaten Repositorys.	Entwickler, Systemadm inistrator
Laden Sie das Projekt hoch.	Öffnen Sie das Repository und wählen Sie Push-Befe hle anzeigen. Folgen Sie den angezeigten Schritten, um das	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Projekt hochzuladen. (Diese Schritte funktionieren nur, wenn Sie AWS CLI Version 1.7 oder höher verwenden.) Wenn der Upload abgeschlossen ist, kopieren Sie die URL des Builds in das Repository. Sie verwenden diese URL, wenn Sie einen Container in Amazon ECS erstellen.	

Erstellen Sie den Container und starten Sie ihn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabendefinition.	Für die Ausführung eines Docker-Containers in Amazon ECS ist eine Aufgabendefinition erforderlich. Öffnen Sie die Amazon ECS-Konsole unter https://console.aws.amazon.com/ecs/, wählen Sie Aufgabendefinitionen und erstellen Sie eine neue Aufgabendefinition. Weitere Informationen finden Sie unter Erstellen einer Aufgabendefinition in der Amazon ECS-Dokumentation.	Entwickler, Systemadministrator
Wählen Sie den Starttyp.	Wählen Sie Fargate als Starttyp.	Entwickler, Systemadministrator
Konfigurieren Sie die Aufgabe.	Definieren Sie einen Aufgabennamen und konfiguri	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eren Sie die Anwendung mit der entsprechenden Menge an Aufgabenspeicher und CPU.	
Definieren Sie den Container.	Fügen Sie den Container hinzu und geben Sie einen Namen, die URL des Amazon ECR-Repositorys, Speicherl imits und Port-Zuordnung an. Die Ports 8080 und 80 sind für Portzuordnungen konfiguriert. Konfigurieren Sie die übrigen Einstellungen entsprechend Ihren Anwendungsanforder ungen.	Entwickler, Systemadm inistrator
Erstellen Sie die Aufgabe.	Wenn die Aufgaben- und Containerkonfigurationen vorhanden sind, erstellen Sie die Aufgabe. Detaillie rte Anweisungen finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	Entwickler, Systemadm inistrator

Erstellen Sie einen Amazon ECS-Cluster und konfigurieren Sie einen Service

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Cluster oder wählen Sie ihn aus.	Ein Amazon ECS-Cluster bietet eine logische Gruppieru ng von Aufgaben oder Services. Sie können sich dafür entscheiden, einen vorhandenen Cluster zu verwenden oder einen neuen	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cluster zu erstellen. Wenn Sie sich entscheiden, einen neuen Cluster zu erstellen , wählen Sie den Clustertyp entsprechend Ihren Anforderu ngen aus. In unserem Beispiel haben wir einen Netzwerkc luster ausgewählt. Geben Sie einen Namen für den Cluster ein und wählen Sie aus, ob Sie eine neue Virtual Private Cloud (VPC) für Fargate-A ufgaben erstellen möchten.	
Erstellen Sie einen Service.	Wählen Sie im Cluster die Option Create service aus.	Entwickler, Systemadm inistrator
Wählen Sie den Starttyp.	Wählen Sie Fargate als Starttyp.	Entwickler, Systemadm inistrator
Wählen Sie Aufgabendefinition , Revision und Plattform version.	Wählen Sie die Aufgabe aus, die Sie ausführen möchten, gefolgt von der Version der Aufgabendefinition und der Plattformversion.	Entwickler, Systemadm inistrator
Wählen Sie den -Cluster.	Wählen Sie aus der Dropdownliste den Cluster aus, in dem Sie Ihren Service erstellen möchten.	Entwickler, Systemadm inistrator
Geben Sie einen Dienstnamen an.	Geben Sie einen eindeutigen Namen für den Dienst ein, den Sie erstellen.	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Anzahl der Aufgaben an.	Konfigurieren Sie die Anzahl der Aufgaben, die beim Start des Dienstes ausgeführt werden sollen. Wenn Sie mit zwei oder mehr Aufgaben starten, ist ein Load Balancer erforderlich, um die Aufgaben auszugleichen. Die Mindestan zahl der zu konfigurierenden Aufgaben ist Eins.	Entwickler, Systemadm inistrator
Legen Sie die Mindest- und Höchstwerte für gesunde Werte fest.	Konfigurieren Sie die minimalen und maximalen fehlerfreien Prozentsätze für die Anwendung, oder akzeptieren Sie die bereitges tellte Standardoption.	Entwickler, Systemadm inistrator
Konfigurieren Sie die Bereitste llungseinstellungen.	Wählen Sie den Bereitste llungstyp entsprechend Ihren Anforderungen aus. Sie können ein fortlaufendes Update oder eine blaue/grüne Bereitstellung wählen.	Entwickler, Systemadm inistrator
Konfigurieren Sie die Cluster-VPC, die Subnetze und die Sicherheitsgruppen.	Konfigurieren Sie die Cluster-VPC, die Subnetze, in denen Sie die Anwendung bereitstellen möchten, und die Sicherheitsgruppen (HTTP, HTTPS und Port 8080) für den Zugriff auf eingehende/ ausgehende Verbindungen.	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die öffentlichen IP-Einstellungen.	Aktivieren oder deaktivieren Sie die öffentliche IP, je nachdem, ob Sie eine öffentliche IP-Adresse für Fargate-Aufgaben verwenden möchten.	Entwickler, Systemadministrator
Konfigurieren Sie den Lastenausgleich.	Konfigurieren Sie den Load Balancer, wenn Sie den Dienst mit mehr als einer Aufgabe starten. Sie müssen einen Load Balancer und seine Zielgruppe erstellen, bevor Sie den Service starten.	Entwickler, Systemadministrator
Konfigurieren Sie die automatische Skalierung.	Konfigurieren Sie Ihren Service so, dass er Amazon ECS Service Auto Scaling verwendet, um die gewünschte Anzahl von Aufgaben je nach Ihren Anforderungen nach oben oder unten anzupassen.	Entwickler, Systemadministrator
Überprüfen Sie die Einstellungen und erstellen Sie den Dienst.	Überprüfen Sie Ihre Diensteinstellungen und wählen Sie dann Dienst erstellen aus.	Entwickler, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihre Anwendung.	Testen Sie die Anwendung mithilfe des öffentlichen DNS, das bei der Bereitstellung der Aufgabe erstellt wird. Wenn	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Anwendung über einen Load Balancer verfügt, testen Sie die Anwendung, indem Sie ihn verwenden, und schalten Sie dann den Vorgang ab.	

Zugehörige Ressourcen

- Docker-Grundlagen für Amazon ECS (Amazon ECS-Dokumentation)
- Amazon ECS auf AWS Fargate (Amazon ECS-Dokumentation)
- Ein privates Repository erstellen (Amazon ECR-Dokumentation)
- Eine Aufgabendefinition erstellen (Amazon ECS-Dokumentation)
- Container-Definitionen (Amazon ECS-Dokumentation)
- Einen Cluster erstellen (Amazon ECS-Dokumentation)
- Konfiguration grundlegender Serviceparameter (Amazon ECS-Dokumentation)
- Konfiguration eines Netzwerks (Amazon ECS-Dokumentation)
- Konfiguration Ihres Service für die Verwendung eines Load Balancers (Amazon ECS-Dokumentation)
- Konfiguration Ihres Service für die Verwendung von Service Auto Scaling (Amazon ECS-Dokumentation)

Stellen Sie Java-Microservices auf Amazon ECS mithilfe von Amazon ECR und Load Balancing bereit

R-Typ: N/A	Quelle: Java	Ziel: Amazon ECS
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Web- und mobile Apps; Container und Microservices
AWS-Dienste: Amazon ECS		

Übersicht

Dieses Muster beschreibt die Schritte zur Bereitstellung einer containerisierten Java-Microservices-Architektur auf Amazon Elastic Container Service (Amazon ECS), um die Skalierung zu vereinfachen und die Entwicklung Ihrer Anwendungen zu beschleunigen. Dies trägt dazu bei, Innovationen zu ermöglichen und die Einführung neuer Funktionen time-to-market zu beschleunigen.

Das Muster verwendet außerdem Amazon Elastic Container Registry (Amazon ECR) zum Speichern und Verwalten der Docker-basierten Container sowie eine CloudFormation AWS-Vorlage mit einem Python-Skript, um die Einrichtung Ihrer Infrastruktur zu automatisieren. Das Muster basiert auf dem Beitrag Deploying Java Microservices on Amazon Elastic Container Service, der im AWS Compute-Blog veröffentlicht wurde.

Microservices bieten einen architektonischen und organisatorischen Ansatz für die Softwareentwicklung, bei dem Software aus kleinen, unabhängigen Services besteht, die über klar definierte Anwendungsprogrammierschnittstellen (APIs) kommunizieren. Kleine, in sich geschlossene Teams sind Eigentümer dieser Dienste.

Amazon ECS ist ein hoch skalierbarer, leistungsstarker Container-Orchestrierungsservice. Es unterstützt Docker-Container und ermöglicht es Ihnen, containerisierte Anwendungen auf AWS schnell auszuführen und zu skalieren. Mit Amazon ECS müssen Sie Ihre Container-Orchestrierungssoftware nicht mehr installieren und betreiben, einen Cluster von virtuellen Maschinen (VMs) verwalten und skalieren oder Container auf diesen VMs planen.

Mit einfachen API-Aufrufen können Sie Docker-fähige Anwendungen starten und beenden, den vollständigen Status Ihrer Anfrage abfragen und auf viele natürliche Funktionen zugreifen, wie z. B.

AWS Identity and Access Management (IAM) -Rollen, Sicherheitsgruppen, Load Balancer, Amazon CloudWatch Events, CloudFormation AWS-Vorlagen und AWS-Protokolle. CloudTrail

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java-Microservices-Quellcode mit Java Development Kit Version 1.7 oder höher
- Ein Zugriffsschlüssel und ein geheimer Zugriffsschlüssel für einen Benutzer im Konto
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- Java, AWS-Softwareentwicklungskit (SDK) für Python (Boto3) und Docker-Software
- Vertrautheit mit der Verwendung der vorherigen Technologien
- Vertrautheit mit AWS-Services wie Amazon ECS CloudFormation, AWS und Elastic Load Balancing

Architektur

Quelltechnologie-Stack

- Microservices, die in Java implementiert und auf Apache Tomcat in einer lokalen Umgebung bereitgestellt werden

Zieltechnologie-Stack

- Der Application Load Balancer, der die Client-Anfrage überprüft. Basierend auf Routing-Regeln leitet der Load Balancer die Anfrage an eine Instanz und einen Port der Zielgruppe weiter, die dem Status entsprechen.
- Eine Zielgruppe für jeden Microservice. Die Zielgruppen werden von den entsprechenden Diensten verwendet, um verfügbare Container-Instances zu registrieren. Jede Zielgruppe hat einen Pfad. Wenn Sie also den Weg für einen bestimmten Microservice aufrufen, wird er der richtigen Zielgruppe zugeordnet. Auf diese Weise können Sie einen Application Load Balancer verwenden, um alle Microservices zu bedienen, auf die über den Pfad zugegriffen wird. Beispielsweise würde https:///owner/ * dem Owner-Microservice zugeordnet und zu diesem weitergeleitet.
- Ein Amazon ECS-Cluster, der die Container für jeden Microservice hostet.

- Ein Amazon Virtual Private Cloud (Amazon VPC) -Netzwerk zum Hosten des Amazon ECS-Clusters und der zugehörigen Sicherheitsgruppen.
- Ein Amazon Elastic Container Registry (Amazon ECR) -Repository für jeden Microservice.
- Eine Service- oder Aufgabendefinition für jeden Microservice, der Container auf den Instances des Amazon ECS-Clusters hochfährt.

Zielarchitektur

Tools

- Amazon ECS — Mit Amazon ECS können Sie containerbasierte Anwendungen mit einfachen API-Aufrufen starten und beenden, den Status Ihres Clusters über einen zentralen Service abrufen und erhalten Zugriff auf viele vertraute Funktionen von Amazon Elastic Compute Cloud (Amazon EC2).
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Registry, die Entwicklern das Speichern, Verwalten und Bereitstellen von Docker-Container-Images erleichtert. Amazon ECR ist in Amazon ECS integriert, um Ihren development-to-production Arbeitsablauf zu vereinfachen. Amazon ECR hostet Ihre Images in einer hochverfügbaren und skalierbaren Architektur, sodass Sie Container für Ihre Anwendungen zuverlässig bereitstellen können. Die Integration mit AWS Identity and Access Management (IAM) ermöglicht die Kontrolle jedes Repositorys auf Ressourcenebene.

Epen

Erstellen Sie eine CloudFormation AWS-Vorlage, um einen Amazon ECS-Cluster zum Hosten der Java-Microservices einzurichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Amazon EC2 EC2-Linux-Instance bereit, installieren Sie Docker und erstellen Sie eine Docker-Da tei für jeden Microservice.		Ops

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Docker-Images auf Amazon ECR ein.	Verwenden Sie das Dockerfile für das Image, um das Image zu pushen, zu erstellen und es für Ihr neues Repositor y zu taggen. Machen Sie dasselbe für jeden Microserv ice. Schieben Sie die neu markierten Bilder in das Repository.	Ops
Erstellen Sie eine CloudForm ation AWS-Vorlage.	Erstellen Sie eine CloudForm ation AWS-Vorlage zur Bereitstellung der Virtual Private Cloud (VPC), des Amazon ECS-Clusters und des Amazon Relational Database Service (Amazon RDS).	Operationen

Bereitstellung von AWS-Services

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS-Infrastruktur mithilfe der CloudFormation Vorlage, die Sie zuvor erstellt haben.	Verwenden Sie das Python-Skript unter https://github.com /awslabs/amazon-ecs-java-mi croservices/blob/master/2_E CS_Java_Spring_ PetClinic _Microservices/setup.py, um die CloudFormation AWS-Vorlage aufzurufen, die Sie zuvor erstellt haben. Diese Vorlage erstellt die AWS-	Ops

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Infrastruktur, die Sie für die Zielumgebung benötigen.	
Erstellen Sie Amazon ECR-Repositorys, Aufgaben, Services, den Application Load Balancer und Zielgrupp en.	Das Python-Skript liest die Ausgaben der CloudFormation AWS-Vorlage und verwendet BOTO3-API-Aufrufe, um Amazon ECR-Repositorys, Aufgaben, Services, den Application Load Balancer und Zielgruppen zu erstellen.	Ops

Zugehörige Ressourcen

- Bereitstellung von Java-Microservices auf Amazon Elastic Container Service (AWS Compute-Blogbeitrag)
- Python-Skript
- Amazon ECS-Dokumentation
- Docker-Grundlagen für Amazon ECS
- AWS SDK für Python
- Amazon VPC-Dokumentation
- Amazon ECR-Dokumentation

Stellen Sie Kubernetes-Ressourcen und -Pakete mithilfe von Amazon EKS und einem Helm-Chart-Repository in Amazon S3 bereit

Erstellt von Sagar Panigrahi (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Mikroservices; DevOps	AWS-Dienste: Amazon EKS

Übersicht

Dieses Muster hilft Ihnen, Kubernetes-Anwendungen unabhängig von ihrer Komplexität effizient zu verwalten. Das Muster integriert Helm in Ihre bestehenden CI/CD-Pipelines (Continuous Integration and Continuous Delivery), um Anwendungen in einem Kubernetes-Cluster bereitzustellen. Helm ist ein Kubernetes-Paketmanager, der Sie bei der Verwaltung von Kubernetes-Anwendungen unterstützt. Helm-Diagramme helfen bei der Definition, Installation und Aktualisierung komplexer Kubernetes-Anwendungen. Diagramme können versioniert und in Helm-Repositorys gespeichert werden, wodurch die mittlere Wiederherstellungszeit (MTTR) bei Ausfällen verbessert wird.

Dieses Muster verwendet Amazon Elastic Kubernetes Service (Amazon EKS) für den Kubernetes-Cluster. Es verwendet Amazon Simple Storage Service (Amazon S3) als Helm-Diagramm-Repository, sodass die Diagramme zentral verwaltet und von Entwicklern im gesamten Unternehmen abgerufen werden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto mit einer Virtual Private Cloud (VPC)
- Ein Amazon EKS-Cluster
- Worker-Knoten, die innerhalb des Amazon EKS-Clusters eingerichtet sind und bereit sind, Workloads aufzunehmen
- Kubectl für die Konfiguration der Amazon EKS kubeconfig-Datei für den Zielcluster auf dem Client-Computer

- Zugriff auf AWS Identity and Access Management (IAM) zur Erstellung des S3-Buckets
- IAM-Zugriff (programmatischer oder Rollenzugriff) auf Amazon S3 vom Client-Computer aus
- Quellcodeverwaltung und eine CI/CD-Pipeline

Einschränkungen

- Derzeit wird das Aktualisieren, Löschen oder Verwalten von benutzerdefinierten Ressourcendefinitionen (CRDs) nicht unterstützt.
- Wenn Sie eine Ressource verwenden, die auf eine CRD verweist, muss die CRD separat installiert werden (außerhalb des Diagramms).

Produktversionen

- Helm v3.6.3

Architektur

Zieltechnologie-Stack

- Amazon EKS
- Amazon VPC
- Amazon S3
- Verwaltung des Quellcodes
- Helm
- Kubectl

Zielarchitektur

Automatisierung und Skalierung

- AWS CloudFormation kann verwendet werden, um die Erstellung der Infrastruktur zu automatisieren. Weitere Informationen finden Sie unter Erstellen von Amazon EKS-Ressourcen mit AWS CloudFormation in der Amazon EKS-Dokumentation.

- Helm soll in Ihr vorhandenes CI/CD-Automatisierungstool integriert werden, um die Paketierung und Versionierung von Helm-Diagrammen zu automatisieren (außerhalb des Geltungsbereichs dieses Musters).
- GitVersion oder Jenkins-Build-Nummern können verwendet werden, um die Versionierung von Diagrammen zu automatisieren.

Tools

Tools

- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service für die Ausführung von Kubernetes auf AWS, ohne dass Sie Ihre eigene Kubernetes-Steuerebene einrichten oder verwalten müssen. Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Anwendungen in Containern.
- Helm — Helm ist ein Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Kubectl — Kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.

Code

Der Beispielcode ist angehängt.

Epen

Helm konfigurieren und initialisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Helm-Client.	Verwenden Sie den folgenden Befehl, um den Helm-Client herunterzuladen und auf Ihrem lokalen System zu installieren.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sudo curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 | bash`	
Validieren Sie die Helm-Installation.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Helm mit dem Kubernetes-API-Server innerhalb des Amazon EKS-Clusters kommunizieren kann. `helm version`	DevOps Ingenieur

Erstellen und installieren Sie ein Helm-Diagramm im Amazon EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Helm-Diagramm für NGINX.	Führen Sie den Befehl aus, um ein Helmdiagramm mit dem Namen `my-nginx` auf dem Client-Computer zu erstellen. `helm create my-nginx`	DevOps Ingenieur
Überprüfen Sie die Struktur des Diagramms.	Um die Struktur des Diagramms zu überprüfen, führen Sie den Befehl tree aus`tree my-nginx/` .	DevOps Ingenieur
Deaktivieren Sie die Erstellung eines Dienstkontos im Diagramm.	Stellen Sie unter dem `serviceAccount` Abschnitt den `create` Schlüssel auf ein`false`. `values.yaml` Dies ist deaktiviert, da für	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieses Muster kein Dienstkonto erstellt werden muss.	
Überprüfe (linte) das geänderte Diagramm auf syntaktische Fehler.	Führen Sie den folgenden Befehl aus, um das Diagramm vor der Installation im Zielcluster auf syntaktische Fehler zu überprüfen. `helm lint my-nginx/`	DevOps Ingenieur
Installieren Sie das Diagramm, um Kubernetes-Ressourcen bereitzustellen.	Verwenden Sie den folgenden Befehl, um die Helm-Chart-Installation auszuführen. `helm install --name my-nginx-release --debug my-nginx/ --namespace helm-space` Das optionale `debug` Flag gibt alle Debug-Meldungen während der Installation aus. Das `namespace` Flag gibt den Namespace an, in dem der Ressourcenteil dieses Diagramms erstellt wird.	DevOps Ingenieur
Überprüfen Sie die Ressourcen im Amazon EKS-Cluster.	Verwenden Sie den folgenden Befehl, um die Ressourcen zu überprüfen, die als Teil des Helm-Diagramms im `helm-space` Namespace erstellt wurden. `kubectl get all -n helm-space`	DevOps Ingenieur

Gehen Sie zurück zu einer früheren Version einer Kubernetes-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern und aktualisieren Sie die Version.	Um das Diagramm zu ändern`values.yaml` , ändern Sie den `replicaCount` Wert in2. Aktualisieren Sie dann die bereits installierte Version, indem Sie den folgenden Befehl ausführen. `helm upgrade my-nginx-release my-nginx/ --namespace helm-space`	DevOps Ingenieur
Sehen Sie sich die Geschichte der Helm-Version an.	Führen Sie den folgenden Befehl aus, um alle Versionen für eine bestimmte Version aufzulisten, die mit Helm installiert wurden. `helm history my-nginx-release`	DevOps Ingenieur
Überprüfen Sie die Details für eine bestimmte Version.	Bevor Sie zu einer funktionierenden Version wechseln oder ein Rollback durchführen und für eine zusätzliche Überprüfungsebene vor der Installation einer Revision, sollten Sie mit dem folgenden Befehl überprüfen, welche Werte an die einzelnen Versionen übergeben wurden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`helm get --revision=2 my-nginx-release`	
Gehen Sie zurück zu einer früheren Version.	Verwenden Sie den folgenden Befehl, um zu einer früheren Version zurückzukehren. `helm rollback my-nginx-release 1` In diesem Beispiel wird auf Version 1 zurückgesetzt.	DevOps Ingenieur

Initialisieren Sie einen S3-Bucket als Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für Helm-Charts.	Erstellen Sie einen eindeutigen S3-Bucket. Erstellen Sie im Bucket einen Ordner mit dem Namen `charts`. Das Beispiel in diesem Muster verwendet `s3://my-helm-charts/charts` als Zieldiagramm-Repository.	Cloud-Administrator
Installieren Sie das Helm-Plugin für Amazon S3.	Verwenden Sie den folgenden Befehl, um das Helm-S3-Plugin auf Ihrem Client-Computer zu installieren. `helm plugin install https://github.com/hypnoglow/helm-s3.git --version 0.10.0`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Helm V3-Unterstützung ist mit der Plugin-Version 0.9.0 und höher verfügbar.	
Initialisieren Sie das Amazon S3 Helm-Repository.	Verwenden Sie den folgenden Befehl, um den Zielordner als Helm-Repository zu initialisieren. `helm S3 init s3://my-helm-charts/charts` Der Befehl erstellt eine `index.yaml` Datei im Ziel, um alle Diagramminformationen zu verfolgen, die an diesem Speicherort gespeichert sind.	DevOps Ingenieur
Fügen Sie das Amazon S3 S3-Repository zu Helm hinzu.	Verwenden Sie den folgenden Befehl, um das Repository auf dem Client-Computer hinzuzufügen. `helm repo add my-helm-charts s3://my-helm-charts/charts` Dieser Befehl fügt dem Ziel-Repository auf dem Helm-Client-Computer einen Alias hinzu.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Repository-Liste.	Führen `helm repo list` Sie den Befehl aus, um die Liste der Repositorys auf dem Helm-Client-Computer anzuzeigen.	DevOps Ingenieur

Package und Speichern von Diagrammen im Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verpacken Sie die Karte.	Führen Sie den Befehl aus, um das von Ihnen erstellte `my-nginx` Diagramm zu verpackenhelm package ./my-nginx/ . Der Befehl packt den gesamten Inhalt des `my-nginx` Diagrammordners in eine Archivdatei, die anhand der Versionsnummer benannt wird, die in der `Chart.yaml` Datei angegeben ist.	DevOps Ingenieur
Speichern Sie das Paket im Amazon S3 Helm-Repository.	Um das Paket in das Helm-Repository in Amazon S3 hochzuladen, führen Sie den folgenden Befehl aus und verwenden Sie dabei den richtigen Namen der `.tgz` Datei. `helm s3 push ./my-nginx-0.1.0.tgz my-helm-charts`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach der Helm-Karte.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Diagramm sowohl lokal als auch im Helm-Repository in Amazon S3 angezeigt wird. `helm search repo my-nginx`	DevOps Ingenieur

Ein Diagramm ändern, versionieren und verpacken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern und verpacken Sie das Diagramm.	Stellen Sie in `values.yaml` den `replicaCount` Wert auf ein`1`. Verpacken Sie dann das Diagramm`helm package ./my-nginx/` , indem Sie es ausführen und diesmal die Version in `Chart.yaml` ändern`0.1.1`. Die Versionierung wird idealerweise durch Automatisierung mithilfe von Tools wie GitVersion Jenkins-Build-Nummern in einer CI/CD-Pipeline aktualisiert. Die Automatisierung der Versionsnummer ist für dieses Muster nicht vorgesehen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pushen Sie die neue Version in das Helm-Repository in Amazon S3.	Führen Sie den folgenden Befehl aus, um das neue Paket mit Version 0.1.1 in das `my-helm-charts` Helm-Repository in Amazon S3 zu übertragen. `helm s3 push ./my-nginx-0.1.1.tgz my-helm-charts`	DevOps Ingenieur

Suchen und installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach allen Versionen des my-nginx-Diagramms.	Um alle verfügbaren Versionen eines Diagramms anzuzeigen, führen Sie den folgenden Befehl mit der Markierung aus. `--versions` `helm search repo my-nginx --versions` Ohne die Markierung zeigt Helm standardmäßig die zuletzt hochgeladene Version eines Diagramms an.	DevOps Ingenieur
Installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository.	Die Suchergebnisse der vorherigen Aufgabe zeigen die verschiedenen Versionen des `my-nginx` Diagramms.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwenden Sie den folgenden Befehl, um die neue Version (0.1.1) aus dem Amazon S3 Helm-Repository zu installie ren. `helm upgrade my-nginx-release my-helm-charts/my-nginx --version 0.1.1 --namespace helm-space`	

Zugehörige Ressourcen

- HELM-Dokumentation
- helm-S3-Plugin (MIT-Lizenz)
- BINÄRDATEI FÜR HELM-Cli
- Amazon EKS-Dokumentation

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Bereitstellen von Lambda-Funktionen mit Container-Images

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Container und Microservices; Cloudnativ; Softwareentwicklung und -tests; Serverless	Workload: Alle anderen Workloads
AWS-Services: Amazon EC2 Container Registry ;AWS Lambda		

Übersicht

AWS Lambda unterstützt Container-Images als Bereitstellungsmodell. Dieses Muster zeigt, wie Lambda-Funktionen über Container-Images bereitgestellt werden.

Lambda ist ein serverloser, ereignisgesteuerter Datenverarbeitungsservice, mit dem Sie Code für praktisch jeden Anwendungs- oder Backend-Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Mit der Unterstützung von Container-Images für Lambda-Funktionen erhalten Sie die Vorteile von bis zu 10 GB Speicher für Ihr Anwendungsartefakt und die Möglichkeit, vertraute Tools zur Entwicklung von Container-Images zu verwenden.

Das Beispiel in diesem Muster verwendet Python als zugrunde liegende Programmiersprache, aber Sie können andere Sprachen wie Java, Node.js oder Go verwenden. Das Muster verwendet AWS CodeCommit als Quelle, aber Sie könnten auch GitHub, Bitbucket oder Amazon Simple Storage Service (Amazon S3) verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Amazon Elastic Container Registry (Amazon ECR) aktiviert
- Anwendungscode
- Docker-Images mit dem Laufzeitschnittstellen-Client und der neuesten Version von Python

Einschränkungen

- Die maximal unterstützte Bildgröße beträgt 10 GB.
- Die maximale Laufzeit für eine Lambda-basierte Containerbereitstellung beträgt 15 Minuten.

Architektur

Zieltechnologie-Stack

- Python-Programmiersprache
- AWS CodeBuild
- AWS CodeCommit
- Docker-Image
- Amazon ECR
- AWS Identity and Access Management (IAM)
- AWS Lambda
- Amazon CloudWatch -Protokolle

Zielarchitektur

1. Sie erstellen ein Repository und übergeben den Anwendungscode mit CodeCommit.
2. Das CodeBuild Projekt wird initiiert, wenn eine Änderung an vorgenommen wird CodeCommit, das als Quellanbieter verwendet wird.
3. Das CodeBuild Projekt erstellt das Docker-Image und veröffentlicht das Image in Amazon ECR.
4. Sie erstellen die Lambda-Funktion, indem Sie das Image in Amazon ECR verwenden.

Automatisierung und Skalierung

Dieses Muster kann mithilfe von AWS CloudFormation, AWS Cloud Development Kit (AWS CDK) oder API-Operationen aus einem SDK automatisiert werden. Lambda kann basierend auf der Anzahl der Anfragen automatisch skalieren und Sie können es mithilfe der Gleichzeitigkeitsparameter optimieren. Weitere Informationen finden Sie in der Lambda-Dokumentation.

Tools

AWS-Services

- AWS CloudFormation Designer bietet einen integrierten JSON- und YAML-Editor, mit dem Sie CloudFormation Vorlagen anzeigen und bearbeiten können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeStar ist ein cloudbasierter Service zum Erstellen, Verwalten und Arbeiten mit Softwareentwicklungsprojekten in AWS. Für dieses Muster können Sie AWS CodeStar oder eine andere Entwicklungsumgebung verwenden.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

Andere Tools

- Docker ist eine Reihe von Platform as a Service (PaaS)-Produkten, die Virtualisierung auf Betriebssystemebene verwenden, um Software in Containern bereitzustellen.

Bewährte Methoden

- Machen Sie Ihre Funktion so effizient und klein wie möglich, um unnötiges Laden von Dateien zu vermeiden.
- Versuchen Sie, statische Ebenen höher in Ihrer Docker-Dateiliste zu haben, und platzieren Sie Ebenen, die sich häufiger nach unten ändern. Dies verbessert das Caching, was die Leistung verbessert.
- Der Image-Besitzer ist für das Aktualisieren und Patchen des Images verantwortlich. Fügen Sie diesen Aktualisierungsintervall zu Ihren Betriebsprozessen hinzu. Weitere Informationen finden Sie in der AWS Lambda-Dokumentation.

Polen

Erstellen eines Projekts in CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Erstellen Sie ein CodeCommit Repository, das das Dockerfile, die `buildspec.yaml` Datei und den Anwendung squellcode enthält. Weitere Informationen finden Sie in der AWS- CodeCommit Dokumentation.	Developer
Erstellen Sie ein CodeBuild Projekt.	Erstellen Sie in der -CodeBuild Konsole ein neues Projekt, das das CodeCommit Repo und die -`buildspec.yaml` Datei verwendet. Sie verwenden das CodeBuild Projekt, um das Image zu erstellen. Vergewissern Sie sich, dass der privilegierte Modus aktiviert ist. Zum Erstellen von Docker-Images ist dies erforderlich. Andernfalls wird das Image nicht erfolgreich erstellt. Geben Sie Werte für Projektname und Beschreibung an. Wählen Sie für den Quellanbieter aus CodeCommit. Weitere Informationen finden	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie in der AWS-Dokumentation.	
Bearbeiten Sie das Dockerfile.	Das Dockerfile sollte sich im Verzeichnis der obersten Ebene befinden, in dem Sie die Anwendung entwickeln. Der Python-Code sollte sich im `src` Ordner befinden. Wenn Sie das Image erstellen, verwenden Sie die offiziellen von Lambda unterstützten Images . Andernfalls tritt ein Bootstrap-Fehler auf, wodurch der Packvorgang schwieriger wird. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.	Developer
Erstellen Sie ein Repo in Amazon ECR.	Erstellen Sie ein Container-Repository in Amazon ECR. Im folgenden Beispielbefehl lautet der Name des erstellten Repositorys `cf-demo`. Das Repository wird in der `buildspec.yaml` Datei wiederverwendet. `aws ecr create-repository --cf-demo`	AWS-Administrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschieben Sie das Image zu Amazon ECR.	Sie können verwenden CodeBuild , um den Image-Build-Prozess durchzufü hren. CodeBuild benötigt die Berechtigung, mit Amazon ECR zu interagieren und mit S3 zu arbeiten. Im Rahmen des Prozesses wird das Docker-Image erstellt und an die Amazon-ECR-Registr ierung übertragen. Weitere Informationen zur Vorlage und zum Code finden Sie im Abschnitt Zusätzliche Informati onen.	Developer
Stellen Sie sicher, dass sich das Image im Repository befindet.	Um zu überprüfen, ob sich das Image im Repository befindet, wählen Sie in der Amazon-ECR-Konsole Repositorys aus. Das Image sollte mit Tags und mit den Ergebniss en eines Schwachstellenscan berichts aufgelistet werden, wenn diese Funktion in den Amazon-ECR-Einstellungen aktiviert wurde. Weitere Informationen finden Sie in der AWS-Dokumentation.	Developer

Erstellen der Lambda-Funktion zum Ausführen des Images

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	Wählen Sie in der Lambda-Konsole Funktion erstellen und dann Container-Image aus. Geben Sie den Funktionsnamen und den URI für das Image ein, das sich im Amazon-ECR-Repository befindet, und wählen Sie dann Funktion erstellen aus. Weitere Informationen finden Sie in der AWS Lambda-Dokumentation.	App-Developer
Testen Sie die Lambda-Funktion.	Um die Funktion aufzurufen und zu testen, wählen Sie Testen aus. Weitere Informationen finden Sie in der AWS Lambda-Dokumentation.	App-Developer

Fehlerbehebung

Problem	Lösung
Build ist nicht erfolgreich.	1. Überprüfen Sie, ob der privilegierte Modus für das CodeBuild Projekt aktiviert ist. 2. Stellen Sie sicher, dass die Docker-bezogenen Befehle über die erforderlichen Berechtigungen verfügen. Versuch, `sudo` zu den Befehlen hinzuzufügen. 3. Stellen Sie sicher, dass die mit verknüpfte IAM-Rolle über eine Richtlinie mit den entsprechenden Aktionen für die Interakti

Problem	Lösung
	on mit Amazon ECR, Amazon S3 und CloudWatch Protokollen CodeBuild verfügt.

Zugehörige Ressourcen

- Basis-Images für Lambda
- Docker-Beispiel für CodeBuild
- Temporäre Anmeldeinformationen übergeben

Zusätzliche Informationen

Bearbeiten der Docker-Datei

Der folgende Code zeigt die Befehle, die Sie im Dockerfile bearbeiten.

```
FROM public.ecr.aws/lambda/python:3.11

# Copy function code
COPY app.py ${LAMBDA_TASK_ROOT}
COPY requirements.txt  ${LAMBDA_TASK_ROOT}

# install dependencies
RUN pip3 install --user -r requirements.txt

# Set the CMD to your handler (could also be done as a parameter override outside of
 the Dockerfile)
CMD [ "app.lambda_handler" ]
```

Der `FROM` Befehlswert entspricht dem Python-3.11-Basis-Image, das die Lambda-Funktion im öffentlichen Amazon-ECR-Image-Repository verwendet.

Der `COPY app.py ${LAMBDA_TASK_ROOT}` Befehl kopiert den Code in das Aufgabenstammverzeichnis, das die Lambda-Funktion verwendet. Dieser Befehl verwendet die Umgebungsvariable , sodass wir uns keine Gedanken über den tatsächlichen Pfad machen müssen. Die auszuführende Funktion wird als Argument an den `CMD [ "app.lambda_handler" ]` Befehl übergeben.

Der `COPY requirements.txt` Befehl erfasst die für den Code erforderlichen Abhängigkeiten.

Der `RUN pip install --user -r requirements.txt` Befehl installiert die Abhängigkeiten im lokalen Benutzerverzeichnis.

Führen Sie den folgenden Befehl aus, um Ihr Image zu erstellen.

```
docker build -t <image name> .
```

Hinzufügen des Images in Amazon ECR

Ersetzen Sie im folgenden Code durch `aws_account_id` die Kontonummer und ersetzen Sie , `us-east-1` wenn Sie eine andere Region verwenden. Die `buildspec` Datei verwendet die CodeBuild Build-Nummer, um Image-Versionen eindeutig als Tag-Wert zu identifizieren. Sie können dies an Ihre Anforderungen anpassen.

Der benutzerdefinierte Code buildspec

```
phases:
  install:
    runtime-versions:
       python: 3.11
  pre_build:
    commands:
      - python3 --version
      - pip3 install --upgrade pip
      - pip3 install --upgrade awscli
      - sudo docker info
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - ls
      - cd app
      - docker build -t cf-demo:$CODEBUILD_BUILD_NUMBER .
      - docker container ls
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker image...
      - aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-east-1.amazonaws.com
```

```
      - docker tag cf-demo:$CODEBUILD_BUILD_NUMBER aws_account_id.dkr.ecr.us-
east-1.amazonaws.com/cf-demo:$CODEBUILD_BUILD_NUMBER
      - docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/cf-demo:
$CODEBUILD_BUILD_NUMBER
```

Stellen Sie einen Java-Beispiel-Microservice auf Amazon EKS bereit und stellen Sie den Microservice mithilfe eines Application Load Balancers bereit

Erstellt von Vijay Thompson (AWS) und Akkamahadevi microSDmath (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices	Workload: Open-Source
AWS-Services: Amazon EC2 Container Registry; Amazon EKS; Amazon ECR		

Übersicht

Dieses Muster beschreibt, wie Sie einen Java-Beispiel-Microservice als containerisierte Anwendung auf Amazon Elastic Kubernetes Service (Amazon EKS) mithilfe des `eksctl` Befehlszeilen-Dienstprogramms und Amazon Elastic Container Registry (Amazon ECR) bereitstellen. Sie können einen Application Load Balancer verwenden, um den Anwendungsverkehr auszugleichen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die AWS Command Line Interface (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert unter macOS , Linux oder Windows
- Ein laufender Docker-Daemon
- Das `eksctl` Befehlszeilen-Dienstprogramm, das unter macOS , Linux oder Windows installiert und konfiguriert wurde (weitere Informationen finden Sie unter Erste Schritte mit Amazon EKS – eksctl in der Amazon-EKS-Dokumentation.)
- Das `kubectl` Befehlszeilen-Dienstprogramm, das unter macOS , Linux oder Windows installiert und konfiguriert wurde (weitere Informationen finden Sie unter Installieren oder Aktualisieren von kubectl in der Amazon-EKS-Dokumentation.)

Einschränkungen

- Dieses Muster deckt die Installation eines SSL-Zertifikats für den Application Load Balancer nicht ab.

Architektur

Zieltechnologie-Stack

- Amazon ECR
- Amazon EKS
- Elastic Load Balancing

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Containerisierung eines Java-Microservice auf Amazon EKS.

Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container und IP-Adressen, in einer oder mehreren Availability Zones.
- eksctl hilft Ihnen beim Erstellen von Clustern auf Amazon EKS.
- kubectl ermöglicht das Ausführen von Befehlen für Kubernetes-Cluster.
- Docker hilft Ihnen beim Erstellen, Testen und Bereitstellen von Anwendungen in Paketen, die als Container bezeichnet werden.

Polen

Erstellen eines Amazon-EKS-Clusters mit eksctl

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-EKS-Cluster.	Führen Sie den folgenden Befehl aus, um einen Amazon-EKS-Cluster zu erstellen, der zwei t2.smallAmazon EC2 als Knoten verwendet: `eksctl create cluster --name <your-cluster-name> --version <version-number> --nodes=1 --node-type=t2.small` Hinweis: Der Vorgang kann zwischen 15 und 20 Minuten dauern. Nachdem der Cluster erstellt wurde, wird die entsprechende Kubernetes-Konfiguration zu Ihrer kubeconfig-Datei hinzugefügt. Sie können die `kubeconfig` Datei mit verwenden `kubectl`, um die Anwendung in späteren Schritten bereitzustellen.	Entwickler, Systemadministrator
Überprüfen Sie den Amazon-EKS-Cluster.	Um zu überprüfen, ob der Cluster erstellt wurde und ob Sie eine Verbindung zu ihm herstellen können, führen Sie den `kubectl get nodes` Befehl aus.	Entwickler, Systemadministrator

Erstellen Sie ein Amazon-ECR-Repository und übertragen Sie das Docker-Image.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Folgen Sie den Anweisungen unter Erstellen eines privaten Repositorys in der Amazon-ECR-Dokumentation.	Entwickler, Systemadministrator
Erstellen Sie eine POM-XML-Datei.	Erstellen Sie eine `pom.xml` Datei basierend auf dem Beispiel-POM-Dateicode im Abschnitt Zusätzliche Informationen dieses Musters.	Entwickler, Systemadministrator

Erstellen Sie eine Quelldatei.	Erstellen Sie eine Quelldatei mit dem Namen `HelloWorld.java` im `src/main/java/eksExample` Pfad basierend auf dem folgenden Beispiel:
	`package eksExample;`
	`import static spark.Spark.get;`
	
	`public class HelloWorld {`
	`  public static void main(String[] args) {`
	`  get("/", (req, res) -> {`
	`  return "Hello World!";`
	`  });`
	`  }`
	`}`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Stellen Sie sicher, dass Sie die folgende Verzeichnisstruktur verwenden:
	`### Dockerfile`
	`### deployment.yaml`
	`### ingress.yaml`
	`### pom.xml`
	`### service.yaml`
	`### src`
	`### main`
	`### java`
	`### eksExample`
	`### HelloWorld.java`	

Erstellen Sie eine Docker-Datei.	Erstellen Sie einen `Dockerfile` basierend auf dem Beispiel-Dockerfile-Code im Abschnitt Zusätzliche Informationen dieses Musters.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen und pushen Sie das Docker-Image.	Führen Sie in dem Verzeichnis, in dem Ihr das Image `Dockerfile` erstellen, markieren und an Amazon ECR übertragen soll, die folgenden Befehle aus:
	`aws ecr get-login -password --region <region>| docker login --username <username> --password-stdin <account_number>.dkr.ecr.<region>.amazonaws.com`
	`docker buildx build --platform linux/amd64 -t hello-world-java:v1 .`
	`docker tag hello-world-java:v1 <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	`docker push <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	Hinweis: Ändern Sie die AWS-Region, die Kontonummer und die Repository-Details in den vorherigen Befehlen. Achten Sie darauf, die Image-URL zur späteren Verwendung zu notieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Ein macOS-System mit einem M1-Chip hat ein Problem beim Erstellen eines Images, das mit Amazon EKS kompatibel ist, das auf einer AMD64-Plattform ausgeführt wird. Um dieses Problem zu beheben, verwenden Sie Docker buildx, um ein Docker-Image zu erstellen, das auf Amazon EKS funktioniert.	

Bereitstellen der Java-Microservices

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Bereitstellungsdatei.	Erstellen Sie eine YAML-Datei mit dem Namen `deployment.yaml` basierend auf dem Beispiel-Bereitstellungsdatencode im Abschnitt Zusätzliche Informationen dieses Musters. Hinweis: Verwenden Sie die Image-URL, die Sie zuvor kopiert haben, als Pfad der Image-Datei für das Amazon-ECR-Repository.	Entwickler, Systemadministrator
Stellen Sie die Java-Microservices auf dem Amazon-EKS-Cluster bereit.	Um eine Bereitstellung in Ihrem Amazon-EKS-Cluster zu erstellen, führen Sie den `kubectl apply -f`	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`deployment.yaml` Befehl aus.	
Überprüfen Sie den Status der Pods.	1. Führen Sie den `kubectl get pods` Befehl aus, um den Status der Pods zu überprüfen. 2. Warten Sie, bis sich der Status in Bereit ändert.	Entwickler, Systemadministrator
Erstellen Sie einen Service.	1. Erstellen Sie eine Datei mit dem Namen `service.yaml` basierend auf dem Beispiel-Servicedateicode im Abschnitt Zusätzliche Informationen dieses Musters. 2. Führen Sie den Befehl `kubectl apply -f service.yaml` aus.	Entwickler, Systemadministrator
Installieren Sie das Add-on AWS Load Balancer Controller.	Folgen Sie den Anweisungen unter Installieren des AWS Load Balancer Controller-Add-ons in der Amazon EKS-Dokumentation. Hinweis: Sie müssen das Add-on installiert haben, um einen Application Load Balancer oder Network Load Balancer für einen Kubernetes-Service zu erstellen.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ressource für eingehenden Datenverkehr.	Erstellen Sie eine YAML-Datei mit dem Namen `ingress.yaml` basierend auf dem Ressourcendateicode Beispiel für eingehenden Datenverkehr im Abschnitt Zusätzliche Informationen dieses Musters.	Entwickler, Systemadministrator
Erstellen Sie einen Application Load Balancer .	Um die Ressource für eingehenden Datenverkehr bereitzustellen und einen Application Load Balancer zu erstellen, führen Sie den `kubectl apply -f ingress.yaml` Befehl aus.	Entwickler, Systemadministrator

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen und überprüfen Sie die Anwendung.	1. Führen Sie den `kubectl get ingress.networking.k8s.io/java-microservice-ingress` Befehl aus, um den DNS-Namen des Load Balancers aus dem Feld ADDRESS abzurufen. 2. Führen Sie auf einer EC2-Instance in derselben VPC wie Ihre Amazon-EKS-Knoten den `curl -v <DNS address from`	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`previous command>` Befehl aus.	

Zugehörige Ressourcen

- Erstellen eines privaten Repositorys (Amazon-ECR-Dokumentation)
- Pushen eines Docker-Images (Amazon-ECR-Dokumentation)
- Controller für eingehenden Datenverkehr (Amazon-EKS-Workshop)
- Docker buildx (Docker-Dokumente)

Zusätzliche Informationen

POM-Beispieldatei

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>


  <groupId>helloWorld</groupId>
  <artifactId>helloWorld</artifactId>
  <version>1.0-SNAPSHOT</version>


  <dependencies>
    <dependency>
      <groupId>com.sparkjava</groupId><artifactId>spark-core</
artifactId><version>2.0.0</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
```

```
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-jar-plugin</
artifactId><version>2.4</version>
        <configuration><finalName>eksExample</finalName><archive><manifest>
              <addClasspath>true</addClasspath><mainClass>eksExample.HelloWorld</
mainClass><classpathPrefix>dependency-jars/</classpathPrefix>
            </manifest></archive>
        </configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-compiler-plugin</
artifactId><version>3.1</version>
        <configuration><source>1.8</source><target>1.8</target></configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-assembly-plugin</
artifactId>
        <executions>
          <execution>
            <goals><goal>attached</goal></goals><phase>package</phase>
            <configuration>
              <finalName>eksExample</finalName>
              <descriptorRefs><descriptorRef>jar-with-dependencies</descriptorRef></
descriptorRefs>
              <archive><manifest><mainClass>eksExample.HelloWorld</mainClass></
manifest></archive>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

Beispiel für Dockerfile

```
FROM bellsoft/liberica-openjdk-alpine-musl:17

RUN apk add maven
WORKDIR /code

# Prepare by downloading dependencies
ADD pom.xml /code/pom.xml
RUN ["mvn", "dependency:resolve"]
```

```
RUN ["mvn", "verify"]

# Adding source, compile and package into a fat jar
ADD src /code/src
RUN ["mvn", "package"]

EXPOSE 4567
CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]
```

Beispiel für eine Bereitstellungsdatei

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      containers:
      - name: java-microservice-container
        image: .dkr.ecr.amazonaws.com/:
        ports:
        - containerPort: 4567
```

Beispiel für eine Servicedatei

```
apiVersion: v1
kind: Service
metadata:
  name: "service-java-microservice"
spec:
  ports:
    - port: 80
      targetPort: 4567
      protocol: TCP
  type: NodePort
```

```
  selector:
    app.kubernetes.io/name: java-microservice
```

Beispiel für eine Ressourcendatei für eingehenden Datenverkehr

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: "java-microservice-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/load-balancer-name: apg2
    alb.ingress.kubernetes.io/target-type: ip
  labels:
    app: java-microservice
spec:
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: "service-java-microservice"
                port:
                  number: 80
```

Bereitstellen einer geclusterten Anwendung in Amazon ECS mithilfe von AWS Copilot

Erstellt von-Baptiste Guis (AWS), Mathew (AWS) und (AWS)

Code-Repository: Demo der geclusterten Beispielanwendung	Umgebung: Produktion	Technologien: Container und Microservices; Unternehmensproduktivität; Cloudnativ; Softwareentwicklung und -tests
AWS-Services: Amazon ECS; AWS Fargate; Amazon ECR		

Übersicht

Dieses Muster zeigt, wie Container in einem Amazon Elastic Container Service (Amazon ECS)-Cluster auf zwei Arten bereitgestellt werden – mithilfe der Amazon Web Services (AWS)-Managementkonsole und mithilfe von AWS Copilot –, um zu demonstrieren, wie AWS Copilot Bereitstellungsaufgaben vereinfacht.

Amazon ECS ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Stoppen und Verwalten von Containern in einem Cluster vereinfacht. Ihre Container sind in einer Aufgabendefinition definiert, die Sie zum Ausführen einzelner Aufgaben oder Aufgaben innerhalb eines Dienstes verwenden. Sie können Ihre Aufgaben und Services auf einer Serverless-Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Alternativ können Sie für mehr Kontrolle über Ihre Infrastruktur Ihre Aufgaben und Services auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2)-Instances ausführen, die Sie verwalten.

Die AWS-Copilot-Befehle der Befehlszeilenschnittstelle (Command Line Interface, CLI) vereinfachen das Erstellen, Freigeben und Betreiben produktionsbereiter containerisierter Anwendungen auf Amazon ECS aus einer lokalen Entwicklungsumgebung. Die AWS-Copilot-CLI richtet sich an Entwicklerworkflows, die moderne bewährte Methoden für Anwendungen unterstützen: von der Verwendung von Infrastruktur als Code bis hin zur Erstellung einer Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD), die im Namen eines Benutzers bereitgestellt

wird. Sie können die AWS-Copilot-CLI als Teil Ihres täglichen Entwicklungs- und Testzyklus als Alternative zur AWS-Managementkonsole verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Command Line Interface (AWS CLI) lokal installiert und für die Verwendung Ihres AWS-Kontos konfiguriert (siehe Installationsanweisungen und Konfigurationsanweisungen in der AWS CLI-Dokumentation)
- AWS Copilot lokal installiert (siehe Installationsanweisungen in der Amazon ECS-Dokumentation)
- Docker auf Ihrem lokalen Computer installiert (siehe Docker-Dokumentation)

Einschränkungen

- Docker erzwingt Pull-Limits von 100 Container-Images pro 6 Stunden pro IP-Adresse im kostenlosen Plan.

Architektur

Zieltechnologie-Stack

- AWS-Umgebung mit einer Virtual Private Cloud (VPC), öffentlichen und privaten Subnetzen und Sicherheitsgruppen eingerichtet
- Amazon-ECS-Cluster
- Amazon-ECS-Service und Aufgabendefinition
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon DynamoDB
- Application Load Balancer
- AWS Fargate
- Amazon Identity and Access Management (IAM)
- Amazon CloudWatch
- AWS CloudTrail

Zielarchitektur

Wenn Sie die Beispielanwendung für dieses Muster bereitstellen, werden mehrere Aufgaben in separaten Availability Zones erstellt und bereitgestellt. Jede Aufgabe speichert Daten in Amazon DynamoDB . Wenn Sie auf die Webseite für eine Aufgabe zugreifen, können Sie die Daten von allen anderen Aufgaben anzeigen.

Tools

AWS-Services

- Amazon ECR – Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. Amazon ECR unterstützt private Container-Image-Repositories mit ressourcenbasierten Berechtigungen unter Verwendung von IAM.
- Amazon ECS – Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Services auf einer Serverless-Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Alternativ können Sie für mehr Kontrolle über Ihre Infrastruktur Ihre Aufgaben und Services auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2)-Instances ausführen, die Sie verwalten.
- AWS-Copilot – AWS Copilot bietet eine Befehlszeilenschnittstelle, mit der Sie containerisierte Anwendungen in AWS starten und verwalten können, einschließlich des Pushs in eine Registrierung, der Erstellung einer Aufgabendefinition und der Erstellung eines Clusters.
- AWS Fargate – AWS Fargate ist eine Serverless- pay-as-you-go Compute-Engine, mit der Sie sich auf die Erstellung von Anwendungen konzentrieren können, ohne Server verwalten zu müssen. AWS Fargate ist sowohl mit Amazon ECS als auch mit Amazon Elastic Kubernetes Service (Amazon EKS) kompatibel. Wenn Sie Ihre Amazon-ECS-Aufgaben und -Services mit dem Starttyp Fargate oder einem Fargate-Kapazitätsanbieter ausführen, packen Sie Ihre Anwendung in Container, spezifizieren die CPU- und Arbeitsspeicheranforderungen, definieren Netzwerk- und IAM-Richtlinien und starten die Anwendung. Jede Fargate-Aufgabe hat ihre eigene Isolationsgrenze und verwendet den zugrunde liegenden Kernel, die CPU-Ressourcen, die Speicherressourcen oder die Elastic-Network-Schnittstelle nicht für eine andere Aufgabe.
- Amazon DynamoDB – Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.

- Elastic Load Balancing (ELB) – Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, z. B. EC2-Instances, Container und IP-Adressen, in einer oder mehreren Availability Zones. Es überwacht den Zustand der registrierten Ziele und leitet den Datenverkehr nur an die fehlerfreien Ziele weiter. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der eingehende Datenverkehr im Laufe der Zeit ändert. Es kann automatisch auf die meisten Workloads skaliert werden.

Tools

- Docker-Befehlszeilenschnittstelle
- AWS-Befehlszeilenschnittstelle (AWS CLI)
- AWS-Copilot-Befehlszeilenschnittstelle

Code

Der Code für die in diesem Muster verwendete Beispielanwendung ist auf GitHubim Cluster-Beispielanwendungs-Repository verfügbar. Folgen Sie den Anweisungen im nächsten Abschnitt, um die Beispieldateien zu verwenden.

Polen

Bereitstellen des Anwendungs-Stacks – Option 1 (AWS-Managementkonsole)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Beispiel-Code-Repository mit dem Befehl : `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	App-Entwickler, AWS DevOps
Erstellen Sie Ihr Amazon-ECR-Repository.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon ECR-Konsole unter https://console.aws.amazon.com/ecr/repositories. 2. Wählen Sie Repository erstellen aus. 3. Geben Sie für den Repository-Namen eincluster-sample-app. 4. Behalten Sie für alle anderen Einstellungen die Standardwerte bei. 5. Wählen Sie Repository erstellen aus. Weitere Informationen finden Sie unter Erstellen eines privaten Repositorys in der Amazon-ECR-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen, markieren und pushen Sie Ihr Docker-Image in Ihr Amazon ECR-Repos itory.	1. Wählen Sie das Repository aus, das Sie gerade erstellt haben, und wählen Sie Push-Befehle anzeigen aus.
	2. Kopieren Sie die angezeigt en Befehle und führen Sie sie lokal aus, um Ihr Docker-Image zu erstellen , zu markieren und zu pushen. Diese Befehle ähneln den folgenden.
	
	So authentifizieren Sie Ihren Docker-Client bei der Registrie rung:
	
	`aws ecr get-login -password --region <YOUR_AWS_REGION> | docker login --usernam e AWS --password-stdin <YOUR_AWS_ACCOUNT> .dkr.ecr.<YOUR_AWS _REGION>.amazonaws .com`
	
	So erstellen Sie Ihr Docker-Im age:
	
	`docker build -t cluster- sample-app .`
	
	So markieren Sie Ihr Docker-Image:
		App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`docker tag cluster-sample-app:latest <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com/cluster-sample-app:latest`
	
	So pushen Sie das Docker-Image in Ihr Repository:
	
	`docker push <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com/cluster-sample-app:latest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Anwendungs-Stack bereit.	1. Öffnen Sie die AWS-CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Wählen Sie Stack erstellen aus. 3. Wählen Sie im Abschnitt Vorlage vorbereiten die Option Vorlage ist bereit aus. 4. Wählen Sie im Abschnitt Specify template (Vorlage angeben) die Option Upload a template file (Vorlagen datei hochladen) aus. 5. Wählen Sie die lokale Datei aus `cluster-sample-app-stack.yml` , die Sie aus dem GitHub Repository als CloudFormation Vorlage geklont haben, und wählen Sie dann Weiter aus. 6. Geben Sie einen Namen für Ihren Stack ein und wählen Sie dann Weiter aus. 7. Behalten Sie alle Standardoptionen bei und wählen Sie dann Weiter aus. 8. Überprüfen Sie alle Optionen, bestätigen Sie die Erstellung von IAM-	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ressourcen und wählen Sie dann Stack erstellen aus. 9. Wenn Ihr Anwendungs-Stack bereitgestellt wurde, wählen Sie die Registerk arte Ausgabe, kopieren Sie die URL und öffnen Sie sie in Ihrem Browser, um auf die Anwendung zuzugreif en. Weitere Informationen zum Bereitstellen von CloudForm ation Vorlagen finden Sie unter Erstellen eines Stacks in der AWS- CloudFormation Dokumentation.	

Bereitstellen des Anwendungs-Stacks – Option 2 (AWS-Copilot-CLI)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Beispiel-Code-Repository mit dem Befehl : `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	App-Entwickler, AWS DevOps
Stellen Sie Ihr Container-Image mithilfe der AWS-Copilot-CLI in AWS bereit.	Stellen Sie die Anwendung in einem Schritt bereit, indem Sie den folgenden Befehl	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Stammverzeichnis Ihres Projekts verwenden: `copilot init --app cluster-sample-app --name demo --type "Load Balanced Web Service" --dockerfile ./Dockerfile --port 8080 --deploy` Sie sollten dann in der Lage sein, mithilfe des als Ausgabe bereitgestellten DNS-Namens auf die Anwendung zuzugreifen.	

Löschen der erstellten Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die über die AWS-Managementkonsole erstellten Ressourcen.	Wenn Sie Option 1 (die AWS-Managementkonsole) verwendet haben, um den Anwendungs-Stack bereitzustellen, gehen Sie wie folgt vor, wenn Sie bereit sind, die von Ihnen erstellten Ressourcen zu löschen: 1. Öffnen Sie die - CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie den Stack aus, den Sie erstellt haben, und wählen Sie dann Löschen aus. 3. Öffnen Sie die Amazon ECR-Konsole unter https://console.aws.amazon.com/ecr/repositories. 4. Wählen Sie das Repository aus, das Sie erstellt haben, und wählen Sie dann Löschen aus.	
Löschen Sie die von AWS Copilot erstellten Ressourcen.	Wenn Sie Option 2 (die AWS-Copilot-CLI) verwendet haben, um den Anwendungs-Stack bereitzustellen, führen Sie den folgenden Befehl aus dem Stammverzeichnis Ihres Projekts aus, wenn Sie bereit sind, die von Ihnen erstellten Ressourcen zu löschen: `copilot app delete`	App-Entwickler, AWS DevOps

Zugehörige Ressourcen

- Installieren oder Aktualisieren der neuesten Version der AWS CLI (AWS CLI-Dokumentation)
- Verwenden der AWS Copilot-Befehlszeilenschnittstelle (Amazon ECS-Dokumentation)
- Amazon ECS auf AWS Fargate (Amazon ECR-Dokumentation)
- Amazon-ECS-Dokumentation
- Amazon-ECR-Dokumentation
- Amazon- CloudFormation Dokumentation

- Docker Desktop (Docker-Dokumentation)

Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu

Erstellt von Kirankumar Chandrashekar (AWS) und Huy Nguyen (AWS)

grpc-traffic-on-albQuellcode-Repository: -to-eks	Umgebung: PoC oder Pilotprojekt	Technologien: Container und Mikroservices; Bereitstellung von Inhalten; Web- und mobile Apps
Arbeitslast: Alle anderen Workloads	AWS-Services: Amazon EKS; Elastic Load Balancing (ELB)	

Übersicht

Dieses Muster beschreibt, wie Sie eine GRPC-basierte Anwendung auf einem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster hosten und über einen Application Load Balancer sicher darauf zugreifen.

gRPC ist ein Open-Source-RPC-Framework (Remote Procedure Call), das in jeder Umgebung ausgeführt werden kann. Sie können es für Microservice-Integrationen und Client-Server-Kommunikation verwenden. Weitere Informationen zu gRPC finden Sie im AWS-Blogbeitrag Application Load Balancer Balancer-Unterstützung für end-to-end HTTP/2 und gRPC.

Dieses Muster zeigt Ihnen, wie Sie eine GRPC-basierte Anwendung hosten, die auf Kubernetes-Pods auf Amazon EKS ausgeführt wird. Der gRPC-Client stellt über das HTTP/2-Protokoll mit einer SSL/TLS-verschlüsselten Verbindung eine Verbindung zu einem Application Load Balancer her. Der Application Load Balancer leitet den Datenverkehr an die gRPC-Anwendung weiter, die auf Amazon EKS-Pods ausgeführt wird. Die Anzahl der gRPC-Pods kann mithilfe des Kubernetes Horizontal Pod Autoscaler automatisch auf der Grundlage des Datenverkehrs skaliert werden. Die Zielgruppe des Application Load Balancers führt Integritätsprüfungen an den Amazon EKS-Knoten durch, bewertet, ob das Ziel fehlerfrei ist, und leitet den Datenverkehr nur an fehlerfreie Knoten weiter.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows.
- eksctl, installiert und konfiguriert unter Linux, MacOS oder Windows.
- `kubectl`, installiert und konfiguriert für den Zugriff auf Ressourcen in Ihrem Amazon EKS-Cluster. Weitere Informationen finden Sie unter Installation oder Aktualisierung von kubectl in der Amazon EKS-Dokumentation.
- grpcURL, installiert und konfiguriert.
- Ein neuer oder vorhandener Amazon EKS-Cluster. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EKS.
- Ihr Computerterminal ist für den Zugriff auf den Amazon EKS-Cluster konfiguriert. Weitere Informationen finden Sie in der Amazon EKS-Dokumentation unter Konfiguration Ihres Computers für die Kommunikation mit Ihrem Cluster.
- AWS Load Balancer Controller, bereitgestellt im Amazon EKS-Cluster.
- Ein vorhandener DNS-Hostname mit einem gültigen SSL- oder SSL/TLS-Zertifikat. Sie können ein Zertifikat für Ihre Domain erhalten, indem Sie AWS Certificate Manager (ACM) verwenden oder ein vorhandenes Zertifikat auf ACM hochladen. Weitere Informationen zu diesen beiden Optionen finden Sie unter Anfordern eines öffentlichen Zertifikats und Importieren von Zertifikaten in AWS Certificate Manager in der ACM-Dokumentation.

Architektur

Das folgende Diagramm zeigt die durch dieses Muster implementierte Architektur.

Das folgende Diagramm zeigt einen Workflow, bei dem SSL/TLS-Verkehr von einem gRPC-Client empfangen wird, der auf einen Application Load Balancer auslagert. Der Datenverkehr wird im Klartext an den gRPC-Server weitergeleitet, da er aus einer Virtual Private Cloud (VPC) stammt.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Elastic Load Balancing verteilt den eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.

Tools

- eksctl ist ein einfaches CLI-Tool zum Erstellen von Clustern auf Amazon EKS.
- kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.
- AWS Load Balancer Controller unterstützt Sie bei der Verwaltung von AWS Elastic Load Balancers für einen Kubernetes-Cluster.
- GrpcURL ist ein Befehlszeilentool, mit dem Sie mit gRPC-Diensten interagieren können.

Code-Repository

Der Code für dieses Muster ist im GitHub grpc-traffic-on-alb-to-eks-Repository verfügbar.

Epen

Erstellen Sie das Docker-Image des gRPC-Servers und übertragen Sie es auf Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon ECR-Konsole und erstellen Sie	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann ein Amazon ECR-Repository. Weitere Informationen finden Sie unter Erstellen eines Repositorys in der Amazon ECR-Dokumentation. Stellen Sie sicher, dass Sie die URL des Amazon ECR-Repositorys aufzeichnen. Sie können auch ein Amazon ECR-Repository mit AWS CLI erstellen, indem Sie den folgenden Befehl ausführen: `aws ecr create-repository --repository-name helloworld-grpc`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das Docker-Image.	1. Klonen Sie das GitHub grpc-traffic-on-alb-to-eks-Repository.
	`git clone https://github.com/aws-samples/grpc-traffic-on-alb-to-eks.git`
	2. Stellen Sie im Stammverzeichnis des Repositorys sicher, dass das Dockerfile vorhanden ist, und führen Sie dann den folgenden Befehl aus, um das Docker-Image zu erstellen:
	`docker build -t <amazon_ecr_repository_url>:<Tag> .`
	Wichtig: Stellen Sie sicher, dass Sie es `<amazon_ecr_repository_url>` durch die URL des Amazon ECR-Repositorys ersetzen, das Sie zuvor erstellt haben.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie das Docker-Image an Amazon ECR.	1. Führen Sie den folgenden Befehl aus, um sich beim Amazon ECR-Repository anzumelden:
	`aws ecr get-login -password --region us-east-1 --no-cli-auto-prompt | docker login --username AWS --password-stdin <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com`
	2. Übertragen Sie das Docker-Image in das Amazon ECR-Repository, indem Sie den folgenden Befehl ausführen:
	`docker push <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-grpc:1.0`
	Wichtig: Stellen Sie sicher, dass Sie es `<your_aws_account_id>` durch Ihre AWS-Konto-ID ersetzen.
		DevOps Ingenieur

Stellen Sie die Kubernetes-Manifeste im Amazon EKS-Cluster bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Werte in der Kubernetes-Manifestdatei.	1. Ändern Sie die `grpc-sample.yaml` Kubernetes-Manifestdatei im Kubernetes-Ordner des Repositorys gemäß Ihren Anforderungen. Sie müssen die Anmerkungen und den Hostnamen in der Eingangsressource ändern. Ein Beispiel für eine Ingress-Ressource finden Sie im Abschnitt Zusätzliche Informationen. Weitere Informationen zu Eingangsanmerkungen finden Sie unter Eingangsanmerkungen in der Kubernetes-Dokumentation. 2. Ändern Sie in der Kubernetes-Bereitstellungsressource die Bereitstellungsressourcen in den Uniform Resource Identifier (URI) für das Amazon ECR-Repository, in das Sie das Docker-Image übertragen haben. `image` Ein Beispiel für eine Bereitstellungsressource finden Sie im Abschnitt Zusätzliche Informationen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Kubernetes-Manifestdatei bereit.	Stellen Sie die `grpc-sample.yaml` Datei im Amazon EKS-Cluster bereit, indem Sie den folgenden `kubectl` Befehl ausführen: `kubectl apply -f ./kubernetes/grpc-sample.yaml`	DevOps Ingenieur

Erstellen Sie den DNS-Eintrag für den FQDN des Application Load Balancers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie den FQDN für den Application Load Balancer.	1. Führen Sie den folgenden `kubectl` Befehl aus, um die Kubernetes-Eingangsressource zu beschreiben, die den Application Load Balancer verwaltet: `kubectl get ingress -n grpcserver` Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen. In der Ausgabe zeigt das `HOSTS` Feld den DNS-Hostnamen an, für den die SSL-Zertifikate erstellt wurden. 2. Notieren Sie den vollqualifizierten Domainnamen (FQDN) des Applicati	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on Load Balancers aus dem `Address` Feld der Ausgabe. 3. Erstellen Sie einen DNS-Eintrag, der auf den FQDN des Application Load Balancers verweist. Wenn Ihr DNS-Anbieter Amazon Route 53 ist, können Sie einen Aliaseintrag erstellen , der auf den FQDN des Application Load Balancers verweist. Weitere Informationen zu dieser Option finden Sie unter Auswahl zwischen Alias- und Nicht-Aliasdatensätzen in der Route 53 53-Dokumentation.	

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den gRPC-Server.	Verwenden Sie grpcURL, um den Endpunkt zu testen, indem Sie den folgenden Befehl ausführen: `grpcurl grpc.example.com:443 list grpc.reflection.v1alpha.ServerReflection helloworld.helloworld`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Ersetzen Sie es `grpc.example.com` durch Ihren DNS-Namen.	

Testen Sie den gRPC-Server mit einem gRPC-Client.	Ersetzen Sie im `helloworld_client_ssl.py` gRPC-Beispielclient den Hostnamen von `grpc.example.com` durch den Hostnamen, der für den gRPC-Server verwendet wird.
	
	Das folgende Codebeispiel zeigt die Antwort des gRPC-Servers auf die Anfrage des Clients:
	
	`python ./app/helloworld_client_ssl.py`
	`message: "Hello to gRPC server from Client"`
	
	`message: "Thanks for talking to gRPC server!! Welcome to hello world. Received message is \"Hello to gRPC server from Client\""`
	`received: true`
	
	Dies zeigt, dass der Client mit dem Server kommunizieren kann und dass die Verbindung erfolgreich ist.
		DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie den DNS-Eintrag.	Entfernen Sie den DNS-Eintrag, der auf den zuvor erstellten FQDN des Application Load Balancers verweist.	Cloud-Administrator
Entfernen Sie den Load Balancer.	Wählen Sie auf der Amazon EC2 EC2-Konsole Load Balancers und entfernen Sie dann den Load Balancer, den der Kubernetes-Controller für Ihre Eingangsressource erstellt hat.	Cloud-Administrator
Löschen Sie den Amazon EKS-Cluster.	Löschen Sie den Amazon EKS-Cluster mithilfe von `eksctl`: `eksctl delete cluster -f ./eks.yaml`	AWS DevOps

Zugehörige Ressourcen

- Netzwerklastenausgleich auf Amazon EKS
- Zielgruppen für Ihre Application Load Balancer

Zusätzliche Informationen

Beispiel für eine Ingress-Ressource:

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
```

```
  annotations:
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
    alb.ingress.kubernetes.io/ssl-redirect: "443"
    alb.ingress.kubernetes.io/backend-protocol-version: "GRPC"
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80}, {"HTTPS":443}]'
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
    alb.ingress.kubernetes.io/certificate-arn: arn:aws:acm:<AWS-
Region>:<AccountId>:certificate/<certificate_ID>
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
  labels:
    app: grpcserver
    environment: dev
  name: grpcserver
  namespace: grpcserver
spec:
  ingressClassName: alb
  rules:
  - host: grpc.example.com # <----- replace this as per your host name for which the
 SSL certtficate is available in ACM
    http:
      paths:
      - backend:
          service:
            name: grpcserver
            port:
              number: 9000
        path: /
        pathType: Prefix
```

Beispiel für eine Bereitstellungsressource:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: grpcserver
  namespace: grpcserver
spec:
  selector:
    matchLabels:
      app: grpcserver
  replicas: 1
  template:
```

```
    metadata:
      labels:
        app: grpcserver
    spec:
      containers:
      - name: grpc-demo
        image: <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-
grpc:1.0   #<------- Change to the URI that the Docker image is pushed to
        imagePullPolicy: Always
        ports:
        - name: grpc-api
          containerPort: 9000
        env:
        - name: POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
      restartPolicy: Always
```

Beispielausgabe:

```
NAME             CLASS           HOSTS                          Address
 PORTS          AGE
 grpcserver      <none>      <DNS-HostName>                 <ELB-address>
 80            27d
```

Bereitstellen und Debuggen von Amazon-EKS-Clustern

Erstellt von Svenja Raether (AWS) und Mathew Bol (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices; Infrastruktur; Modernisierung; Serverless; Cloudnativ	Workload: Alle anderen Workloads
AWS-Services: Amazon EKS; AWS Fargate		

Übersicht

Container werden zu einem wesentlichen Teil der Entwicklung cloudnativer Anwendungen. Kubernetes bietet eine effiziente Möglichkeit, Container zu verwalten und zu orchestrieren. Amazon Elastic Kubernetes Service (Amazon EKS) ist ein vollständig verwalteter, zertifizierter Kubernetes-konformer Service zum Erstellen, Sichern, Betreiben und Verwalten von Kubernetes-Clustern auf Amazon Web Services (AWS). Es unterstützt die Ausführung von Pods auf AWS Fargate, um On-Demand-Rechenkapazität in der richtigen Größe bereitzustellen.

Es ist wichtig, dass Entwickler und Administratoren die Debugging-Optionen kennen, wenn sie containerisierte Workloads ausführen. Dieses Muster führt Sie durch die Bereitstellung und das Debuggen von Containern auf Amazon EKS mit AWS Fargate . Dazu gehören das Erstellen, Bereitstellen, Zugreifen, Debuggen und Bereinigen der Amazon-EKS-Workloads.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Identity and Access Management (IAM)-Rolle, die mit ausreichenden Berechtigungen konfiguriert ist, um Amazon EKS, IAM-Rollen und serviceverknüpfte Rollen zu erstellen und mit ihnen zu interagieren
- AWS Command Line Interface (AWS CLI) ,die auf dem lokalen Computer installiert ist
- eksctl

- kubectl
- Helm

Einschränkungen

- Dieses Muster bietet Entwicklern nützliche Debugging-Methoden für Entwicklungsumgebungen. Es gibt keine bewährten Methoden für Produktionsumgebungen.
- Wenn Sie Windows ausführen, verwenden Sie Ihre betriebssystemspezifischen Befehle, um die Umgebungsvariablen festzulegen.

Verwendete Produktversionen

- AWS CLI Version 2
- kubectl-Version innerhalb eines Unterversionsunterschieds der von Ihnen verwendeten Amazon-EKS-Steuerebene
- Neueste Version von eksctl
- Helm v3

Architektur

Technologie-Stack

- Application Load Balancer
- Amazon EKS
- AWS Fargate

Zielarchitektur

Alle im Diagramm gezeigten Ressourcen werden mithilfe der `kubectl` Befehle `eksctl` und bereitgestellt, die von einem lokalen Computer ausgegeben werden. Private Cluster müssen von einer Instance ausgeführt werden, die sich in der privaten VPC befindet.

Die Zielarchitektur besteht aus einem EKS-Cluster, der den Starttyp Fargate verwendet. Dies bietet On-Demand-Rechenkapazität in richtiger Größe, ohne dass Servertypen angegeben werden müssen. Der EKS-Cluster verfügt über eine Steuerebene, die zur Verwaltung der Cluster-Knoten und

Workloads verwendet wird. Die Pods werden in privaten VPC-Subnetzen bereitgestellt, die sich über mehrere Availability Zones erstrecken. Auf die Amazon ECR Public Gallery wird verwiesen, um ein NGINX-Webserver-Image abzurufen und auf den Pods des Clusters bereitzustellen.

Das Diagramm zeigt, wie Sie mithilfe von -`kubectl`Befehlen auf die Amazon-EKS-Steuerebene zugreifen und wie Sie mithilfe des Application Load Balancers auf die Anwendung zugreifen.

.

1. Ein lokaler Computer außerhalb der AWS Cloud sendet Befehle an die Kubernetes-Steuerebene innerhalb einer von Amazon EKS verwalteten VPC.
2. Amazon EKS plant Pods basierend auf den Selektoren im Fargate-Profil.
3. Der lokale Computer öffnet die Application Load Balancer-URL im Browser.
4. Der Application Load Balancer teilt den Datenverkehr zwischen den Kubernetes-Pods in Fargate-Clusterknoten auf, die in privaten Subnetzen bereitgestellt werden, die sich über mehrere Availability Zones erstrecken.

Tools

AWS-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen. Dieses Muster verwendet auch das Befehlszeilen-Tool eksctl, um mit Kubernetes-Clustern auf Amazon EKS zu arbeiten.
- AWS Fargate unterstützt Sie bei der Ausführung von Containern, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2)-Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet die Steuerungskomponente des AWS Load Balancer Controllers, um den Application Load Balancer zu erstellen, wenn ein Kubernetes-Eingang

bereitgestellt wird. Der Application Load Balancer verteilt eingehenden Datenverkehr auf mehrere Ziele.

Andere Tools

- Helm ist ein Open-Source-Paketmanager für Kubernetes. In diesem Muster wird Helm verwendet, um den AWS Load Balancer Controller zu installieren.
- Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen.
- NGINX ist ein hochleistungsfähiger Web- und Reverse-Proxy-Server.

Polen

Erstellen eines EKS-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Dateien.	Erstellen Sie mithilfe des Codes im Abschnitt Zusätzliche Informationen die folgenden Dateien: • `clusterconfig-fargate.yaml` • `nginx-deployment.yaml` • `nginx-service.yaml` • `nginx-ingress.yaml` • `index.html`	App-Entwickler, AWS-Administrator, AWS DevOps
Legen Sie Umgebungsvariablen fest.	Hinweis: Wenn ein Befehl aufgrund früherer nicht abgeschlossener Aufgaben fehlschlägt, warten Sie einige Sekunden und führen Sie den Befehl dann erneut aus.	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Dieses Muster verwendet die AWS-Region und den Clusternamen, die in der Datei definiert sind`clusterconfig-fargate.yaml` . Legen Sie die gleichen Werte wie Umgebungsvariablen fest, um sie in weiteren Befehlen zu referenzieren.
	`export AWS_REGION="us-east-1"`
	`export CLUSTER_NAME="my-fargate"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen EKS-Cluster.	Führen Sie den folgenden Befehl aus, um einen EKS-Cluster zu erstellen, der die Spezifikationen aus der `-clusterconfig-fargate.yaml` Datei verwendet. `eksctl create cluster -f clusterconfig-fargate.yaml` Die Datei enthält die `ClusterConfig` , die einen neuen EKS-Cluster mit dem Namen `my-fargate-cluster` in der `us-east-1` Region und ein Fargate-Standardprofil () bereitstelltfp-default . Das Fargate-Standardprofil ist mit zwei Selektoren (`default` und `kube-system`) konfiguriert.	App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie den erstellten Cluster.	Führen Sie den folgenden Befehl aus, um den erstellten Cluster zu überprüfen.
	`eksctl get cluster --output yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`- Name: my-fargate`
	`  Owned: "True"`
	`  Region: us-east-1`
	Überprüfen Sie das erstellte Fargate-Profil mithilfe der `CLUSTER_NAME` .
	`eksctl get fargatepr ofile --cluster $CLUSTER_NAME --output yaml`
	Dieser Befehl zeigt Informationen zu den Ressourcen an. Sie können die Informationen verwenden, um den erstellten Cluster zu überprüfen. Die Ausgabe sollte wie folgt aussehen.
	`- name: fp-default`
	`  podExecutionRoleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cluster-FargatePod ExecutionRole-xxx`
	`  selectors:`
	`  - namespace: default`
	`  - namespace: kube-system`
	`  status: ACTIVE`
	`  subnets:`
	`  - subnet-aaa`
	`  - subnet-bbb`
	`  - subnet-ccc`	

Bereitstellen eines Containers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den NGINX-Web server bereit.	Führen Sie den folgenden Befehl aus, um die NGINX-Webserver-Bereitstellung auf den Cluster anzuwenden.
	`kubectl apply -f ./ nginx-deployment.yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`deployment.apps/nginx-deployment created`
	Die Bereitstellung umfasst drei Replikate des NGINX-Images aus der Amazon ECR Public Gallery. Das Image wird im Standard-Namespace bereitgestellt und auf Port
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	80 auf den laufenden Pods bereitgestellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellung und die Pods.	(Optional) Überprüfen Sie die Bereitstellung. Sie können den Status Ihrer Bereitstellung mit dem folgenden Befehl überprüfen.
	`kubectl get deployment`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME READY UP-TO-DATE AVAILABLE AGE nginx-deployment 3/3 3 3 7m14s`
	Ein Pod ist ein bereitstellbares Objekt in Kubernetes, das einen oder mehrere Container enthält. Führen Sie den folgenden Befehl aus, um alle Pods aufzulisten.
	`kubectl get pods`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME READY STATUS RESTARTS AGE`
		App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`nginx-deployment-xxxx-aaa 1/1 Running 0 94s`
	`nginx-deployment-xxxx-bbb 1/1 Running 0 94s`
	`nginx-deployment-xxxx-ccc 1/1 Running 0 94s`	

Skalieren Sie die Bereitstellung.	Verwenden Sie den folgenden Befehl, um die Bereitstellung von den drei Replikaten, die in angegeben wurden, `deployment.yaml` auf vier Replikate zu skalieren.
	`kubectl scale deployment nginx-deployment --replicas 4`
	Die Ausgabe sollte wie folgt aussehen.
	`deployment.apps/nginx-deployment scaled`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Bereitstellen eines AWS Load Balancer Controllers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Umgebungsvariablen fest.	Beschreiben Sie den CloudFormation Stack des Clusters, um Informationen über seine VPC abzurufen.	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws cloudformation describe-stacks --stack-name eksctl-$CLUSTER_NAME-cluster --query "Stacks[0].Outputs[?OutputKey==\`VPC\`].OutputValue"`
	
	Die Ausgabe sollte wie folgt aussehen.
	
	`[ "vpc-<YOUR-VPC-ID>" ]`
	
	Kopieren Sie die VPC-ID und exportieren Sie sie als Umgebungsvariable.
	
	`export VPC_ID="vpc-<YOUR-VPC-ID>"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM für das Cluster-Servicekonto.	Verwenden Sie die `AWS_REGION` und `CLUSTER_NAME` aus der vorherigen Ausgabe, um einen IAM-Open-ID-Connect-Anbieter für den Cluster zu erstellen. `eksctl utils associate-iam-oidc-provider \ --region $AWS_REGION \ --cluster $CLUSTER_ NAME \ --approve`	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie die IAM-Richtlinie herunter und erstellen Sie sie.	Laden Sie die IAM-Richtlinie für den AWS Load Balancer Controller herunter, mit der er in Ihrem Namen Aufrufe an AWS-APIs tätigen kann.
	`curl -o iam-policy.json https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam_policy.json`
	Erstellen Sie die Richtlinie in Ihrem AWS-Konto mithilfe der AWS CLI.
	`aws iam create-policy \ --policy-name AWSLoadBalancerControllerIAMPolicy \ --policy-document file://iam-policy.json`
	Die Ausgabe sollte folgender maßen aussehen.
	`{ "Policy": { "PolicyName": "AWSLoadBalancerControllerIAMPolicy", "PolicyId": "<YOUR_POLICY_ID>",`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Arn": "arn:aws:
	iam::<YOUR-ACCOUNT
	-ID>:policy/AWSLoa
	dBalancerControlle
	rIAMPolicy",
	"Path": "/",
	"DefaultV
	ersionId": "v1",
	"Attachme
	ntCount": 0,
	"Permissi
	onsBoundaryUsageCo
	unt": 0,
	"IsAttachable":
	true,
	"CreateDate":
	"<YOUR-DATE>",
	"UpdateDate":
	"<YOUR-DATE>"
	}
	}</pre> Speichern Sie den Amazon-Ressourcennamen (ARN) der Richtlinie als `$POLICY_ARN` . <pre>export POLICY_AR
	N=”arn:aws:iam::<Y
	OUR-ACCOUNT-ID>:po
	licy/AWSLoadBalanc
	erControllerIAMPol
	icy”</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein IAM-Servicekonto.	Erstellen Sie ein IAM-Servicekonto mit dem Namen `aws-load-balancer-controller` im `kube-system` Namespace. Verwenden Sie die `CLUSTER_NAME`, und `AWS_REGION`, `POLICY_ARN` die Sie zuvor konfiguriert haben.
	`eksctl create iamserviceaccount \ --cluster=$CLUSTER_NAME \ --region=$AWS_REGION \ --attach-policy-arn=$POLICY_ARN \ --namespace=kube-system \ --name=aws-load-balancer-controller \ --override-existing-serviceaccounts \ --approve`
	Überprüfen Sie die Erstellung.
	`eksctl get iamserviceaccount \ --cluster $CLUSTER_NAME \ --name aws-load-balancer-controller \ --namespace kube-system \ --output yaml`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Die Ausgabe sollte wie folgt aussehen.
	
	`- metadata:`
	`    name: aws-load-balancer-controller`
	`    namespace: kube-system`
	`  status:`
	`    roleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-addon-iam serviceaccount-ku-Role1-<YOUR-ROLE-ID>`
	`  wellKnownPolicies:`
	`    autoScaler: false`
	`    awsLoadBalancerController: false`
	`    certManager: false`
	`    ebsCSIController: false`
	`    efsCSIController: false`
	`    externalDNS: false`
	`    imageBuilder: false`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie den AWS Load Balancer Controller.	Aktualisieren Sie das Helm-Repository.
	`helm repo update`
	Fügen Sie das Amazon-EKS-Chart-Repository zum Helm-Repo hinzu.
	`helm repo add eks https://aws.github.io/eks-charts`
	Wenden Sie die benutzerdefinierten Kubernetes-Ressourcendefinitionen (CRDs) an, die vom AWS Load Balancer Controller eks-chart im Hintergrund verwendet werden.
	`kubectl apply -k "github.com/aws/eks-charts/stable/aws-load-balancer-controller//crds?ref=master"`
	Die Ausgabe sollte wie folgt aussehen.
	`customresourcedefinition.apiextensions.k8s.io/ingressclassparams.elbv2.k8s.aws created`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`customresourcedefinition.apiextensions.k8s.io/targetgroupbindings.elbv2.k8s.aws created`
	
	Installieren Sie das Helm-Diagramm mit den zuvor festgelegten Umgebungsvariablen.
	
	`helm install aws-load-balancer-controller eks/aws-load-balancer-controller \`
	`--set clusterName=$CLUSTER_NAME \`
	`--set serviceAccount.create=false \`
	`--set region=$AWS_REGION \`
	`--set vpcId=$VPC_ID \`
	`--set serviceAccount.name=aws-load-balancer-controller \`
	`-n kube-system`
	
	Die Ausgabe sollte wie folgt aussehen.
	
	`NAME: aws-load-balancer-controller`
	`LAST DEPLOYED: <YOUR-DATE>`
	`NAMESPACE: kube-system`
	`STATUS: deployed`
	`REVISION: 1`
	`TEST SUITE: None`
	`NOTES:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AWS Load Balancer controller installed!`	

Erstellen Sie einen NGINX-Service.	Erstellen Sie einen Service, um die NGINX-Pods mithilfe der `-nginx-service.yaml` Datei verfügbar zu machen.
	`kubectl apply -f nginx-service.yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`service/nginx-service created`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Erstellen Sie die Kubernetes-Ingress-Ressource.	Erstellen Sie einen Service, um den Kubernetes-NGINX-Eingang mithilfe der `-nginx-ingress.yaml` Datei verfügbar zu machen.
	`kubectl apply -f nginx-ingress.yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`ingress.networking.k8s.io/nginx-ingress created`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie die Load Balancer-URL ab.	Verwenden Sie den folgenden Befehl, um die Ingress-I nformationen abzurufen.
	`kubectl get ingress nginx-ingress`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME CLASS HOSTS ADDRESS PORTS AGE nginx-ingress <none> * k8s-defau lt-nginxing-xxx.us -east-1.elb.amazon aws.com 80 80s`
	Kopieren Sie die ADDRESS (z. B. `k8s-default-nginxi ng-xxx.us-east-1.e lb.amazonaws.com`) aus der Ausgabe und fügen Sie sie in Ihren Browser ein, um auf die `index.html` Datei zuzugreifen.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Debuggen von laufenden Containern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Wählen Sie einen Pod aus.	Listen Sie alle Pods auf und kopieren Sie den Namen des gewünschten Pods.
	`kubectl get pods`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME READY STATUS RESTARTS AGE nginx-deployment-xxxx-aaa 1/1 Running 0 55m nginx-deployment-xxxx-bbb 1/1 Running 0 55m nginx-deployment-xxxx-ccc 1/1 Running 0 55m nginx-deployment-xxxx-ddd 1/1 Running 0 42m`
	Dieser Befehl listet die vorhandenen Pods und zusätzliche Informationen auf.
	Wenn Sie an einem bestimmte n Pod interessiert sind, geben
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Namen des Pods ein, an dem Sie für die `POD_NAME` Variable interessiert sind, oder legen Sie ihn als Umgebungsvariable fest. Andernfalls lassen Sie diesen Parameter weg, um alle Ressourcen nachzuschlagen. `export POD_NAME="nginx-deployment-<YOUR-POD-NAME>"`	
Greifen Sie auf die Protokolle zu.	Rufen Sie die Protokolle von dem Pod ab, den Sie debuggen möchten. `kubectl logs $POD_NAME`	App-Entwickler, AWS-Systemadministrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Weiterleiten des NGINX-Ports.	Verwenden Sie die Port-Weiterleitung, um den Port des Pods für den Zugriff auf den NGINX-Webserver einem Port auf Ihrem lokalen Computer zuzuordnen.
	`kubectl port-forward deployment/nginx-deployment 8080:80`
	Öffnen Sie in Ihrem Browser die folgende URL.
	`http://localhost:8080`
	Der `port-forward` Befehl bietet Zugriff auf die `index.html` Datei, ohne sie über einen Load Balancer öffentlich verfügbar zu machen. Dies ist nützlich, um beim Debuggen auf die laufende Anwendung zuzugreifen. Sie können die Portweiterleitung beenden, indem Sie den Tastaturbefehl Strg+C drücken.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Befehle innerhalb des Pods aus.	Verwenden Sie den folgenden Befehl, um sich die aktuelle `index.html` Datei anzusehen. `kubectl exec $POD_NAME -- cat /usr/share/nginx/html/index.html` Sie können den `exec` Befehl verwenden, um jeden Befehl direkt im Pod auszugeben. Dies ist nützlich für das Debuggen laufender Anwendungen.	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Kopieren Sie Dateien in einen Pod.	Entfernen Sie die `index.html` Standarddatei auf diesem Pod.
	`kubectl exec $POD_NAME -- rm /usr/share/nginx/html/index.html`
	Laden Sie die benutzerdefinierte lokale Datei `index.html` in den Pod hoch.
	`kubectl cp index.html $POD_NAME:/usr/share/nginx/html/`
	Sie können den `cp` Befehl verwenden, um Dateien direkt zu einem der Pods zu ändern oder hinzuzufügen.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Verwenden Sie Port-Weit erleitung, um die Änderung anzuzeigen.	Verwenden Sie die Port-Weit erleitung, um die Änderunge n zu überprüfen, die Sie an diesem Pod vorgenommen haben.
	`kubectl port-forward pod/$POD_NAME 8080:80`
	Öffnen Sie die folgende URL in Ihrem Browser.
	`http://localhost:8080`
	Die angewendeten Änderunge n an der `index.html` Datei sollten im Browser sichtbar sein.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Löschen von Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie den Load Balancer.	Löschen Sie den Eingang.
	`kubectl delete ingress/nginx-ingress`
	Die Ausgabe sollte wie folgt aussehen.
	`ingress.networking.k8s.io "nginx-ingress" deleted`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Löschen Sie den Service:
	`kubectl delete service/nginx-service`
	Die Ausgabe sollte wie folgt aussehen.
	`service "nginx-service" deleted`
	Löschen Sie den Load Balancer-Controller.
	`helm delete aws-load-balancer-controller -n kube-system`
	Die Ausgabe sollte wie folgt aussehen.
	`release "aws-load-balancer-controller" uninstalled`
	Löschen Sie das Servicekonto.
	`eksctl delete iamserviceaccount --cluster $CLUSTER_NAME --namespace kube-system --name aws-load-balancer-controller`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie die Bereitstellung.	Verwenden Sie den folgenden Befehl, um die Bereitstellungsressourcen zu löschen.
	`kubectl delete deploy/nginx-deployment`
	Die Ausgabe sollte wie folgt aussehen.
	`deployment.apps "nginx-deployment" deleted`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Löschen Sie den Cluster.	Löschen Sie den EKS-Cluster mit dem folgenden Befehl, wobei der Clustername `my-fargate` ist. `eksctl delete cluster --name $CLUSTER_NAME` Dieser Befehl löscht den gesamten Cluster, einschließlich aller zugehörigen Ressourcen.	App-Entwickler, AWS DevOps, AWS-Systemadministrator
Löschen Sie die IAM-Richtlinie.	Löschen Sie die zuvor erstellte Richtlinie mithilfe der AWS CLI. `aws iam delete-policy --policy-arn $POLICY_ARN`	App-Entwickler, AWS-Administrator, AWS DevOps

Fehlerbehebung

Problem	Lösung
Sie erhalten bei der Clustererstellung eine Fehlermeldung, die besagt, dass Ihre Ziel-Availability Zone nicht über genügend Kapazität verfügt, um den Cluster zu unterstützen. Sie sollten eine Meldung ähnlich der folgenden sehen. `Cannot create cluster 'my-fargate' because us-east-1e, the targeted availability zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1f`	Erstellen Sie den Cluster erneut mit den empfohlenen Availability Zones aus der Fehlermeldung. Geben Sie in der letzten Zeile Ihrer `clusterconfig-fargate.yaml` Datei eine Liste der Availability Zones an (z. B. `availabilityZones: ["us-east-1a", "us-east-1b", "us-east-1c"]`).

Zugehörige Ressourcen

- Amazon-EKS-Dokumentation
- Application Load Balancing auf Amazon EKS
- Bewährte Methoden für EKS
- AWS Load Balancer Controller – Dokumentation
- eksctl-Dokumentation
- Amazon-ECR-Public-Galerie-NGINX-Image
- Helm-Dokumentation
- Debuggen von laufenden Pods (Kubernetes-Dokumentation)
- Amazon-EKS-Workshop
- EKS-Cluster-Erstellungsfehler

Zusätzliche Informationen

clusterconfig-fargate.yaml

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-fargate
  region: us-east-1

fargateProfiles:
  - name: fp-default
    selectors:
      - namespace: default
      - namespace: kube-system
```

nginx-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: "nginx-deployment"
  namespace: "default"
spec:
  replicas: 3
  selector:
    matchLabels:
      app: "nginx"
  template:
    metadata:
      labels:
        app: "nginx"
    spec:
      containers:
      - name: nginx
        image: public.ecr.aws/nginx/nginx:latest
        ports:
        - containerPort: 80
```

nginx-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    alb.ingress.kubernetes.io/target-type: ip
  name: "nginx-service"
  namespace: "default"
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  type: NodePort
  selector:
    app: "nginx"
```

nginx-ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  namespace: "default"
  name:  "nginx-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/scheme: internet-facing
spec:
  rules:
    - http:
        paths:
        - path: /
          pathType: Prefix
          backend:
            service:
              name: "nginx-service"
              port:
                number: 80
```

index.html

```
<!DOCTYPE html>
<html>
```

```
<body>
    <h1>Welcome to your customized nginx!</h1>
    <p>You modified the file on this running pod</p>
</body>

</html>
```

Bereitstellen von Containern mithilfe von Elastic Beanstalk

Erstellt von Bol Bol Bol Bol (AWS) und Bol-Baptiste Guis (AWS)

Code-Repository: Cluster-Beispiel-App	Umgebung: Produktion	Technologien: Container und Microservices; Cloudnativ; Modernisierung
AWS-Services: AWS Elastic Beanstalk		

Übersicht

In der Amazon Web Services (AWS) Cloud unterstützt AWS Elastic Beanstalk Docker als verfügbare Plattform, sodass Container mit der erstellten Umgebung ausgeführt werden können. Dieses Muster zeigt, wie Container mit dem Elastic Beanstalk-Service bereitgestellt werden. Bei der Bereitstellung dieses Musters wird die Webserverumgebung verwendet, die auf der Docker-Plattform basiert.

Um Elastic Beanstalk für die Bereitstellung und Skalierung von Webanwendungen und Services zu verwenden, laden Sie Ihren Code hoch und die Bereitstellung wird automatisch durchgeführt. Kapazitätsbereitstellung, Load Balancing, automatische Skalierung und Überwachung des Anwendungsstatus sind ebenfalls enthalten. Wenn Sie Elastic Beanstalk verwenden, können Sie die volle Kontrolle über die AWS-Ressourcen übernehmen, die es in Ihrem Namen erstellt. Für die Nutzung von Elastic Beanstalk fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die AWS-Ressourcen, die zum Speichern und Ausführen Ihrer Anwendungen verwendet werden.

Dieses Muster enthält Anweisungen für die Bereitstellung mit der AWS Elastic Beanstalk Command Line Interface (EB CLI) und der AWS-Managementkonsole.

Anwendungsfälle

Zu den Anwendungsfällen für Elastic Beanstalk gehören die folgenden:

- Stellen Sie eine Prototyp-Umgebung bereit, um eine Frontend-Anwendung zu demonstrieren. (Dieses Muster verwendet ein Dockerfile als Beispiel.)
- Stellen Sie eine API bereit, um API-Anforderungen für eine bestimmte Domain zu verarbeiten.

- Stellen Sie eine Orchestrierungslösung mit Docker-Compose bereit (`docker-compose.yml` wird in diesem Muster nicht als praktisches Beispiel verwendet).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto
- AWS EB CLI lokal installiert
- Docker auf einem lokalen Computer installiert

Einschränkungen

- Es gibt ein Docker-Pull-Limit von 100 Pulls pro 6 Stunden pro IP-Adresse im kostenlosen Plan.

Architektur

Zieltechnologie-Stack

- Instances von Amazon Elastic Compute Cloud (Amazon EC2)
- Sicherheitsgruppe
- Application Load Balancer
- Auto Scaling-Gruppe

Zielarchitektur

Automatisierung und Skalierung

AWS Elastic Beanstalk kann basierend auf der Anzahl der gestellten Anforderungen automatisch skaliert werden. Zu den für eine Umgebung erstellten AWS-Ressourcen gehören ein Application Load Balancer , eine Auto Scaling-Gruppe und eine oder mehrere Amazon EC2-Instances.

Der Load Balancer befindet sich vor den Amazon EC2-Instances, die Teil der Auto Scaling-Gruppe sind. Amazon EC2 Auto Scaling startet automatisch weitere Amazon EC2-Instances, um die

Datenverarbeitung der Anwendung auch bei einer erhöhten Workload zu gewährleisten. Wenn die Last Ihrer Anwendung abnimmt, stoppt Amazon EC2 Auto Scaling Instances, hält jedoch mindestens eine Instance laufen.

Auto Scaling-Auslöser

Die Auto Scaling-Gruppe in Ihrer Elastic Beanstalk-Umgebung verwendet zwei Amazon- CloudWatch Alarme, um Skalierungsvorgänge zu initiieren. Mit den Standardauslösern wird die Skalierung durchgeführt, wenn der durchschnittliche ausgehende Netzwerkdatenverkehr von der jeweiligen Instance innerhalb von 5 Minuten 6 MB über- oder 2 MB unterschreitet. Um Amazon-EC2-Auto-Scaling effektiv nutzen zu können, müssen Sie Auslöser konfigurieren, die für Ihre Anwendung, Ihren Instance-Typ und die Serviceanforderungen geeignet sind. Sie können die Skalierung anhand unterschiedlicher Statistiken wie Latenz, Festplatten-I/O-Vorgänge, CPU-Auslastung und Anforderungsanzahl ausführen. Weitere Informationen finden Sie unter Auto Scaling-Auslöser.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS EB Command Line Interface (EB CLI) ist ein Befehlszeilen-Client, mit dem Sie Elastic Beanstalk-Umgebungen erstellen, konfigurieren und verwalten können.
- Elastic Load Balancing verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Andere -Services

- Docker verpackt Software in standardisierte Einheiten, die als Container bezeichnet werden und Bibliotheken, Systemtools, Code und Laufzeit enthalten.

Code

Der Code für dieses Muster ist im GitHub Cluster-Beispielanwendungs-Repository verfügbar.

Polen

Erstellen mit einer Dockerfile-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Remote-Repository.	• Um das Repository zu klonen, führen Sie den Befehl `git clone https://github.com/aws-samples/cluster-sample-app.git`.< /p> aus.	App-Entwickler, AWS-Administrator, AWS DevOps
Initialisieren Sie das Docker-Projekt von Elastic Beanstalk.	1. Erstellen Sie eine Datei mit dem Namen `aws.json` im Stammverzeichnis. 2. Fügen Sie in der `aws.json` Datei den folgenden Code hinzu. `{ "AWSEBDockerrunVersion":"1", "Image":{ "Name":"cluster-sample-app" }, "Ports":[ { "ContainerPort":80 , "HostPort":8080 } ] }`	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Führen Sie den Befehl `eb init -p docker` im Stammverzeichnis des Projekts aus.	
Testen Sie das Projekt lokal.	1. Führen Sie den Befehl `eb local run` im Stammverzeichnis des Projekts aus. 2. Testen Sie die Anwendung, indem Sie zu navigiere `nhttp://localhost` .	App-Entwickler, AWS-Administrator, AWS DevOps

Bereitstellen mit EB CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ausführen des Bereitstellungsbefehls	1. Führen Sie den Befehl `eb create docker-sample-cluster-app` im Stammverzeichnis des Projekts aus.	App-Entwickler, AWS-Administrator, AWS DevOps
Greifen Sie auf die bereitgestellte Version zu.	Nachdem der Bereitstellungsbefehl abgeschlossen ist, greifen Sie mit dem `eb open` Befehl auf das Projekt zu.	App-Entwickler, AWS-Administrator, AWS DevOps

Bereitstellen über die Konsole

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung mithilfe des Browsers bereit.	1. Öffnen Sie die -Konsole.	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Navigieren Sie zur Elastic Beanstalk-Konsole. 3. Wählen Sie Anwendung erstellen aus. 4. Geben Sie für den Anwendungsnamen Cluster-Sample-App ein. 5. Wählen Sie Docker als Plattform aus. 6. Wählen Sie Code hochladen aus. 7. Wählen Sie Ihre lokale ZIP-Datei (im Stammverz eichnis des geklonten Projekts) oder eine öffentlic he Amazon Simple Storage Service (Amazon S3)-URL aus.	
Greifen Sie auf die bereitges tellte Version zu.	Greifen Sie nach der Bereitste llung auf die bereitgestellte Anwendung zu und wählen Sie die angegebene URL aus.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Zugehörige Ressourcen

- Webserver-Umgebungen
- Installieren der EB CLI unter macOS
- Manuelles Installieren der EB CLI

Zusätzliche Informationen

Vorteile der Verwendung von Elastic Beanstalk

- Automatische Infrastrukturbereitstellung
- Automatische Verwaltung der zugrunde liegenden Plattform
- Automatisches Patchen und Updates zur Unterstützung der Anwendung
- Automatische Skalierung der Anwendung
- Möglichkeit, die Anzahl der Knoten anzupassen
- Möglichkeit, bei Bedarf auf die Infrastrukturkomponenten zuzugreifen
- Einfache Bereitstellung gegenüber anderen Container-Bereitstellungslösungen

Generieren Sie eine statische ausgehende IP-Adresse mithilfe einer Lambda-Funktion, Amazon VPC und einer serverlosen Architektur

Erstellt von Thomas Scott (AWS)

Umgebung: Produktion	Technologien: Container und Mikroservices; Softwaree ntwicklung und -tests	AWS-Dienste: AWS Lambda

Übersicht

Dieses Muster beschreibt, wie eine statische ausgehende IP-Adresse in der Amazon Web Services (AWS) -Cloud mithilfe einer serverlosen Architektur generiert wird. Ihr Unternehmen kann von diesem Ansatz profitieren, wenn es Dateien mithilfe des Secure File Transfer Protocol (SFTP) an eine separate Geschäftseinheit senden möchte. Das bedeutet, dass die Geschäftseinheit Zugriff auf eine IP-Adresse haben muss, über die Dateien ihre Firewall passieren können.

Der Ansatz des Musters hilft Ihnen bei der Erstellung einer AWS Lambda Lambda-Funktion, die eine Elastic IP-Adresse als ausgehende IP-Adresse verwendet. Wenn Sie die Schritte in diesem Muster befolgen, können Sie eine Lambda-Funktion und eine Virtual Private Cloud (VPC) erstellen, die ausgehenden Datenverkehr über ein Internet-Gateway mit einer statischen IP-Adresse weiterleitet. Um die statische IP-Adresse zu verwenden, fügen Sie die Lambda-Funktion der VPC und ihren Subnetzen hinzu.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Identity and Access Management (IAM) -Berechtigungen zum Erstellen und Bereitstellen einer Lambda-Funktion sowie zum Erstellen einer VPC und ihrer Subnetze. Weitere Informationen dazu finden Sie unter Ausführungsrolle und Benutzerberechtigungen in der AWS Lambda Lambda-Dokumentation.

- Wenn Sie den Ansatz dieses Musters mithilfe von Infrastructure as Code (IaC) implementieren möchten, benötigen Sie eine integrierte Entwicklungsumgebung (IDE) wie AWS Cloud9. Weitere Informationen dazu finden Sie unter Was ist AWS Cloud9? in der AWS Cloud9 Cloud9-Dokumentation.

Architektur

Das folgende Diagramm zeigt die serverlose Architektur für dieses Muster.

Das Diagramm zeigt den folgenden Workflow:

1. Ausgehender Verkehr geht `NAT gateway 1` rein. `Public subnet 1`
2. Ausgehender Verkehr geht `NAT gateway 2` rein. `Public subnet 2`
3. Die Lambda-Funktion kann in `Private subnet 1` oder `Private subnet 2` ausgeführt werden.
4. `Private subnet 1`und leitet `Private subnet 2` den Verkehr zu den NAT-Gateways in den öffentlichen Subnetzen weiter.
5. Die NAT-Gateways senden ausgehenden Datenverkehr von den öffentlichen Subnetzen an das Internet-Gateway.
6. Ausgehende Daten werden vom Internet-Gateway zum externen Server übertragen.

Technologie-Stack

- Lambda
- Amazon Virtual Private Cloud (Amazon VPC)

Automatisierung und Skalierung

Sie können Hochverfügbarkeit (HA) sicherstellen, indem Sie zwei öffentliche und zwei private Subnetze in unterschiedlichen Availability Zones verwenden. Selbst wenn eine Availability Zone nicht mehr verfügbar ist, funktioniert die Pattern-Lösung weiterhin.

Tools

- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) stellt einen logisch isolierten Bereich der AWS-Cloud bereit, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Epen

Erstellen einer neuen VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer neuen VPC.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon VPC-Konsole und erstellen Sie dann eine VPC mit dem Namen `Lambda VPC` IPv4 `10.0.0.0/25` CIDR-Bereich. Weitere Informationen zum Erstellen einer VPC finden Sie unter Erste Schritte mit Amazon VPC in der Amazon VPC-Dokumentation.	AWS-Administrator

Erstellen Sie zwei öffentliche Subnetze

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das erste öffentliche Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `public-one` ein. 3. Wählen Sie für VPC `Lambda VPC` aus. 4. Wählen Sie eine Availability Zone und zeichnen Sie sie auf. 5. Geben Sie für IPv4 CIDR-Block den Wert Subnetz erstellen ein `10.0.0.0/28` und wählen Sie dann Create subnet aus.	AWS-Administrator
Erstellen Sie das zweite öffentliche Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `public-two` ein. 3. Wählen Sie für VPC `Lambda VPC` aus. 4. Wählen Sie eine Availability Zone und zeichnen Sie sie auf. Wichtig: Sie können die Availability Zone, die das `public-one` Subnetz enthält, nicht verwenden. 5. Geben Sie für IPv4 CIDR-Block Subnetz erstellen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein **10.0.0.16/28** und wählen Sie dann Create subnet aus.	

Erstellen Sie zwei private Subnetze

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das erste private Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `private-one` ein. 3. Wählen Sie für VPC `Lambda VPC` aus. 4. Wählen Sie die Availability Zone aus, die das `public-one` Subnetz enthält, das Sie zuvor erstellt haben. 5. Geben Sie für IPv4 CIDR-Block Subnetz erstellen ein **10.0.0.32/28** und wählen Sie dann Create subnet aus.	AWS-Administrator
Erstellen Sie das zweite private Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `private-two` ein. 3. Wählen Sie für VPC `Lambda VPC` aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie dieselbe Availability Zone, die das `public-two` Subnetz enthält, das Sie zuvor erstellt haben. 5. Geben Sie für IPv4 CIDR-Block Subnetz erstellen ein **`10.0.0.64/28`** und wählen Sie dann Create subnet aus.	

Erstellen Sie zwei Elastic IP-Adressen für Ihre NAT-Gateways

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erste Elastic IP-Adresse.	1. Wählen Sie in der Amazon VPC-Konsole Elastic IPs und dann Allocate new address aus. 2. Wählen Sie Allocate und notieren Sie die Allocation ID für Ihre neu erstellte Elastic IP-Adresse. Hinweis: Diese Elastic IP-Adresse wird für Ihr erstes NAT-Gateway verwendet.	AWS-Administrator
Erstellen Sie die zweite Elastic IP-Adresse.	1. Wählen Sie in der Amazon VPC-Konsole Elastic IPs und dann Allocate new address aus. 2. Wählen Sie Allocate und notieren Sie die Allocation	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ID für diese zweite Elastic IP-Adresse. Hinweis: Diese Elastic IP-Adresse wird für Ihr zweites NAT-Gateway verwendet.	

Ein Internet-Gateway erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Internet-Gateways	1. Wählen Sie in der Amazon VPC-Konsole Internet Gateways und dann Create Internet Gateway aus. 2. Geben Sie `Lambda internet gateway` den Namen ein und wählen Sie dann Internet-Gateway erstellen. Stellen Sie sicher, dass Sie die Internet-Gateway-ID notieren.	AWS-Administrator
Verbinden Sie das Internet-Gateway mit der VPC.	Wählen Sie zuerst das Internet-Gateway aus, das Sie eben erstellt haben, und anschließend Actions, Attach to VPC (Aktionen, An VPC anfügen).	AWS-Administrator

Erstellen Sie zwei NAT-Gateways

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das erste NAT-Gateway.	1. Wählen Sie auf der Amazon VPC-Konsole NAT Gateways und dann Create NAT Gateway aus. 2. Geben Sie den `nat-one` Namen des NAT-Gateways ein. 3. Wählen Sie `public-one` als Subnetz, in dem das NAT-Gateway erstellt werden soll. 4. Wählen Sie als Konnektivitätstyp die Option Öffentlich aus. 5. Wählen Sie für Elastic IP Allocation ID die erste Elastic IP-Adresse aus, die Sie zuvor erstellt haben, und verknüpfen Sie sie mit dem NAT-Gateway. 6. Wählen Sie NAT-Gateway erstellen aus.	AWS-Administrator
Erstellen Sie das zweite NAT-Gateway.	1. Wählen Sie auf der Amazon VPC-Konsole NAT Gateways und dann Create NAT Gateway aus. 2. Geben Sie den `nat-two` Namen des NAT-Gateways ein.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie `public-two` als Subnetz, in dem das NAT-Gateway erstellt werden soll. 4. Wählen Sie als Konnektivitätstyp die Option Öffentlich aus. 5. Wählen Sie für Elastic IP Allocation ID die zweite Elastic IP-Adresse aus, die Sie zuvor erstellt haben, und verknüpfen Sie sie mit dem NAT-Gateway. 6. Wählen Sie NAT-Gateway erstellen aus.	

Erstellen Sie Routentabellen für Ihre öffentlichen und privaten Subnetze

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das öffentliche Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `public-one-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `public-one-subnet` Routentabelle aus, klicken Sie auf Routen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bearbeiten und wählen Sie dann Route hinzufügen. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann die Internet-Gateway-ID in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`public-one`** Subnetz mit dem **`10.0.0.0/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das Public-Two-Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `public-two-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `public-two-subnet` Routentabelle aus, klicken Sie auf Routen bearbeiten und wählen Sie dann Route hinzufügen. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann die Internet-Gateway-ID in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`public-two`** Subnetz mit dem **`10.0.0.16/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das private One-Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `private-one-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `private-one-subnet` Routentabelle aus, klicken Sie auf Routen bearbeiten und wählen Sie dann Route hinzufügen. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann das NAT-Gateway im `public-one` Subnetz in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`private-one`** Subnetz mit dem **`10.0.0.32/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das Private-Two-Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `private-two-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `private-two-subnet` Routentabelle aus, klicken Sie auf Routen bearbeiten und wählen Sie dann Route hinzufügen. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann das NAT-Gateway im `public-two` Subnetz in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`private-two`** Subnetz mit dem **`10.0.0.64/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	AWS-Administrator

Erstellen Sie die Lambda-Funktion, fügen Sie sie der VPC hinzu und testen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue Lambda-Funktion.	1. Öffnen Sie die AWS Lambda Lambda-Konsole und wählen Sie Create function. 2. Geben Sie unter Basisinfo rmationen `Lambda test` unter Funktionsname ein und wählen Sie dann unter Runtime die Sprache Ihrer Wahl aus. 3. Wählen Sie Funktion erstellen.	AWS-Administrator
Fügen Sie die Lambda-Fu nktion zu Ihrer VPC hinzu.	1. Wählen Sie in der AWS Lambda Lambda-Konsole Funktionen und dann die Funktion aus, die Sie zuvor erstellt haben. 2. Wählen Sie Konfiguration und dann VPC aus. 3. Wählen Sie Bearbeiten und anschließend beide privaten Subnetze aus `Lambda VPC`. 4. Wählen Sie zu Testzweck en die Standardsicherheit sgruppe und dann Speichern aus.	AWS-Administrator
Schreiben Sie Code, um einen externen Service aufzurufen.	1. Schreiben Sie in der Programmiersprache Ihrer Wahl Code, um einen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	externen Dienst aufzurufen, der Ihre IP-Adresse zurückgibt. 2. Stellen Sie sicher, dass die zurückgegebene IP-Adresse mit einer Ihrer Elastic IP-Adressen übereinstimmt.	

Zugehörige Ressourcen

- Konfigurieren einer Lambda-Funktion für den Zugriff auf Ressourcen in einer VPC

Installieren des SSM-Agenten auf Amazon-EKS-Worker-Knoten mithilfe von Kubernetes DaemonSet

Erstellt vonendra Siddappa (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices DevOps; Infrastruktur	AWS-Services: Amazon EKS; AWS Systems Manager

Übersicht

Hinweis: September 2021: Die neuesten für Amazon EKS optimierten AMIs installieren SSM Agent automatisch. Weitere Informationen finden Sie in den Versionshinweisen für die AMIs vom Juni 2021.

In Amazon Elastic Kubernetes Service (Amazon EKS) sind Worker-Knoten aufgrund von Sicherheitsrichtlinien nicht mit Secure Shell (SSH)-Schlüsselpaaren verbunden. Dieses Muster zeigt, wie Sie den Kubernetes- DaemonSet Ressourcentyp verwenden können, um AWS Systems Manager Agent (SSM Agent) auf allen Worker-Knoten zu installieren, anstatt ihn manuell zu installieren oder das Amazon Machine Image (AMI) für die Knoten zu ersetzen. DaemonSet verwendet einen Cron-Auftrag auf dem Worker-Knoten, um die Installation von SSM Agent zu planen. Sie können dieses Muster auch verwenden, um andere Pakete auf Worker-Knoten zu installieren.

Wenn Sie Probleme im Cluster beheben, können Sie durch die Installation von SSM Agent on demand eine SSH-Sitzung mit dem Worker-Knoten einrichten, Protokolle sammeln oder die Instance-Konfiguration ohne SSH-Schlüsselpaare untersuchen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandener Amazon-EKS-Cluster mit Amazon Elastic Compute Cloud (Amazon EC2)-Worker-Knoten.
- Container-Instances sollten über die erforderlichen Berechtigungen für die Kommunikation mit dem SSM-Service verfügen. Die von AWS Identity and Access Management (IAM) verwaltete Rolle AmazonSSMManagedInstanceCore stellt die erforderlichen Berechtigungen für SSM Agent

bereit, um auf EC2-Instances ausgeführt zu werden. Weitere Informationen finden Sie in der AWS Systems Manager-Dokumentation.

Einschränkungen

- Dieses Muster gilt nicht für AWS Fargate, da auf der Fargate-Plattform nicht unterstützt DaemonSets wird.
- Dieses Muster gilt nur für Linux-basierte Worker-Knoten.
- Die DaemonSet Pods werden im privilegierten Modus ausgeführt. Wenn der Amazon-EKS-Cluster über einen Webhook verfügt, der Pods im privilegierten Modus blockiert, wird der SSM-Agent nicht installiert.

Architektur

Das folgende Diagramm veranschaulicht die Architektur für dieses Muster.

Tools

Tools

- kubectl ist ein Befehlszeilendienstprogramm, das für die Interaktion mit einem Amazon-EKS-Cluster verwendet wird. Dieses Muster verwendet , `kubectl` um einen DaemonSet auf dem Amazon-EKS-Cluster bereitzustellen, der SSM Agent auf allen Worker-Knoten installiert.
- Amazon EKS macht es Ihnen leicht, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren, betreiben und warten zu müssen. Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Anwendungen in Containern.
- Mit AWS Systems Manager Session Manager können Sie Ihre EC2-Instances, On-Premises-Instances und virtuellen Maschinen (VMs) über eine interaktive browserbasierte One-Click-Shell oder über die AWS Command Line Interface (AWS CLI) verwalten.

Code

Verwenden Sie den folgenden Code, um eine DaemonSet Konfigurationsdatei zu erstellen, die den SSM Agent auf dem Amazon-EKS-Cluster installiert. Folgen Sie den Anweisungen im Abschnitt „Epics“.

```
cat << EOF > ssm_daemonset.yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    k8s-app: ssm-installer
  name: ssm-installer
  namespace: kube-system
spec:
  selector:
    matchLabels:
      k8s-app: ssm-installer
  template:
    metadata:
      labels:
        k8s-app: ssm-installer
    spec:
      containers:
      - name: sleeper
        image: busybox
        command: ['sh', '-c', 'echo I keep things running! && sleep 3600']
      initContainers:
      - image: amazonlinux
        imagePullPolicy: Always
        name: ssm
        command: ["/bin/bash"]
        args: ["-c","echo '* * * * * root yum install -y https://s3.amazonaws.com/
ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm & rm -rf /etc/
cron.d/ssmstart' > /etc/cron.d/ssmstart"]
        securityContext:
          allowPrivilegeEscalation: true
        volumeMounts:
        - mountPath: /etc/cron.d
          name: cronfile
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      volumes:
      - name: cronfile
        hostPath:
```

```
          path: /etc/cron.d
          type: Directory
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
EOF
```

Polen

Einrichten von kubectl

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie kubectl für den Zugriff auf den EKS-Cluster.	Wenn noch nicht installiert und für den Zugriff auf den Amazon-EKS-Cluster konfiguriert `kubectl` ist, finden Sie weitere Informationen unter Installieren von kubectl in der Amazon-EKS-Dokumentation.	DevOps

Bereitstellen der DaemonSet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die DaemonSet Konfigurationsdatei.	Verwenden Sie den Code im Abschnitt Code weiter oben in diesem Muster, um eine DaemonSet Konfigurationsdatei mit dem Namen zu erstellen `ssm_daemonset.yaml` , die auf dem Amazon-EKS-Cluster bereitgestellt wird. Der von gestartete Pod DaemonSet verfügt über	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen Hauptcontainer und einen -`init`Container. Der Hauptcontainer hat einen -`sleep`Befehl. Der `init` Container enthält einen -`command`Abschnitt, der eine Cron-Auftragsdatei zur Installation von SSM Agent im Pfad erstellt`/etc/cron .d/` . Der Cron-Auftrag wird nur einmal ausgeführt, und die erstellte Datei wird automatis ch gelöscht, nachdem der Auftrag abgeschlossen ist. Wenn der Init-Container abgeschlossen ist, wartet der Hauptcontainer 60 Minuten, bevor er beendet wird. Nach 60 Minuten wird ein neuer Pod gestartet. Dieser Pod installiert SSM Agent, falls er fehlt, oder aktualisiert SSM Agent auf die neueste Version. Bei Bedarf können Sie den `sleep` Befehl ändern, um den Pod einmal täglich neu zu starten oder häufiger auszuführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die DaemonSet auf dem Amazon-EKS-Cluster bereit.	Verwenden Sie den folgenden Befehl, um die DaemonSet Konfigurationsdatei bereitzustellen, die Sie im vorherigen Schritt auf dem Amazon-EKS-Cluster erstellt haben: `kubectl apply -f ssm_daemonset.yaml` Mit diesem Befehl wird eine erstellt DaemonSet , um die Pods auf Worker-Knoten auszuführen und SSM Agent zu installieren.	DevOps

Zugehörige Ressourcen

- Installieren von kubectl (Amazon-EKS-Dokumentation)
- Session Manager einrichten (AWS Systems Manager-Dokumentation)

Installieren Sie den SSM-Agenten und - CloudWatch Agenten auf Amazon-EKS-Worker-Knoten mit preBootstrapCommands

Erstellt von Akkamahadevi microSDmath (AWS)

Umgebung: Produktion	Technologien: Container und Microservices; Infrastruktur; Betrieb	AWS-Services: Amazon EKS; AWS Systems Manager; Amazon CloudWatch

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zum Installieren des AWS Systems Manager Agent (SSM Agent) und des Amazon CloudWatch Agent auf Amazon Elastic Kubernetes Service (Amazon EKS)-Worker-Knoten in der Amazon Web Services (AWS) Cloud während der Amazon EKS-Clustererstellung. Sie können den SSM-Agenten und den CloudWatch Agenten mithilfe der `-preBootstrapCommands`Eigenschaft aus dem `eksctl`Konfigurationsdateischema installieren (Dokumentation zu Komponenten). Anschließend können Sie den SSM Agent verwenden, um eine Verbindung zu Ihren Worker-Knoten herzustellen, ohne ein Amazon Elastic Compute Cloud (Amazon EC2)-Schlüsselpaar zu verwenden. Darüber hinaus können Sie den CloudWatch Agenten verwenden, um die Speicher- und Festplattenauslastung auf Ihren Amazon-EKS-Worker-Knoten zu überwachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Das eksctl-Befehlszeilen-Dienstprogramm , installiert und konfiguriert unter macOS , Linux oder Windows
- Das kubectl-Befehlszeilen-Dienstprogramm , installiert und konfiguriert unter macOS , Linux oder Windows

Einschränkungen

- Wir empfehlen, dass Sie vermeiden, der -`preBootstrapCommands`Eigenschaft länger laufende Skripts hinzuzufügen, da dies den Beitritt des Knotens zum Amazon-EKS-Cluster während der Skalierung verzögert. Wir empfehlen Ihnen, stattdessen ein benutzerdefiniertes Amazon Machine Image (AMI) zu erstellen.
- Dieses Muster gilt nur für Amazon EC2 Linux-Instances.

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Systems Manager Parameter Store

Zielarchitektur

Das folgende Diagramm zeigt ein Beispiel für einen Benutzer, der mithilfe des SSM Agent, der mit der installiert wurde, eine Verbindung zu Amazon-EKS-Worker-Knoten herstelltpreBootstrapCommands.

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer erstellt einen Amazon-EKS-Cluster unter Verwendung der `eksctl` Konfigurationsdatei mit der -`preBootstrapCommands`Eigenschaft, die den SSM-Agent und den CloudWatch Agenten installiert.
2. Alle neuen Instances, die aufgrund von Skalierungsaktivitäten später dem Cluster beitreten, werden mit dem vorinstallierten SSM-Agent und - CloudWatch Agent erstellt.
3. Der Benutzer stellt mithilfe des SSM-Agenten eine Verbindung zu Amazon EC2 her und überwacht dann die Speicher- und Festplattenauslastung mithilfe des CloudWatch Agenten.

Tools

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.

- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- AWS Systems Manager Parameter Store bietet eine sichere, hierarchische Speicherung für die Verwaltung von Konfigurationsdaten und Secrets.
- AWS Systems Manager Session Manager unterstützt Sie bei der Verwaltung Ihrer EC2-Instances, On-Premises-Instances und virtuellen Maschinen über eine interaktive browserbasierte One-Click-Shell oder über die AWS Command Line Interface (AWS CLI).
- eksctl ist ein Befehlszeilen-Dienstprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.
- kubectl ist ein Befehlszeilendienstprogramm für die Kommunikation mit dem Cluster-API-Server.

Polen

Erstellen eines Amazon-EKS-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die CloudWatch Agentenkonfigurationsdatei.	Speichern Sie die CloudWatch Agentenkonfigurationsdatei im AWS Systems Manager Parameter Store in der AWS-Region, in der Sie Ihren Amazon EKS-Cluster erstellen möchten. Erstellen Sie dazu einen Parameter in AWS Systems Manager Parameter Store und notieren Sie sich den Namen des Parameters (z. B. `AmazonCloudwatch-linux`). Weitere Informationen finden Sie im Beispielcode für CloudWatch die Agentenkonfigurationsdatei im Abschnitt	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zusätzliche Informationen dieses Musters.	
Erstellen Sie die eksctl-Konfigurationsdatei und den Cluster.	1. Erstellen Sie eine `-eksctl`Konfigurationsdatei, die die Installationsschritte CloudWatch für Agent und SSM Agent enthält. Weitere Informationen finden Sie im Beispielcode der eksctl-Konfigurationsdatei im Abschnitt Zusätzliche Informationen dieses Musters. 2. Erstellen Sie einen Cluster, indem Sie den `eksctl create cluster -f cluster.yaml` Befehl ausführen.	AWS DevOps

Stellen Sie sicher, dass der SSM-Agent und der CloudWatch Agent funktionieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den SSM-Agent.	Verwenden Sie SSH, um eine Verbindung zu Ihren Amazon EKS-Cluster-Knoten herzustellen, indem Sie eine der Methoden verwenden, die unter Starten einer Sitzung in der AWS Systems Manager-Dokumentation behandelt werden.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den CloudWatch Agenten.	Verwenden Sie die CloudWatch -Konsole, um den CloudWatch Agenten zu validieren: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Erweitern Sie im Navigationsbereich Metriken und wählen Sie dann Alle Metriken aus. 3. Geben Sie in das Suchfeld auf der Registerkarte Durchsuchen ein und wählen Sie dann CWAgent-Metriken aus, um die Speicher- und Datenträgermetriken anzuzeigen.	AWS DevOps

Zugehörige Ressourcen

- Installieren und Ausführen des CloudWatch Agenten auf Ihren Servern (Amazon- CloudWatch Dokumentation)
- Erstellen eines Systems Manager-Parameters (Konsole) (AWS Systems Manager-Dokumentation)
- Erstellen der CloudWatch Agentenkonfigurationsdatei (Amazon- CloudWatch Dokumentation)
- Starten einer Sitzung (AWS CLI) (AWS Systems Manager-Dokumentation)
- Starten einer Sitzung (Amazon EC2-Konsole) (AWS Systems Manager-Dokumentation)

Zusätzliche Informationen

Beispiel für eine CloudWatch Agentenkonfigurationsdatei

Im folgenden Beispiel ist der CloudWatch Agent für die Überwachung der Festplatten- und Speicherauslastung auf Amazon Linux-Instances konfiguriert:

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "disk": {
                "measurement": [
                    "used_percent"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

Beispiel für eine eksctl-Konfigurationsdatei

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: test
  region: us-east-2
  version: "1.24"
```

```
managedNodeGroups:
  - name: test
    minSize: 2
    maxSize: 4
    desiredCapacity: 2
    volumeSize: 20
    instanceType: t3.medium
    preBootstrapCommands:
    - sudo yum install amazon-ssm-agent -y
    - sudo systemctl enable amazon-ssm-agent
    - sudo systemctl start amazon-ssm-agent
    - sudo yum install amazon-cloudwatch-agent -y
    - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-
config -m ec2 -s -c ssm:AmazonCloudwatch-linux
    iam:
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Zusätzliche Codedetails

- In der letzten Zeile der `preBootstrapCommands` Eigenschaft `AmazonCloudwatch-linux` ist der Name des Parameters, der im AWS System Manager Parameter Store erstellt wurde. Sie müssen `AmazonCloudwatch-linux` in Parameter Store in derselben AWS-Region einschließen, in der Sie den Amazon EKS-Cluster erstellt haben. Sie können auch einen Dateipfad angeben, aber wir empfehlen die Verwendung von Systems Manager für eine einfachere Automatisierung und Wiederverwendbarkeit.
- Wenn Sie `preBootstrapCommands` in der `eksctl` Konfigurationsdatei verwenden, sehen Sie zwei Startvorlagen in der AWS-Managementkonsole. Die erste Startvorlage enthält die in angegebenen Befehle`preBootstrapCommands`. Die zweite Vorlage enthält die Befehle, die in `preBootstrapCommands` und den standardmäßigen Amazon-EKS-Benutzerdaten angegeben sind. Diese Daten sind erforderlich, damit die Knoten dem Cluster beitreten können. Die Auto Scaling-Gruppe der Knotengruppe verwendet diese Benutzerdaten, um neue Instances zu erstellen.
- Wenn Sie das `iam` Attribut in der `eksctl` Konfigurationsdatei verwenden, müssen Sie die standardmäßigen Amazon EKS-Richtlinien mit allen zusätzlichen Richtlinien auflisten, die in Ihren angehängten AWS Identity and Access Management (IAM)-

Richtlinien erforderlich sind. Im Codeausschnitt aus dem Schritt Erstellen der eksctl-Konfigurationsdatei und des Clusters `AmazonSSMMangedInstanceCore` werden `CloudWatchAgentServerPolicy` zusätzliche Richtlinien hinzugefügt, um sicherzustellen, dass der CloudWatch Agent und der SSM-Agent wie erwartet funktionieren. Die Richtlinien `AmazonEKSWorkerNodePolicy`, und `AmazonEC2ContainerRegistryReadOnly` sind obligatorische Richtlinien`AmazonEKS_CNI_Policy`, die erforderlich sind, damit der Amazon-EKS-Cluster ordnungsgemäß funktioniert.

Von AWS App2Container generierte Docker-Images optimieren

Erstellt von Varun Sharma (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices; Modernisierung; DevOps	AWS-Services: Amazon ECS

Übersicht

AWS App2Container ist ein Befehlszeilen-Tool, mit dem vorhandene Anwendungen, die On-Premises oder auf virtuellen Maschinen ausgeführt werden, in Container umgewandelt werden können, ohne dass Codeänderungen erforderlich sind.

Basierend auf dem Anwendungstyp verfolgt App2Container einen konservativen Ansatz, um Abhängigkeiten zu identifizieren. Im Prozessmodus sind alle Nicht-Systemdateien auf dem Anwendungsserver im Container-Image enthalten. In solchen Fällen kann ein ziemlich großes Image generiert werden.

Dieses Muster bietet einen Ansatz zur Optimierung der von App2Container generierten Container-Images. Sie gilt für alle Java-Anwendungen, die von App2Container im Prozessmodus erkannt werden. Der im Muster definierte Workflow ist für die Ausführung auf dem Anwendungsserver konzipiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Java-Anwendung, die auf einem Anwendungsserver auf einem Linux-Server ausgeführt wird
- App2Container installiert und eingerichtet, wobei alle Voraussetzungen erfüllt sind, auf dem Linux-Server

Architektur

Quelltechnologie-Stack

- Eine Java-Anwendung, die auf einem Linux-Server ausgeführt wird

Zieltechnologie-Stack

- Ein von App2Container generiertes Docker-Image

Ablauf der Zielarchitektur

1. Ermitteln Sie die Anwendungen, die auf dem Anwendungsserver ausgeführt werden, und analysieren Sie die Anwendungen.
2. Containerisieren Sie die Anwendungen.
3. Bewerten Sie die Größe des Docker-Images. Wenn das Image zu groß ist, fahren Sie mit Schritt 4 fort.
4. Verwenden Sie das Shell-Skript (angefügt), um große Dateien zu identifizieren.
5. Aktualisieren Sie die `appSpecificFiles` Listen `appExcludedFiles` und in der `analysis.json` Datei .

Tools

Tools

- AWS App2Container – AWS App2Container (A2C) ist ein Befehlszeilen-Tool, mit dem Sie Anwendungen, die in Ihrem On-Premises-Rechenzentrum oder auf virtuellen Maschinen ausgeführt werden, in Containern ausführen können, die von Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) verwaltet werden.

Code

Das `optimizeImage.sh` Shell-Skript und eine `analysis.json` Beispieldatei sind angehängt.

Die `optimizeImage.sh` Datei ist ein Hilfsprogrammskript zur Überprüfung des Inhalts der von App2Container generierten Datei, `ContainerFiles.tar`. Die Überprüfung identifiziert Dateien oder Unterverzeichnisse, die groß sind und ausgeschlossen werden können. Das Skript ist ein Wrapper für den folgenden tar-Befehl.

```
tar -Ptvf <path>|tr -s ' '|cut -d ' ' -f3,6| awk '$2 ~/<filetype>$/'| awk '$2 ~/
^<toplevel>/'| cut -f1-<depth> -d'/'|awk '{ if ($1>= <size>) arr[$2]+=$1 } END { for
 (key in arr) { if(<verbose>) printf("%-50s\t%-50s\n", key, arr[key]) else printf("%s,
\n", key) } } '|sort -k2 -nr
```

Im tar-Befehl verwendet das Skript die folgenden Werte:

`path`	Der Pfad zu `ContainerFiles.tar`
`filetype`	Der abzugleichende Dateityp
`toplevel`	Das abzugleichende Verzeichnis der obersten Ebene
`depth`	Die Tiefe des absoluten Pfads
`size`	Die Größe für jede Datei

Das -Skript führt folgende Aktionen aus:

1. Es verwendet `tar -Ptvf`, um die Dateien aufzulisten, ohne sie zu extrahieren.
2. Es filtert die Dateien nach Dateityp, beginnend mit dem Verzeichnis der obersten Ebene.
3. Basierend auf der Tiefe wird der absolute Pfad als Index generiert.
4. Basierend auf dem Index und den Speichern stellt er die Gesamtgröße des Unterverzeichnisses bereit.
5. Es gibt die Größe des Unterverzeichnisses aus.

Sie können die Werte auch manuell im tar-Befehl ersetzen.

Polen

Anwendungen erkennen, analysieren und containerisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entdecken Sie die On-Premises-Java-Anwendungen.	Führen Sie den folgenden Befehl aus, um alle	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anwendungen zu ermitteln , die auf dem Anwendung sserver ausgeführt werden. `sudo app2container inventory`	
Analysieren Sie die erkannten Anwendungen.	Um jede Anwendung mithilfe der zu analysieren`application-id` , die in der Bestandsphase abgerufen wurde, führen Sie den folgenden Befehl aus. `sudo app2container analyze --application-id <java-app-id>`	AWS DevOps
Containerisieren Sie die analysierten Anwendungen.	Führen Sie den folgenden Befehl aus, um eine Anwendung zu containerisieren. `sudo app2container containerize --application-id <application-id>` Der Befehl generiert das Docker-Image zusammen mit einem tar-Paket am Workspace-Standort. Wenn das Docker-Image zu groß ist, fahren Sie mit dem nächsten Schritt fort.	AWS DevOps

Identifizieren Sie appExcludedFiles und appSpecificFiles aus der extrahierten tar-Datei von App2Container

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Größe der Artifacts-Tar-Datei.	Identifizieren Sie die `ContainerFiles.tar` Datei in `{workspace}/{java-app-id}/Artifacts`, wobei `workspace` der App2Container-Workspace und die Anwendungs-ID `java-app-id` ist. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Dies ist die Gesamtgröße der tar-Datei nach der Optimierung.	AWS DevOps

Listen Sie die Unterverzeichnisse im Verzeichnis / und ihre Größe auf.	Führen Sie den folgenden Befehl aus, um die Größe der Haupt-Unterverzeichnisse im Verzeichnis der / obersten Ebene zu ermitteln.
	`./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 1 -t / -s 1000000 -v`
	`/var`
	`554144711`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`/usr 2097300819`
	`/tmp 18579660`
	`/root 43645397`
	`/opt 222320534`
	`/home 65212518`
	`/etc 11357677`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie große Unterverzeichnisse im Verzeichnis /.	Identifizieren Sie für jedes wichtige Unterverzeichnis, das im vorherigen Befehl aufgeführt ist, die Größe seiner Unterverzeichnisse. Verwenden Sie `-d`, um die Tiefe zu erhöhen, und `-t`, um das Verzeichnis der obersten Ebene anzugeben. Verwenden Sie beispielsweise `/var` als Verzeichnis der obersten Ebene. Identifizieren `/var`Sie unter alle großen Unterverzeichnisse und ihre Größe. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 2 -t /var -s 1000000 -v` Wiederholen Sie diesen Vorgang für jedes im vorherigen Schritt aufgeführte Unterverzeichnis (z. B. `/usr`, `/tmp/opt`, und `/home`).	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie den großen Ordner in jedem Unterverz eichnis unter dem Verzeichn is /.	Identifizieren Sie für jedes Unterverzeichnis, das im vorherigen Schritt aufgeführ t ist, alle Ordner, die zum Ausführen der Anwendung erforderlich sind. Wenn Sie beispielsweise die Unterverzeichnisse aus dem vorherigen Schritt verwenden, listen Sie alle Unterverzeichnisse im `/var` Verzeichnis und ihre Größe auf. Identifizieren Sie alle Unterverzeichnisse, die von der Anwendung benötigt werden. `/var/tmp 237285851 /var/lib 24489984 /var/cache 237285851` Um Unterverzeichnisse auszuschließen, die von der Anwendung nicht benötigt werden, fügen Sie diese Unterverz eichnisse in der `-analysis.json` Datei zum `appExcludedFiles` Abschnitt unter hinzu`container Parameters` .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Eine `analysis.json` Beispieldatei ist angehängt.	
Identifizieren Sie die benötigten Dateien aus der Liste appExcludes.	Identifizieren Sie für jedes Unterverzeichnis, das der Liste appExcludes hinzugefügt wird, alle Dateien in diesem Unterverzeichnis, die von der Anwendung benötigt werden. Fügen Sie in der Datei analysis.json die spezifischen Dateien oder Unterverzeichnisse im `appSpecificFiles` Abschnitt unter hinzu`containerParameters`. Wenn das `/usr/lib` Verzeichnis beispielsweise der Ausschlussliste hinzugefügt wird, aber von der Anwendung benötigt `/usr/lib/jvm` wird, fügen Sie `/usr/lib/jvm` zum `appSpecificFiles` Abschnitt hinzu.	AWS DevOps

Extrahieren und containerisieren Sie die Anwendung erneut

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Containerisieren Sie die analysierte Anwendung.	Führen Sie den folgenden Befehl aus, um die Anwendung zu containerisieren.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sudo app2container containerize --application-id <application-id>` Der Befehl generiert das Docker-Image zusammen mit einem tar-Paket am Workspace-Standort.	
Identifizieren Sie die Größe der Artifacts-Tar-Datei.	Identifizieren Sie die `ContainerFiles.tar` Datei in `{workspace}/{java-app-id}/Artifacts`, wobei `workspace` der App2Container-Workspace und `java-app-id` die Anwendungs-ID ist. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Dies ist die Gesamtgröße der tar-Datei nach der Optimierung.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Docker-Image aus.	Um zu überprüfen, ob das Image fehlerfrei gestartet wird, führen Sie das Docker-Image lokal mit den folgenden Befehlen aus. Um die `imageId` des Containers zu identifizieren, verwenden Sie `docker images |grep java-app-id .` Um den Container auszuführen, verwenden Sie `docker run -d <image id>`.	AWS DevOps

Zugehörige Ressourcen

- Was ist App2Container?
- AWS App2Container – Ein neues Containerisierungstool für Java- und .NET-Anwendungen (Blogbeitrag)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Platzieren Sie Kubernetes-Pods auf Amazon EKS mithilfe von Knotenaffinität, Taints und Toleranzen

Erstellt von Hitesh Parikh (AWS) und Raghu Bhamidimarri (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices	Workload: Open-Source
AWS-Services: Amazon EKS		

Übersicht

Dieses Muster zeigt die Verwendung von Kubernetes-Knotenaffinität, Knoten-Taints und Pod-Tolerationen, um Anwendungs-Pods auf bestimmten Worker-Knoten in einem Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster in der Amazon Web Services (AWS) Cloud absichtlich zu planen.

Ein Taint ist eine Knoteneigenschaft, mit der Knoten eine Reihe von Pods ablehnen können. Eine Toleranz ist eine Pod-Eigenschaft, mit der der Kubernetes-Scheduler Pods auf Knoten planen kann, die übereinstimmende Taints haben.

Toleranzen allein können jedoch nicht verhindern, dass ein Scheduler einen Pod auf einem Worker-Knoten platziert, der keine Taints hat. Beispielsweise kann ein rechenintensiver Pod mit einer Toleranz unbeabsichtigt auf einem universellen, nicht verunreinigten Knoten geplant werden. In diesem Szenario weist die Knotenaffinitätseigenschaft eines Pods den Scheduler an, den Pod auf einem Knoten zu platzieren, der die in der Knotenaffinität angegebenen Knotenauswahlkriterien erfüllt.

Taints, Toleranzen und Knotenaffinität weisen den Scheduler zusammen an, Pods konsistent auf den Knoten mit übereinstimmenden Taints und den Knotenbezeichnungen zu planen, die den auf dem Pod angegebenen Kriterien für die Knotenaffinität entsprechen.

Dieses Muster enthält ein Beispiel für eine Kubernetes-Bereitstellungsmanifestdatei und die Schritte zum Erstellen eines EKS-Clusters, Bereitstellen einer Anwendung und Validieren der Pod-Platzierung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto mit Anmeldeinformationen, die zum Erstellen von Ressourcen in Ihrem AWS-Konto konfiguriert sind
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- eksctl
- kubectl
- Docker installiert (für das verwendete Betriebssystem) und die Engine gestartet (Informationen zu den Docker-Lizenzanforderungen finden Sie auf der Docker-Website)
- Java Version 11 oder höher
- Ein Java-Microservice, der in Ihrer bevorzugten integrierten Entwicklungsumgebung (IDE) ausgeführt wird, z. B. AWS Cloud9, IntelliJ IDEA Community Edition oder Eclipse (wenn Sie keinen Java-Microservice haben, finden Sie im Abschnitt Bereitstellen eines Java-Microservice auf Amazon-EKS-Mustern und Microservices mit Spring Hilfe bei der Erstellung des Microservice).

Einschränkungen

- Dieses Muster stellt den Java-Code nicht bereit und setzt voraus, dass Sie bereits mit Java vertraut sind. Informationen zum Erstellen eines einfachen Java-Microservice finden Sie unter Bereitstellen eines Java-Beispiel-Microservice auf Amazon EKS.
- Die Schritte in diesem Artikel erstellen AWS-Ressourcen, für die Kosten anfallen können. Stellen Sie sicher, dass Sie die AWS-Ressourcen bereinigen, nachdem Sie die Schritte zur Implementierung und Validierung des Musters abgeschlossen haben.

Architektur

Zieltechnologie-Stack

- Amazon EKS
- Java
- Docker
- Amazon Elastic Container Registry (Amazon ECR)

Zielarchitektur

Das Lösungsarchitekturdiagramm zeigt Amazon EKS mit zwei Pods (Bereitstellung 1 und Bereitstellung 2) und zwei Knotengruppen (ng1 und ng2) mit jeweils zwei Knoten. Die Pods und Knoten haben die folgenden Eigenschaften.

	Bereitstellung 1 Pod	Pod für Bereitstellung 2	Knotengruppe 1 (ng1)	Knotengruppe 2 (ng2)
Toleranz	Schlüssel: classified_workload, Wert: true, Effekt: NoSchedule Schlüssel: machine_Learning_workload, Wert: true, Effekt: NoSchedule	None		
Knotenaffinität	Schlüssel: alpha.eksctl.io/nodegroup-name = ng1;	None	nodeGroups.name = ng1	
Taint			Schlüssel: classified_workload, Wert: true, Effekt: NoSchedule Schlüssel: machine_Learning_	None

	workload, Wert: true, Effekt: NoSchedule

1. Für den Deployment 1 Pod sind Toleranzen und Knotenaffinität definiert, die den Kubernetes-Scheduler anweist, die Bereitstellungs-Pods auf den Knoten der Knotengruppe 1 (ng1) zu platzieren.
2. Knotengruppe 2 (ng2) hat keine Knotenbezeichnung, die dem Knotenaffinitätsknoten-Selektorausdruck für Bereitstellung 1 entspricht, sodass die Pods nicht auf ng2-Knoten geplant werden.
3. Für den Bereitstellung-2-Pod sind keine Toleranzen oder Knotenaffinitäten im Bereitstellungsmanifest definiert. Der Scheduler lehnt die Planung von Bereitstellung-2-Pods auf Knotengruppe 1 aufgrund der Taints auf den Knoten ab.
4. Die Bereitstellung-2-Pods werden stattdessen in Knotengruppe 2 platziert, da die Knoten keine Taints haben.

Dieses Muster zeigt, dass Sie durch die Verwendung von Taints und Toleranzen in Kombination mit der Knotenaffinität die Platzierung von Pods auf bestimmten Gruppen von Worker-Knoten steuern können.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- eksctl entspricht AWS kubectl und hilft bei der Erstellung von EKS.

Andere Tools

- Docker ist eine Reihe von Platform as a Service (PaaS)-Produkten, die Virtualisierung auf Betriebssystemebene verwenden, um Software in Containern bereitzustellen.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.

Polen

Erstellen des EKS-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Datei cluster.yaml.	Erstellen Sie eine Datei mit dem Namen `cluster.yaml` mit dem folgenden Code.
	
	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
	
	`metadata:`
	`  name: eks-taint-demo`
	`  region: us-west-1`
	
	`# Unmanaged nodegroups with and without taints.`
	`nodeGroups:`
	`  - name: ng1`
	`  instanceType: m5.xlarge`
	`  minSize: 2`
	`  maxSize: 3`
	`  taints:`
	`  - key: classified_workload`
	`  value: "true"`
	`  effect: NoSchedule`
	`  - key: machine_learning_workload`
	`  value: "true"`
		App-Besitzer, AWS DevOps, Cloud-Administrator, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>effect:
	NoSchedule
	
	- name: ng2
	instanceType:
	m5.xlarge
	minSize: 2
	maxSize: 3</pre>	

Erstellen Sie den Cluster mit eksctl.	Führen Sie die `cluster.yaml` Datei aus, um den EKS-Cluster zu erstellen. Das Erstellen des Clusters kann einige Minuten dauern. <pre>eksctl create cluster -f cluster.yaml</pre>	AWS DevOps, AWS-Systemadministrator, App-Entwickler

Erstellen eines Images und Hochladen in Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein privates Amazon-ECR-Repository.	Informationen zum Erstellen eines Amazon-ECR-Repositorys finden Sie unter Erstellen eines privaten Repositorys. Notieren Sie sich den URI des Repo.	AWS DevOps, DevOps Techniker, App-Entwickler
Erstellen Sie das Dockerfile.	Wenn Sie über ein vorhandenes Docker-Container-Image verfügen, das Sie zum Testen des Musters verwenden möchten, können Sie diesen Schritt überspringen.	AWS DevOps, DevOps Engineering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Verwenden Sie den folgenden Ausschnitt als Referenz, um ein Dockerfile zu erstellen. Wenn Sie auf Fehler stoßen, lesen Sie den Abschnitt Fehlerbehebung.
	
	`FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`
	
	`RUN apk add maven`
	`WORKDIR /code`
	
	`# Prepare by downloading dependencies`
	`ADD pom.xml /code/pom.xml`
	`RUN ["mvn", "dependency:resolve"]`
	`RUN ["mvn", "verify"]`
	
	`# Adding source, compile and package into a fat jar`
	`ADD src /code/src`
	`RUN ["mvn", "package"]`
	
	`EXPOSE 4567`
	`CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quelldate ien pom.xml und sowie das Docker-Image und übertragen Sie es.	Informationen zum Erstellen der -`pom.xml`Datei und der Java-Quelldatei finden Sie unter Bereitstellen eines Java-Microservice-Beispielmusters auf Amazon EKS. Verwenden Sie die Anweisung en in diesem Muster, um das Docker-Image zu erstellen und zu pushen.	AWS DevOps, DevOps Techniker, App-Entwickler

Bereitstellen in Amazon EKS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datei deployment.yaml.	Um die `deployment.yaml` Datei zu erstellen, verwenden Sie den Code im Abschnitt Zusätzliche Informationen. Im Code ist der Schlüssel für die Knotenaffinität jede Bezeichnung, die Sie beim Erstellen von Knotengru ppen erstellen. Dieses Muster verwendet die von eksctl erstellte Standardb ezeichnung. Informationen zum Anpassen von Labels finden Sie unter Zuweisen von Pods zu Knoten in der Kubernetes-Dokumentation.	AWS DevOps, DevOps Techniker, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Wert für den Knotenaff initätsschlüssel ist der Name der Knotengruppe, die von erstellt wurde`cluster.yaml` . Führen Sie den folgenden Befehl aus, um den Schlüssel und den Wert für den Taint abzurufen. `kubectl get nodes -o json | jq '.items[].spec.taints'` Das Image ist der URI des Amazon-ECR-Repositorys, das Sie in einem früheren Schritt erstellt haben.	
Stellen Sie die Datei bereit.	Führen Sie den folgenden Befehl aus, um in Amazon EKS bereitzustellen. `kubectl apply -f deployment.yaml`	App-Entwickler, DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellung.	1. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Pods READY sind.
	`kubectl get pods -o wide`
	Wenn das POD bereit ist, sollte die Ausgabe in etwa wie folgt aussehen, wobei als Wird ausgeführt `STATUS` angezeigt wird.
	`NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES`
	`<pod_name> 1/1 Running 0 12d 192.168.18.50 ip-192-168-20-110.us-west-1.compute.internal <none> <none>`
	Notieren Sie sich den Namen des Pods und den Namen des Knotens. Sie können den nächsten Schritt überspringen.
	2. (Optional) Führen Sie den folgenden Befehl aus, um zusätzliche Details zum
		App-Entwickler, DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Pod zu erhalten und die Toleranzen auf dem Pod zu überprüfen.
	
	`kubectl describe pod <pod_name>`
	
	Ein Beispiel für die Ausgabe finden Sie im Abschnitt Zusätzliche Informationen.
	3. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Pod-Platzierung auf dem Knoten korrekt ist.
	
	`kubectl describe node <node name> | grep -A 1 "Taints"`
	
	Vergewissern Sie sich, dass der Taint auf dem Knoten mit der Toleranz übereinst immt und die Bezeichnung auf dem Knoten mit der in definierten Knotenaffinität übereinstimmt`deploymen t.yaml` .
	
	Der Pod mit Toleranzen und Knotenaffinität sollte auf einem Knoten mit den übereinstimmenden Taints und den Knotenaffinitätsbe schriftungen platziert	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	werden. Mit dem vorherige n Befehl erhalten Sie die Taints auf dem Knoten. Im Folgenden finden Sie eine Beispielausgabe.
	
	`kubectl describe node ip-192-168-29-181. us-west-1.compute. internal | grep -A 1 "Taints" Taints: classifled_workloa d=true:NoSchedule`
	
	`machine_learning_w orkload=true:NoSch edule`
	
	Führen Sie außerdem den folgenden Befehl aus, um zu überprüfen, ob der Knoten, auf dem der Pod platziert ist, eine Bezeichnu ng hat, die der Knotenaff initätsknotenbezeichnung entspricht.
	
	`kubectl get node <node name> --show-labels`
	
	4. Um zu überprüfen, ob die Anwendung das macht, was sie tun soll, überprüfen Sie die Pod-Protokolle, indem Sie den folgenden Befehl ausführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`kubectl logs -f <name-of-the-pod>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine zweite Bereitstellungs-.yaml-Datei ohne Toleranz und Knotenaffinität.	Dieser zusätzliche Schritt dient zur Validierung, dass der resultierende Pod nicht auf einem Knoten mit Taints geplant ist, wenn in der Bereitstellungsmanifestdatei keine Knotenaffinität oder -toleranz angegeben ist. (Er sollte auf einem Knoten geplant werden, der keine Taints hat). Verwenden Sie den folgenden Code, um eine neue Bereitstellungsdatei namens zu erstellen `deploy_no_taint.yaml` .
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: microservice-deployment-non-tainted`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app.kubernetes.io/name: java-microservice-no-taint`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app.kubernetes.io/name: java-microservice-no-taint`
	`  spec:`
	`  containers:`
		App-Entwickler, AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- name: java-
	microservice-container
	-2
	image:
	<account_number>.d
	kr.ecr<region>.ama
	zonaws.com/<reposi
	tory_name>:latest
	ports:
	- container
	Port: 4567</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die zweite Bereitstellungs-.yaml-Datei bereit und validieren Sie die Pod-Platzierung	1. Führen Sie den folgenden Befehl aus.
	`kubectl apply -f deploy_no_taint.yaml`
	2. Nachdem die Bereitstellung erfolgreich war, führen Sie dieselben Befehle aus, die Sie zuvor ausgeführt haben, um die Pod-Platzierung in einer Knotengruppe ohne Taint zu überprüfen.
	`kubectl describe node <node_name> | grep "Taints"`
	Die Ausgabe sollte wie folgt aussehen.
	`Taints: <none>`
	Damit ist der Test abgeschlossen.
		App-Entwickler, AWS DevOps, DevOps Techniker

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Ressourcen.	Verwenden Sie den folgenden Befehl, um AWS-Gebühren für Ressourcen zu vermeiden, die noch ausgeführt werden.	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`eksctl delete cluster --name <Name of the cluster> --region <region-code>`	

Fehlerbehebung

Problem	Lösung
Einige dieser Befehle werden möglicherweise nicht ausgeführt, wenn Ihr System arm64-Architektur verwendet (insbesondere wenn Sie dies auf einem M1-Mac ausführen). In der folgenden Zeile kann ein Fehler auftreten. `FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`	Wenn beim Ausführen der Dockerfile-Datei Fehler auftreten, ersetzen Sie die `FROM` Zeile durch die folgende Zeile. `FROM bellsoft/liberica-openjdk-alpine-musl:17`

Zugehörige Ressourcen

- Bereitstellen eines Java-Beispiel-Microservice auf Amazon EKS
- Erstellen eines privaten Amazon-ECR-Repositorys
- Zuweisen von Pods zu Knoten (Kubernetes-Dokumentation)
- Taints und Toleranzen (Kubernetes-Dokumentation)
- Amazon EKS
- Amazon ECR
- AWS-CLI
- Docker
- IntelliJ IDEA CE
- Eclipse

Zusätzliche Informationen

deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: alpha.eksctl.io/nodegroup-name
                    operator: In
                    values:
                      - <node-group-name-from-cluster.yaml>
      tolerations: #only this pod has toleration and is viable to go to ng with taint
        - key: "<Taint key>" #classified_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
        - key: "<Taint key>" #machine_learning_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
      containers:
        - name: java-microservice-container
          image: <account_number>.dkr.ecr<region>.amazonaws.com/
<repository_name>:latest
          ports:
            - containerPort: 4567
```

Beispielausgabe für das Beschreiben eines Pods

```
Name:         microservice-deployment-in-tainted-nodes-5684cc495b-vpcfx
Namespace:    default
Priority:     0
Node:         ip-192-168-29-181.us-west-1.compute.internal/192.168.29.181
Start Time:   Wed, 14 Sep 2022 11:06:47 -0400
Labels:       app.kubernetes.io/name=java-microservice-taint
              pod-template-hash=5684cc495b
Annotations:  kubernetes.io/psp: eks.privileged
Status:       Running
IP:           192.168.13.44
IPs:
  IP:           192.168.13.44
Controlled By:  ReplicaSet/microservice-deployment-in-tainted-nodes-5684cc495b
Containers:
  java-microservice-container-1:
    Container ID:
 docker://5c158df8cc160de8f57f62f3ee16b12725a87510a809d90a1fb9e5d873c320a4
    Image:          934188034500.dkr.ecr.us-east-1.amazonaws.com/java-eks-apg
    Image ID:       docker-pullable://934188034500.dkr.ecr.us-east-1.amazonaws.com/
java-eks-apg@sha256:d223924aca8315aab20d54eddf3443929eba511b6433017474d01b63a4114835
    Port:           4567/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Wed, 14 Sep 2022 11:07:02 -0400
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-ddvvw (ro)
Conditions:
  Type              Status
  Initialized       True
  Ready             True
  ContainersReady   True
  PodScheduled      True
Volumes:
  kube-api-access-ddvvw:
    Type:                     Projected (a volume that contains injected data from
 multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
```

```
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 classifled_workload=true:NoSchedule
                             machine_learning_workload=true:NoSchedule
                             node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for
 300s
Events:                      <none>
```

Replizieren Sie gefilterte Amazon ECR-Container-Images über Konten oder Regionen hinweg

Erstellt von Abdal Garuba (AWS)

Umgebung: Produktion	Technologien: Container und Mikroservices; DevOps	AWS-Services: Amazon EC2 Container Registry; Amazon CloudWatch; AWS CodeBuild ; AWS Identity and Access Management; AWS CLI

Übersicht

Amazon Elastic Container Registry (Amazon ECR) kann alle Container-Images in einem Image-Repository über Amazon Web Services (AWS) -Regionen und AWS-Konten nativ replizieren, indem die Funktionen für die regionsübergreifende und kontoübergreifende Replikation verwendet werden. (Weitere Informationen finden Sie im AWS-Blogbeitrag Regionsübergreifende Replikation in Amazon ECR ist gelandet.) Es gibt jedoch keine Möglichkeit, die Bilder, die zwischen AWS-Regionen oder Konten kopiert werden, anhand von Kriterien zu filtern.

Dieses Muster beschreibt, wie Container-Images, die in Amazon ECR gespeichert sind, auf der Grundlage von Image-Tag-Mustern über AWS-Konten und Regionen hinweg repliziert werden. Das Muster verwendet Amazon CloudWatch Events, um auf Push-Ereignisse für Bilder zu warten, die ein vordefiniertes, benutzerdefiniertes Tag haben. Ein Push-Ereignis startet ein CodeBuild AWS-Projekt und übergibt die Bilddetails an dieses Projekt. Das CodeBuild Projekt kopiert die Bilder auf der Grundlage der bereitgestellten Details aus der Amazon ECR-Quellregistrierung in die Zielregistrierung.

Dieses Muster kopiert Bilder, die bestimmte Tags haben, kontenübergreifend. Sie können dieses Muster beispielsweise verwenden, um nur produktionsbereite, sichere Images auf das AWS-Produktionskonto zu kopieren. Im Entwicklungskonto können Sie, nachdem die Bilder gründlich getestet wurden, den sicheren Images ein vordefiniertes Tag hinzufügen und die markierten Bilder mithilfe der Schritte in diesem Muster in das Produktionskonto kopieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto für Amazon ECR-Quell- und Zielregister
- Administratorberechtigungen für die in diesem Muster verwendeten Tools
- Docker wurde zum Testen auf Ihrem lokalen Computer installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI) für die Authentifizierung bei Amazon ECR

Einschränkungen

- Dieses Muster überwacht die Push-Ereignisse der Quellregistrierung nur in einer AWS-Region. Sie können dieses Muster in anderen Regionen bereitstellen, um Registrierungen in diesen Regionen zu überwachen.
- In diesem Muster wartet eine Amazon CloudWatch Events-Regel auf ein einzelnes Bild-Tag-Muster. Wenn Sie nach mehreren Mustern suchen möchten, können Sie Ereignisse hinzufügen, um auf zusätzliche Bild-Tag-Muster zu warten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

Dieses Muster kann mit einem Infrastructure-as-Code-Skript (IaC) automatisiert und in großem Umfang eingesetzt werden. Um dieses Muster mithilfe von CloudFormation AWS-Vorlagen bereitzustellen, laden Sie den Anhang herunter und folgen Sie den Anweisungen im Abschnitt Zusätzliche Informationen.

Sie können mehrere Amazon CloudWatch Events-Ereignisse (mit unterschiedlichen benutzerdefinierten Ereignismustern) auf dasselbe CodeBuild AWS-Projekt verweisen, um mehrere Image-Tag-Muster zu replizieren. Sie müssen jedoch die sekundäre Validierung in der `buildspec.yaml` Datei (die im Anhang und im Abschnitt Tools enthalten ist) wie folgt aktualisieren, um mehrere Muster zu unterstützen.

```
...
```

```
if [[ ${IMAGE_TAG} != release-* ]]; then
...
```

Tools

Amazon-Dienste

- IAM — Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf AWS-Services und -Ressourcen sicher verwalten. In diesem Muster müssten Sie die kontoübergreifende IAM-Rolle erstellen, die AWS beim Push von Container-Images in die Zielregistrierung CodeBuild übernimmt.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Container-Registry, die es einfach macht, Ihre Container-Images und Artefakte überall zu speichern, zu verwalten, zu teilen und bereitzustellen. Image-Push-Aktionen an die Quellregistrierung senden Systemereignisdetails an den Event-Bus, der von Amazon CloudWatch Events abgeholt wird.
- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Service für kontinuierliche Integration, der Rechenleistung für Aufgaben wie das Kompilieren von Quellcode, das Ausführen von Tests und das Erstellen von Artefakten bereitstellt, die sofort einsatzbereit sind. Dieses Muster verwendet AWS CodeBuild , um den Kopiervorgang von der Amazon ECR-Quellregistrierung in die Zielregistrierung durchzuführen.
- CloudWatch Ereignisse — Amazon CloudWatch Events liefert einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben. Dieses Muster verwendet Regeln, um Amazon ECR-Push-Aktionen einem bestimmten Image-Tag-Muster zuzuordnen.

Tools

- Docker CLI — Docker ist ein Tool, das das Erstellen und Verwalten von Containern erleichtert. Container packen eine Anwendung und all ihre Abhängigkeiten in einer Einheit oder einem Paket, das problemlos auf jeder Plattform bereitgestellt werden kann, die die Container-Laufzeit unterstützt.

Code

Sie können dieses Muster auf zwei Arten implementieren:

- Automatisierte Einrichtung: Stellen Sie die beiden CloudFormation AWS-Vorlagen bereit, die im Anhang enthalten sind. Anweisungen finden Sie im Abschnitt Zusätzliche Informationen.
- Manuelle Einrichtung: Folge den Schritten im Abschnitt Epics.

Beispiel für buildspec.yaml

Wenn Sie die CloudFormation Vorlagen verwenden, die mit diesem Muster bereitgestellt werden, ist die `buildspec.yaml` Datei in den Ressourcen enthalten. CodeBuild

```
  version: 0.2
  env:
    shell: bash
  phases:
    install:
      commands:
        - export CURRENT_ACCOUNT=$(echo ${CODEBUILD_BUILD_ARN} | cut -d':' -f5)
        - export CURRENT_ECR_REGISTRY=${CURRENT_ACCOUNT}.dkr.ecr.
${AWS_REGION}.amazonaws.com
        - export DESTINATION_ECR_REGISTRY=${DESTINATION_ACCOUNT}.dkr.ecr.
${DESTINATION_REGION}.amazonaws.com
    pre_build:
      on-failure: ABORT
      commands:
        - echo "Validating Image Tag ${IMAGE_TAG}"
        - |
          if [[ ${IMAGE_TAG} != release-* ]]; then
            aws codebuild stop-build --id ${CODEBUILD_BUILD_ID}
            sleep 60
            exit 1
          fi
        - aws ecr get-login-password --region ${AWS_REGION} | docker login -u AWS --
password-stdin ${CURRENT_ECR_REGISTRY}
        - docker pull ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
    build:
      commands:
        - echo "Assume cross-account role"
        - CREDENTIALS=$(aws sts assume-role --role-arn ${CROSS_ACCOUNT_ROLE_ARN} --
role-session-name Rolesession)
        - export AWS_DEFAULT_REGION=${DESTINATON_REGION}
        - export AWS_ACCESS_KEY_ID=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.AccessKeyId')
```

```
      - export AWS_SECRET_ACCESS_KEY=$(echo ${CREDENTIALS} | jq -r
'.Credentials.SecretAccessKey')
      - export AWS_SESSION_TOKEN=$(echo ${CREDENTIALS} | jq -r
'.Credentials.SessionToken')
      - echo "Logging into cross-account registry"
      - aws ecr get-login-password --region ${DESTINATION_REGION} | docker login -u
AWS --password-stdin ${DESTINATION_ECR_REGISTRY}
      - echo "Check if Destination Repository exists, else create"
      - |
        aws ecr describe-repositories --repository-names ${REPO_NAME} --region
${DESTINATION_REGION} \
        || aws ecr create-repository --repository-name ${REPO_NAME} --region
${DESTINATION_REGION}
      - echo "retag image and push to destination"
      - docker tag ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
      - docker push ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
```

Epen

Erstellen Sie IAM-Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle „ CloudWatch Ereignisse“.	Erstellen Sie im AWS-Quell konto eine IAM-Rolle, die Amazon CloudWatch Events übernehmen soll. Die Rolle sollte über Berechtigungen zum Starten eines CodeBuild AWS-Projekts verfügen. Folgen Sie den Anweisungen in der IAM-Dokumentation, um die Rolle mithilfe der AWS-CLI zu erstellen. Beispiel für eine Vertrauen srichtlinie (`trustpoli cy.json`):	AWS-Administrator DevOps, AWS, AWS-Systemadminist rator, Cloud-Administrato r, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	  "Version": "2012-10-17",
	  "Statement": {
	  "Effect": "Allow",
	  "Principal": {"Service": "events.amazonaws.com"},
	  "Action": "sts:AssumeRole"
	  }
	}</pre>
	Beispiel für eine Berechtigungsrichtlinie (`permissionpolicy.json`):
	<pre>{
	  "Version": "2012-10-17",
	  "Statement": {
	  "Effect": "Allow",
	  "Action": "codebuild:StartBuild",
	  "Resource": "<CodeBuild Project ARN>"
	  }
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CodeBuild Rolle.	Erstellen Sie eine IAM-Rolle , die AWS übernehmen CodeBuild soll, indem Sie den Anweisungen in der IAM-Dokumentation folgen. Die Rolle sollte über die folgenden Berechtigungen verfügen: • Erlaubnis, die kontoüber greifende Zielrolle zu übernehmen • Berechtigung zum Erstellen von Protokollgruppen und Protokollströmen sowie zum Speichern von Protokoll ereignissen • Schreibgeschützte Berechtigungen für alle Amazon ECR-Repositorys, indem Sie der Rolle die verwaltete AmazonEC2-Richtlinie ContainerRegistry ReadOnly hinzufügen • Erlaubnis zum Beenden CodeBuild Beispiel für eine Vertrauen srichtlinie (`trustpoli cy.json`): `{ "Version": "2012-10-17", "Statement": [ {`	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> "Effect": "Allow",
	      "Principal": {
	        "Service":
	 "codebuild.amazona
	ws.com"
	      },
	      "Action":
	 "sts:AssumeRole"
	    }
	  ]
	}</pre>
	Beispiel für eine Berechtigungsrichtlinie (`permissionpolicy.json`):
	<pre>{
	    "Version":
	 "2012-10-17",
	    "Statement": [
	        {
	            "Action": [
	
	 "codebuild:StartBu
	ild",
	
	 "codebuild:StopBui
	ld",
	
	 "codebuild:Get*",
	
	 "codebuild:List*",
	
	 "codebuild:BatchGet*"
	            ],
	            "Resource":
	 "*",
	            "Effect":
	 "Allow"
	        },
	        {</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Action": [
	
	"logs:CreateLogGroup",
	
	"logs:CreateLogStream",
	
	"logs:PutLogEvents"
	],
	"Resource": "*",
	"Effect": "Allow"
	},
	{
	"Action": "sts:AssumeRole",
	"Resource": "<ARN of destination role>",
	"Effect": "Allow",
	"Sid": "AssumeCrossAccountArn"
	}
	]
	}</pre> Hängen Sie die verwaltete Richtlinie wie folgt `AmazonEC2ContainerRegistryReadOnly` an den CLI-Befehl an: <pre>~$ aws iam attach-role-policy \
	--policy-arn arn:aws:iam::aws:policy/Ama</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`zonEC2ContainerRegistryReadOnly \` `--role-name <name of CodeBuild Role>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine kontoüber greifende Rolle.	Erstellen Sie im AWS-Zielk onto eine IAM-Rolle für die CodeBuild AWS-Rolle, die das Quellkonto übernehmen soll. Die kontoübergreifende Rolle sollte es Container-Images ermöglichen, ein neues Repository zu erstellen und Container-Images auf Amazon ECR hochzuladen. Folgen Sie den Anweisung en in der IAM-Dokumentation, um die IAM-Rolle mithilfe der AWS-CLI zu erstellen. Verwenden Sie die folgende Vertrauensrichtlinie, um das CodeBuild AWS-Projekt aus dem vorherigen Schritt zuzulassen: `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": { "AWS": "<ARN of source codebuild role>" }, "Action": "sts:AssumeRole" } }`	AWS-Administrator DevOps, AWS, Cloud-Administrato r, Cloud-Architekt, DevOps Ingenieur, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwenden Sie die folgende Berechtigungsrichtlinie, damit das CodeBuild AWS-Projekt aus dem vorherigen Schritt Bilder in der Zielregistrierung speichern kann: `{ "Version": "2012-10-17", "Statement": [ { "Action": [ "ecr:GetDownloadUrlForLayer", "ecr:BatchCheckLayerAvailability", "ecr:PutImage", "ecr:InitiateLayerUpload", "ecr:UploadLayerPart", "ecr:CompleteLayerUpload", "ecr:GetRepositoryPolicy", "ecr:DescribeRepositories", "ecr:GetAuthorizationToken",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"ecr:CreateRepository"
	            ],
	            "Resource": "*",
	            "Effect": "Allow"
	        }
	    ]
	}</pre>	

Erstellen Sie das CodeBuild Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeBuild Projekt.	Erstellen Sie ein CodeBuild AWS-Projekt im Quellkonto, indem Sie den Anweisungen in der CodeBuild AWS-Dokumentation folgen. Das Projekt sollte sich in derselben Region wie die Quellregistrierung befinden. Konfigurieren Sie das Projekt wie folgt: • Art der Umgebung: `LINUX CONTAINER` • Rolle im Dienst: `CodeBuild Role` • Privilegierter Modus: `true` • Umgebungsbild: `aws/codebuild/standard:x.x` (verwenden	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie das neueste verfügbare Image)
	• Umgebungsvariablen:
	  • `CROSS_ACCOUNT_ROLE_ARN` : Der Amazon-Ressourcenname (ARN) der kontoübergreifenden Rolle
	  • `DESTINATION_REGION` : Der Name der kontoübergreifenden Region
	  • `DESTINATION_ACCOUNT` : Die Nummer des Zielkontos
	• Build-Spezifikationen: Verwenden Sie die `buildspec.yaml` Datei, die im Abschnitt Tools aufgeführt ist.	

Erstellen Sie das Ereignis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ereignisregel.	Da das Muster die Inhaltsfilterfunktion verwendet, müssen Sie das Ereignis mithilfe von Amazon erstellen EventBridge. Erstellen Sie das Ereignis und das Ziel, indem Sie den Anweisungen in der EventBridge Dokumentation	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgen, mit einigen Änderungen: • Wählen Sie für Muster definieren die Option Ereignismuster und anschließend Benutzerdefiniertes Muster aus. • Kopieren Sie den folgenden Beispielcode für ein benutzerdefiniertes Ereignismuster in das dafür vorgesehene Textfeld: `{ "source": ["aws.ecr"], "detail-type": ["ECR Image Action"], "detail": { "action-type": ["PUSH"], "result": ["SUCCESS"], "image-tag": [{ "prefix": "release-"}] } }` • Wählen Sie für Select targets das CodeBuild AWS-Projekt aus und fügen Sie den ARN für das CodeBuild AWS-Projekt ein, das Sie im vorherigen Epic erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Wählen Sie für Configure Input die Option Input Transformer aus.
	  • Fügen Sie in das Textfeld Eingabepfad Folgendes ein:
	  `{"IMAGE_TAG":"$.detail.image-tag","REPO_NAME":"$.detail.repository-name"}`
	  • Fügen Sie in das Textfeld Eingabevorlage Folgendes ein:
	  `{"environmentVariablesOverride": [ {"name": "IMAGE_TAG", "value":<IMAGE_TAG>},{"name":"REPO_NAME","value":<REPO_NAME>}]}`
	• Wählen Sie „Bestehende Rolle verwenden“ und anschließend den Namen der Rolle „ CloudWatch Ereignisse“, die Sie zuvor im Epos „IAM-Rollen erstellen“ erstellt haben.	

Validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizieren Sie sich mit Amazon ECR.	Authentifizieren Sie sich sowohl bei der Quell- als auch bei der Zielregistrierung, indem Sie die Schritte in der Amazon ECR-Dokumentation befolgen.	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur, Cloud-Architekt
Testen Sie die Image-Replikation.	Übertragen Sie in Ihrem Quellkonto ein Container-Image in ein neues oder vorhandenes Amazon ECR-Quell-Repository mit einem Image-Tag als Präfix. `release-` Um das Bild zu übertragen, folgen Sie den Schritten in der Amazon ECR-Dokumentation. Sie können den Fortschritt des CodeBuild Projekts in der CodeBuild Konsole überwachen. Melden Sie sich nach erfolgreichem Abschluss des CodeBuild Projekts beim AWS-Zielkonto an, öffnen Sie die Amazon ECR-Konsole und vergewissern Sie sich, dass das Bild in der Amazon ECR-Zielregistrierung vorhanden ist.	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Image-Aus schluss.	Übertragen Sie in Ihrem Quellkonto ein Container -Image in ein neues oder vorhandenes Amazon ECR-Quell-Repository mit einem Image-Tag, das nicht über das benutzerdefinierte Präfix verfügt. Vergewissern Sie sich, dass das CodeBuild Projekt nicht gestartet wurde und dass keine Container-Images in der Zielregistrierung erscheinen.	AWS-Administrator DevOps, AWS, AWS-Systemadminist rator, Cloud-Administrato r, Cloud-Architekt, DevOps Ingenieur

Zugehörige Ressourcen

- Erste Schritte mit CodeBuild
- Erste Schritte mit Amazon EventBridge
- Inhaltsbasierte Filterung in EventBridge Amazon-Ereignismustern
- Delegieren Sie den Zugriff über AWS-Konten hinweg mithilfe von IAM-Rollen
- Replikation privater Images

Zusätzliche Informationen

Gehen Sie folgendermaßen vor, um die Ressourcen für dieses Muster automatisch bereitzustellen:

1. Laden Sie den Anhang herunter und extrahieren Sie die beiden CloudFormation Vorlagen: `part-1-copy-tagged-images.yaml` und`part-2-destination-account-role.yaml`.
2. Melden Sie sich bei der CloudFormation AWS-Konsole an und führen Sie die Bereitstellung `part-1-copy-tagged-images.yaml` in demselben AWS-Konto und derselben Region wie die Amazon ECR-Quellregistrierungen durch. Aktualisieren Sie die Parameter nach Bedarf. Die Vorlage stellt die folgenden Ressourcen bereit:

- CloudWatch IAM-Rolle bei Amazon Events
- CodeBuild IAM-Rolle des AWS-Projekts
- CodeBuild AWS-Projekt
- CloudWatch AWS-Ereignisregel

3. Notieren Sie sich den Wert von `SourceRoleName` auf der Registerkarte Ausgaben. Sie benötigen diesen Wert im nächsten Schritt.
4. Stellen Sie die zweite CloudFormation Vorlage in dem AWS-Konto bereit, `part-2-destination-account-role.yaml` in das Sie die Amazon ECR-Container-Images kopieren möchten. Aktualisieren Sie die Parameter nach Bedarf. Geben Sie für den `SourceRoleName` Parameter den Wert aus Schritt 3 an. Diese Vorlage stellt die kontoübergreifende IAM-Rolle bereit.
5. Überprüfen Sie die Replikation und den Ausschluss von Images, wie im letzten Schritt des Abschnitts Epics beschrieben.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern

Erstellt von Josh Joy (AWS)

Umgebung: Produktion	Technologien: Container und Microservices; Datenbanken; DevOpsInfrastruktur; Sicherheit, Identität, Compliance; Management und Governance	AWS-Services: Amazon ECS; Amazon Aurora; AWS Fargate; AWS Secrets Manager; Amazon VPC

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie AWS Secrets Manager verwenden, um Datenbankanmeldeinformationen während ihres gesamten Lebenszyklus zu rotieren, zu verwalten und abzurufen. Benutzer und Anwendungen rufen Secrets mit einem Aufruf der Secrets-Manager-API ab, sodass keine Hartcodierung sensibler Informationen im Klartext erforderlich ist.

Wenn Sie Container für Microservice-Workloads verwenden, können Sie Anmeldeinformationen sicher in AWS Secrets Manager speichern. Um die Konfiguration vom Code zu trennen, werden diese Anmeldeinformationen häufig in den Container eingefügt. Es ist jedoch wichtig, Ihre Anmeldeinformationen regelmäßig und automatisch zu rotieren. Es ist auch wichtig, die Möglichkeit zu unterstützen, Anmeldeinformationen nach dem Widerruf zu aktualisieren. Gleichzeitig erfordern Anwendungen die Möglichkeit, Anmeldeinformationen zu rotieren und gleichzeitig mögliche Auswirkungen auf die nachgelagerte Verfügbarkeit zu reduzieren.

Dieses Muster beschreibt, wie Sie Ihre Secrets rotieren, die mit AWS Secrets Manager innerhalb Ihrer Container gesichert sind, ohne dass Ihre Container neu gestartet werden müssen. Darüber hinaus reduziert dieses Muster die Anzahl der Suchen nach Anmeldeinformationen in Secrets Manager mithilfe der clientseitigen Caching-Komponente von Secrets Manager . Wenn Sie die clientseitige Caching-Komponente verwenden, um die Anmeldeinformationen innerhalb der Anwendung zu aktualisieren, muss der Container nicht neu gestartet werden, um rotierte Anmeldeinformationen abzurufen.

Dieser Ansatz funktioniert für Amazon Elastic Kubernetes Service (Amazon EKS) und Amazon Elastic Container Service (Amazon ECS).

Zwei Szenarien werden behandelt. Im Einzelbenutzerszenario werden die Datenbankanmeldeinformationen bei der Rotation von Secrets aktualisiert, indem die abgelaufenen Anmeldeinformationen erkannt werden. Der Cache für Anmeldeinformationen wird angewiesen, das Secret zu aktualisieren, und dann stellt die Anwendung die Datenbankverbindung wieder her. Die clientseitige Caching-Komponente speichert die Anmeldeinformationen innerhalb der Anwendung zwischen und trägt dazu bei, dass Sie sich bei jeder Suche nach Anmeldeinformationen nicht an Secrets Manager wenden. Die Anmeldeinformationen werden innerhalb der Anwendung rotiert, ohne dass die Aktualisierung der Anmeldeinformationen durch einen Neustart des Containers erzwungen werden muss.

Im zweiten Szenario wird das Secret gedreht, indem zwischen zwei Benutzern gewechselt wird. Zwei aktive Benutzer reduzieren das Risiko von Ausfallzeiten, da die Anmeldeinformationen eines Benutzers immer aktiv sind. Die Rotation von Anmeldeinformationen für zwei Benutzer ist hilfreich, wenn Sie eine große Bereitstellung mit Clustern haben, in denen es zu einer geringen Verzögerung bei der Verbreitung von Aktualisierungen der Anmeldeinformationen kommen kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Anwendung, die in einem Container in Amazon EKS oder Amazon ECS ausgeführt wird.
- In Secrets Manager gespeicherte Anmeldeinformationen mit aktivierter Rotation .
- Ein zweiter Satz von Anmeldeinformationen, die in Secrets Manager gespeichert sind, wenn die Zwei-Benutzer-Lösung bereitgestellt wird. Codebeispiele finden Sie im GitHub Repository aws-secrets-manager-rotation-lambdas .
- Eine Amazon-Aurora-Datenbank.

Einschränkungen

- Dieses Beispiel ist für Python-Anwendungen bestimmt. Für Java-Anwendungen können Sie die clientseitige Java-Caching-Komponente oder die clientseitige JDBC-Caching-Bibliothek für Secrets Manager verwenden.

Architektur

Zielarchitektur

Szenario 1 – Rotation von Anmeldeinformationen für einen einzelnen Benutzer

Im ersten Szenario wird eine einzelne Datenbankanmeldeinformation regelmäßig von Secrets Manager gedreht. Der Anwendungscontainer wird in Fargate ausgeführt. Wenn die erste Datenbankverbindung hergestellt wird, ruft der Anwendungscontainer die Datenbankanmeldeinformationen für Aurora ab. Die Secrets-Manager-Caching-Komponente speichert dann die Anmeldeinformationen für den zukünftigen Verbindungsaufbau zwischen. Wenn der Drehungszeitraum abgelaufen ist, laufen die Anmeldeinformationen ab und die Datenbank gibt einen Authentifizierungsfehler zurück. Die Anwendung ruft dann die rotierten Anmeldeinformationen ab, macht den Cache ungültig und aktualisiert den Cache der Anmeldeinformationen über die clientseitige Caching-Komponente von Secrets Manager.

In diesem Szenario kann es zu einer minimalen Unterbrechung kommen, während die Anmeldeinformationen gedreht werden und veraltete Verbindungen die veralteten Anmeldeinformationen verwenden. Dieses Problem kann mithilfe des Szenarios mit zwei Benutzern behoben werden.

Szenario 2 – Rotation der Anmeldeinformationen für zwei Benutzer

Im zweiten Szenario werden von Secrets Manager regelmäßig zwei Datenbankbenutzeranmeldeinformationen (die von Alice und Bob) rotiert. Der Anwendungscontainer wird in einem Fargate-Cluster ausgeführt. Wenn die erste Datenbankverbindung hergestellt wird, ruft der Anwendungscontainer die Aurora-Datenbankanmeldeinformationen für den ersten Benutzer (Alice) ab. Die Secrets-Manager-Caching-Komponente speichert dann die Anmeldeinformationen für den zukünftigen Verbindungsaufbau zwischen.

Obwohl es zwei Benutzer und Anmeldeinformationen gibt, wird nur eine aktive Anmeldeinformation von Secrets Manager verwaltet. In diesem Fall läuft die Caching-Komponente regelmäßig ab und ruft die neuesten Anmeldeinformationen ab. Wenn der Secrets-Manager-Rotationszeitraum länger als das Cache-Timeout ist, übernimmt die Caching-Komponente die gedrehten Anmeldeinformationen für den zweiten Benutzer (Bob). Wenn beispielsweise der Cache-Ablauf in Minuten und der Drehungszeitraum in Tagen gemessen wird, ruft die Caching-Komponente die neuen Anmeldeinformationen im Rahmen ihrer regelmäßigen Cache-Aktualisierung ab. Auf diese Weise wird die Ausfallzeit minimiert, da die Anmeldeinformationen jedes Benutzers für eine Secrets-Manager-Rotation aktiv sind.

Automatisierung und Skalierung

Sie können AWS CloudFormation verwenden, um dieses Muster bereitzustellen, indem Sie Infrastruktur als Code verwenden. Dadurch wird der Anwendungscontainer erstellt und erstellt, die Fargate-Aufgabe erstellt, der Container in Fargate bereitgestellt und Secrets Manager mit Aurora eingerichtet und konfiguriert. Anweisungen zur step-by-step Bereitstellung finden Sie in der Readme-Datei.

Tools

Tools

- AWS Secrets Manager ermöglicht den Ersatz von fest codierten Anmeldeinformationen, einschließlich Passwörtern, durch einen API-Aufruf an Secrets Manager, um das Secret abzurufen. Da Secrets Manager das Secret automatisch nach einem Zeitplan rotieren kann, können Sie langfristige Secrets durch kurzfristige ersetzen, wodurch das Risiko einer Kompromittierung reduziert wird.
- Docker hilft Entwicklern dabei, jede Anwendung als leichtgewichtigen, portablen und selbstzureichenden Container zu packen, zu versenden und auszuführen.

Code

Python-Beispielcode

Dieses Muster verwendet die clientseitige Python-Caching-Komponente für Secrets Manager, um die Authentifizierungsanmeldeinformationen beim Herstellen der Datenbankverbindung abzurufen. Die clientseitige Caching-Komponente trägt dazu bei, dass Sie Secrets Manager nicht jedes Mal kontaktieren.

Wenn nun der Rotationszeitraum abgelaufen ist, sind die zwischengespeicherten Anmeldeinformationen abgelaufen und die Verbindung mit der Datenbank führt zu einem Authentifizierungsfehler. Für MySQL lautet der Authentifizierungsfehlercode 1045. In diesem Beispiel wird Amazon Aurora für MySQL verwendet, obwohl Sie eine andere Engine wie PostgreSQL verwenden könnten. Nach dem Authentifizierungsfehler wird der Fehler vom Code für die Ausnahmebehandlung der Datenbankverbindung erfasst. Anschließend wird die clientseitige Caching-Komponente von Secrets Manager angewiesen, das Secret zu aktualisieren und dann die Datenbankverbindung erneut zu authentifizieren und wiederherzustellen. Wenn Sie PostgreSQL oder eine andere Engine verwenden, müssen Sie den entsprechenden Authentifizierungsfehlercode suchen.

Die Containeranwendung kann jetzt das Datenbankpasswort mit dem rotierten Passwort aktualisieren, ohne den Container neu zu starten.

Platzieren Sie den folgenden Code in Ihrem Anwendungscode, der Datenbankverbindungen verarbeitet. In diesem Beispiel wird Django verwendet und das Datenbank-Backend wird durch einen Datenbank-Wrapper für Verbindungen ersetzt. Wenn Sie eine andere Programmiersprache oder Datenbankverbindungsbibliothek verwenden, finden Sie in Ihrer Datenbankverbindungsbibliothek Informationen zum Abrufen von Datenbankverbindungen.

```
    def get_new_connection(self, conn_params):
        try:
            logger.info("get connection")
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn =super(DatabaseWrapper,self).get_new_connection(conn_params)
            return conn
        except MySQLdb.OperationalError as e:
            error_code=e.args[0]
            if error_code!=1045:
                raise e

            logger.info("Authentication error. Going to refresh secret and try again.")
            databasecredentials.refresh_now()
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn=super(DatabaseWrapper,self).get_new_connection(conn_params)
            logger.info("Successfully refreshed secret and established new database
connection.")
            return conn
```

AWS- CloudFormation und Python-Code

- https://github.com/aws-samples/aws-secrets-manager-credential-rotation-without-container-restart

Polen

Aufrechterhaltung der Anwendungsverfügbarkeit während der Rotation von Anmeldeinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Caching-K omponente.	Laden Sie die clientseitige Caching-Komponente von	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Secrets Manager für Python herunter und installieren Sie sie. Den Download-Link finden Sie im Abschnitt Verwandte Ressourcen.	
Zwischenspeichern Sie die funktionierenden Anmeldeinformationen.	Verwenden Sie die clientseitige Caching-Komponente von Secrets Manager, um die funktionierenden Anmeldeinformationen lokal zwischenzuspeichern.	Developer
Aktualisieren Sie den Anwendungscode, um die Anmeldeinformationen bei dem nicht autorisierten Fehler der Datenbankverbindung zu aktualisieren.	Aktualisieren Sie den Anwendungscode, um Secrets Manager zum Abrufen und Aktualisieren von Datenbankanmeldeinformationen zu verwenden. Fügen Sie die Logik hinzu, um nicht autorisierte Fehlercodes zu behandeln, und rufen Sie dann die neu gedrehten Anmeldeinformationen ab. Siehe den Abschnitt Python-Beispielcode.	Developer

Zugehörige Ressourcen

Erstellen eines Secrets-Manager-Secrets

- Erstellen von Schlüsseln in AWS KMS
- Erstellen und Verwalten von Secrets mit AWS Secrets Manager

Erstellen eines Amazon-Aurora-Clusters

- Erstellen einer Amazon RDS-DB-Instance

Erstellen der Amazon-ECS-Komponenten

- Erstellen eines Clusters mit der klassischen Konsole
- Erstellen eines Docker-Images
- Erstellen eines privaten Repositorys
- Private Registrierung von Amazon ECR
- Übertragen eines Docker-Images
- Amazon-ECS-Aufgabendefinitionen
- Erstellen eines Amazon-ECS-Service in der klassischen Konsole

Herunterladen und Installieren der clientseitigen Caching-Komponente von Secrets Manager

- Python-Caching-Client

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Ausführen von Amazon-ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere

Erstellt von Akash Kumar (AWS)

Umgebung: Produktion	Technologien: Container und Microservices; Modernisierung	Workload: Alle anderen Workloads
AWS-Services: Amazon ECS; Amazon WorkSpaces; AWS Directory Service		

Übersicht

Amazon Elastic Container Service (Amazon ECS) Anywhere unterstützt die Bereitstellung von Amazon-ECS-Aufgaben in jeder Umgebung, einschließlich der von Amazon Web Services (AWS) verwalteten Infrastruktur und der vom Kunden verwalteten Infrastruktur. Sie können dies tun, während Sie eine vollständig von AWS verwaltete Steuerebene verwenden, die in der Cloud ausgeführt wird und immer auf dem neuesten Stand ist.

Unternehmen verwenden häufig Amazon WorkSpaces für die Entwicklung Container-basierter Anwendungen. Dies erforderte Amazon Elastic Compute Cloud (Amazon EC2) oder AWS Fargate mit einem Amazon ECS-Cluster, um ECS-Aufgaben zu testen und auszuführen. Durch die Verwendung von Amazon ECS Anywhere können Sie Amazon WorkSpaces als externe Instances direkt zu einem ECS-Cluster hinzufügen und Ihre Aufgaben direkt ausführen. Dies reduziert Ihre Entwicklungszeit, da Sie Ihren Container mit einem ECS-Cluster lokal auf Amazon testen können WorkSpaces. Sie können auch die Kosten für die Verwendung von EC2- oder Fargate-Instances zum Testen Ihrer Container-Anwendungen sparen.

Dieses Muster zeigt, wie ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere bereitgestellt werden. Es richtet den ECS-Cluster ein und verwendet AWS Directory Service Simple AD, um die zu starten WorkSpaces. Dann startet die Beispiel-ECS-Aufgabe NGINX im WorkSpaces.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto

- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- Auf Ihrem Computer konfigurierte AWS-Anmeldeinformationen

Architektur

Zieltechnologie-Stack

- Eine Virtual Private Cloud (VPC)
- Ein Amazon-ECS-Cluster
- Amazon WorkSpaces
- AWS Directory Service mit Simple AD

Zielarchitektur

Die Architektur umfasst die folgenden Services und Ressourcen:

- Ein ECS-Cluster mit öffentlichen und privaten Subnetzen in einer benutzerdefinierten VPC
- Simple AD in der VPC zur Bereitstellung des Benutzerzugriffs auf Amazon WorkSpaces
- Amazon WorkSpaces bereitgestellt in der VPC mit Simple AD
- AWS Systems Manager zum Hinzufügen von Amazon WorkSpaces als verwaltete Instances aktiviert
- Verwenden von Amazon ECS und AWS Systems Manager Agent (SSM Agent), Amazon wurde zu Systems Manager und dem ECS-Cluster WorkSpaces hinzugefügt
- Ein Beispiel für eine ECS-Aufgabe, die in der WorkSpaces im ECS-Cluster ausgeführt werden soll

Tools

- AWS Directory Service Simple Active Directory (Simple AD) ist ein eigenständig verwaltetes Verzeichnis, das von einem Samba 4 Active Directory kompatiblen Server unterstützt wird. Simple AD bietet eine Teilmenge der Funktionen von AWS Managed Microsoft AD, einschließlich der Möglichkeit, Benutzer zu verwalten und eine sichere Verbindung zu Amazon EC2-Instances herzustellen.

- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang.
- Amazon WorkSpaces unterstützt Sie bei der Bereitstellung virtueller, cloudbasierter Microsoft-Windows- oder Amazon-Linux-Desktops für Ihre Benutzer, die als bezeichnet werdenWorkSpaces. WorkSpaces Mit entfällt die Notwendigkeit, Hardware zu erwerben und bereitzustellen oder komplexe Software zu installieren.

Polen

Einrichten des ECS-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie den ECS-Cluster.	Um den ECS-Cluster zu erstellen, folgen Sie den Anweisungen in der AWS-Dokumentation , einschließlich der folgenden Schritte: • Wählen Sie für Clusterkompatibilität auswählen die Option Nur Netzwerk aus, die eine Amazon-WorkSpace als externe Instance für den ECS-Cluster unterstützt. • Wählen Sie , um eine neue VPC zu erstellen.	Cloud-Architekt

Starten von Amazon WorkSpaces

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Simple AD ein und starten Sie Amazon WorkSpaces.	Um ein Simple AD-Verzeichnis für Ihre neu erstellte VPC bereitzustellen und Amazon zu starten WorkSpaces, folgen Sie den Anweisungen in der AWS-Dokumentation .	Cloud-Architekt

Einrichten von AWS Systems Manager für eine Hybrid-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die angehängten Skripts herunter.	Laden Sie auf Ihrem lokalen Computer die `ssm-activation.json` Dateien `ssm-trust-policy.json` und herunter, die sich im Abschnitt Anhänge befinden.	Cloud-Architekt

Fügen Sie die IAM-Rolle hinzu.	Fügen Sie Umgebungsvariablen basierend auf Ihren Geschäftsanforderungen hinzu.
	`export AWS_DEFAULT_REGION=${AWS_REGION_ID}`
	`export ROLE_NAME=${ECS_TASK_ROLE}`
	`export CLUSTER_NAME=${ECS_CLUSTER_NAME}`
	`export SERVICE_NAME=${ECS_CLUSTER_SERVICE_NAME}`
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie den folgenden Befehl aus. `aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file://ssm-trust-policy.json`	
Fügen Sie die AmazonSSM ManagedInstanceCore - Richtlinie zur IAM-Rolle hinzu.	Führen Sie den folgenden Befehl aus. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`	Cloud-Architekt
Fügen Sie die AmazonEC2 ContainerServiceforEC2Role-Richtlinie zur IAM-Rolle hinzu.	Führen Sie den folgenden Befehl aus. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`	Cloud-Architekt
Überprüfen Sie die IAM-Rolle.	Führen Sie den folgenden Befehl aus, um die IAM-Rolle zu überprüfen. `aws iam list-attached-role-policies --role-name $ROLE_NAME`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Systems Manager.	Führen Sie den folgenden Befehl aus. `aws ssm create-activation --iam-role $ROLE_NAME | tee ssm-activation.json`	Cloud-Architekt

WorkSpaces Dem ECS-Cluster hinzufügen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung zu Ihrem her WorkSpaces.	Um eine Verbindung zu Ihren Workspaces herzustellen und diese einzurichten, folgen Sie den Anweisungen in der AWS-Dokumentation.	App-Developer
Laden Sie das ecs-where-Installationsskript herunter.	Führen Sie an der Eingabeaufforderung den folgenden Befehl aus. `curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh" && sudo chmod +x ecs-anywhere-install.sh`	App-Developer
Überprüfen Sie die Integrität des Shell-Skripts.	(Optional) Führen Sie den folgenden Befehl aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`curl -o "ecs-anywhere-install.sh.sha256" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh.sha256" && sha256sum -c ecs-anywhere-install.sh.sha256`	
Fügen Sie ein EPEL-Repository auf Amazon Linux hinzu.	Um ein EPEL-Repository (Extra Packages for Enterprise Linux) hinzuzufügen, führen Sie den Befehl aus `sudo amazon-linux-extras install epel -y`.	App-Developer
Installieren Sie Amazon ECS Anywhere .	Verwenden Sie den folgenden Befehl, um das Installationsskript auszuführen. `sudo ./ecs-anywhere-install.sh --cluster $CLUSTER_NAME --activation-id $ACTIVATION_ID --activation-code $ACTIVATION_CODE --region $AWS_REGION`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Instance-Informationen aus dem ECS-Cluster.	Führen Sie den folgenden Befehl auf Ihrem lokalen Computer aus, um die Systems Manager- und ECS-Cluster-Instance-Informationen zu überprüfen und zu überprüfen, die dem Cluster hinzugefügt WorkSpaces wurden. `aws ssm describe-instance-information" && "aws ecs list-container-instances --cluster $CLUSTER_NAME`	App-Developer

Hinzufügen einer ECS-Aufgabe für die WorkSpaces

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für die Aufgabenausführung.	Laden Sie `task-execution-assume-role.json` und `external-task-definition.json` aus dem Abschnitt Anhänge herunter. Führen Sie auf Ihrem lokalen Computer den folgenden Befehl aus. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	
Fügen Sie die Richtlinie zur Ausführungsrolle hinzu.	Führen Sie den folgenden Befehl aus. `aws iam --region $AWS_DEFAULT_REGION attach-role-policy --role-name $ECS_TASK_EXECUTION_ROLE --policy-arn arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`	Cloud-Architekt
Erstellen Sie eine Aufgabenrolle.	Führen Sie den folgenden Befehl aus. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie die Aufgabendefinition für den Cluster.	Führen Sie auf Ihrem lokalen Computer den folgenden Befehl aus. `aws ecs register-task-definition --cli-input-json file://external-task-definition.json`	Cloud-Architekt
Führen Sie die Aufgabe aus.	Führen Sie auf Ihrem lokalen Computer den folgenden Befehl aus. `aws ecs run-task --cluster $CLUSTER_NAME --launch-type EXTERNAL --task-definition nginx`	Cloud-Architekt

Überprüfen Sie den Status der Aufgabenausführung.	Führen Sie den folgenden Befehl aus, um die Aufgaben-ID abzurufen.
	`export TEST_TASKID=$(aws ecs list-tasks --cluster $CLUSTER_NAME | jq -r '.taskArns[0]')`
	Führen Sie mit der Aufgaben-ID den folgenden Befehl aus.
	`aws ecs describe-tasks --cluster $CLUSTER_NAME --tasks ${TEST_TASKID}`
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Aufgabe auf dem WorkSpace.	Um zu überprüfen, ob NGINX auf der ausgeführt wird WorkSpace, führen Sie den Befehl aus `curl http://localhost:8080` .	App-Developer

Zugehörige Ressourcen

- ECS-Cluster
- Einrichten einer Hybrid-Umgebung
- Amazon WorkSpaces
- Simple AD

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 EC2-Linux-Instance aus

Erstellt von Vijai Anand Ramalingam (AWS) und Sreelaxmi Pai (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Mikroservices; Softwareentwicklung und Tests; Web- und mobile Apps	Arbeitslast: Microsoft
AWS-Services: Amazon EC2; Elastic Load Balancing (ELB)		

Übersicht

Dieses Muster ist für Benutzer gedacht, die damit beginnen, ihre Anwendungen in der Amazon Web Services (AWS) Cloud zu containerisieren. Wenn Sie beginnen, Apps in der Cloud zu containerisieren, sind in der Regel keine Container-Orchestrierungsplattformen eingerichtet. Mit diesem Muster können Sie schnell eine Infrastruktur auf AWS einrichten, um Ihre containerisierten Anwendungen zu testen, ohne dass eine aufwändige Container-Orchestrierungsinfrastruktur erforderlich ist.

Der erste Schritt auf dem Weg zur Modernisierung besteht darin, die Anwendung zu transformieren. Wenn es sich um eine ältere .NET Framework-Anwendung handelt, müssen Sie zuerst die Laufzeit auf ASP.NET Core ändern. Führen Sie dann die folgenden Schritte aus:

- Erstellen Sie das Docker-Container-Image
- Führen Sie den Docker-Container mit dem erstellten Image aus
- Überprüfen Sie die Anwendung, bevor Sie sie auf einer beliebigen Container-Orchestrierungsplattform wie Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) bereitstellen.

Dieses Muster behandelt die Aspekte der Erstellung, Ausführung und Validierung der modernen Anwendungsentwicklung auf einer Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instance.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Eine AWS Identity and Access Management (IAM) -Rolle mit ausreichendem Zugriff, um AWS-Ressourcen für dieses Muster zu erstellen
- Visual Studio Community 2022 oder höher wurde heruntergeladen und installiert
- Ein auf ASP.NET Core modernisiertes .NET Framework-Projekt
- Ein Repository GitHub

Produktversionen

- Visual Studio Community 2022 oder höher

Architektur

Zielarchitektur

Dieses Muster verwendet eine CloudFormation AWS-Vorlage, um die im folgenden Diagramm gezeigte Architektur mit hoher Verfügbarkeit zu erstellen. Eine Amazon EC2 EC2-Linux-Instance wird in einem privaten Subnetz gestartet. AWS Systems Manager Session Manager wird verwendet, um auf die private Amazon EC2 EC2-Linux-Instance zuzugreifen und die API zu testen, die im Docker-Container läuft.

1. Zugriff auf die Linux-Instance über Session Manager

Tools

AWS-Services

- AWS-Befehlszeilenschnittstelle — AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS-CLI-Befehle ausführen, die Funktionen implementieren, die denen der browserbasierten AWS-Managementkonsole entsprechen.

- AWS-Managementkonsole — Die AWS-Managementkonsole ist eine Webanwendung, die eine breite Sammlung von Servicekonsolen für die Verwaltung von AWS-Ressourcen umfasst und sich auf diese bezieht. Wenn Sie sich zum ersten Mal anmelden, sehen Sie die Startseite der Konsole. Die Startseite bietet Zugriff auf jede Servicekonsole und bietet einen zentralen Ort, an dem Sie auf die Informationen zugreifen können, die Sie zur Ausführung Ihrer AWS-bezogenen Aufgaben benötigen.
- AWS Systems Manager Session Manager — Session Manager ist eine vollständig verwaltete Funktion von AWS Systems Manager. Mit Session Manager können Sie Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten. Session Manager bietet eine sichere und überprüfbare Knotenverwaltung, ohne dass eingehende Ports geöffnet, Bastion-Hosts verwaltet oder SSH-Schlüssel verwaltet werden müssen.

Andere Tools

- Visual Studio 2022 — Visual Studio 2022 ist eine integrierte Entwicklungsumgebung (IDE).
- Docker — Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.

Code

```
FROM mcr.microsoft.com/dotnet/aspnet:5.0 AS base
 WORKDIR /app
EXPOSE 80
EXPOSE 443

FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build
WORKDIR /src
COPY ["DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj", "DemoNetCoreWebAPI/"]
RUN dotnet restore "DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj"
COPY . .
WORKDIR "/src/DemoNetCoreWebAPI"
RUN dotnet build "DemoNetCoreWebAPI.csproj" -c Release -o /app/build

FROM build AS publish
RUN dotnet publish "DemoNetCoreWebAPI.csproj" -c Release -o /app/publish

FROM base AS final
WORKDIR /app
COPY --from=publish /app/publish .
```

```
ENTRYPOINT ["dotnet", "DemoNetCoreWebAPI.dll"]
```

Epen

Entwickeln Sie die ASP.NET Core-Web-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie mit Visual Studio ein Beispiel für eine ASP.NET Core-Web-API.	Gehen Sie wie folgt vor, um ein Beispiel für eine ASP.NET Core-Web-API zu erstellen: 1. Öffnen Sie Visual Studio 2022. 2. Wählen Sie Create a new project (Neues Projekt erstellen). 3. Wählen Sie die ASP.NET Core Web API-Proje ktvorlage aus und klicken Sie auf Weiter. 4. Geben Sie als Projektna men DemoNetCoreWebAPI ein und wählen Sie Weiter aus. 5. Wählen Sie Erstellen. 6. Um das Projekt lokal auszuführen, drücken Sie F5. 7. Stellen Sie mithilfe von Swagger sicher, dass der WeatherForecastStandard-API-Endpunkt die Ergebniss e zurückgibt. 8. Öffnen Sie die Befehlsze ile, navigieren Sie zum	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Projektordner .csproj und führen Sie die folgenden Befehle aus, um die neue Web-API in Ihr Repository zu übertragen. GitHub
	
	`git add --all`
	`git commit -m “Initial Version”`
	`git push`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Docker-Datei.	Gehen Sie wie folgt vor, um ein Dockerfile zu erstellen: • Erstellen Sie das Dockerfile manuell mithilfe des Dockerfile-Beispiels im Abschnitt Code. Wählen Sie je nach den Anforderungen das entsprechende .NET-Basisimage aus. Informationen zu Images, die sich auf .NET und ASP.NET Core beziehen, finden Sie unter Docker Hub. • Erstellen Sie das Dockerfile mit Visual Studio und Docker Desktop. Klicken Sie im Solution Explorer mit der rechten Maustaste auf das Projekt und wählen Sie Hinzufügen -> Docker Support. Wählen Sie für Target OS Linux aus. Stellen Sie sicher, dass sich das neue Dockerfile im selben Pfad wie die Lösungsdatei (.sln) befindet. Führen Sie den folgenden Befehl aus, um die Änderungen in Ihr GitHub Repository zu übertragen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`git add --all`
	`git commit -m “Dockerfile added”`
	`git push`	

Richten Sie die Amazon EC2 EC2-Linux-Instance ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Infrastruktur ein.	Starten Sie die CloudFormation AWS-Vorlage, um die Infrastruktur zu erstellen, die Folgendes umfasst: • Eine virtuelle private Cloud (VPC), die den AWS VPC Quick Start verwendet, mit zwei öffentlichen und zwei privaten Subnetzen, die sich über zwei Availability Zones erstrecken. • Die für die Aktivierung von AWS Systems Manager erforderliche IAM-Rolle. • In einem der privaten Subnetze eine Amazon Linux 2-Demo-Instance mit dem neuesten SSM-Agenten. Obwohl diese Instance keine direkte Verbindung über das Internet hat, kann sie mit dem AWS Systems Manager Session Manager sicher aufgerufen werden,	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ohne dass ein Bastion-Host erforderlich ist. Weitere Informationen zum Zugriff auf eine private Amazon EC2 EC2-Insta nce mit Session Manager, ohne dass ein Bastion-Host erforderlich ist, finden Sie im Blogbeitrag Toward a bastion-less world.	
Melden Sie sich bei der Amazon EC2 EC2-Linux-Instance an.	Gehen Sie wie folgt vor, um eine Verbindung zur Amazon EC2 EC2-Linux-Instance im privaten Subnetz herzustellen: 1. Öffnen Sie die Amazon EC2-Konsole. 2. Wählen Sie im Navigatio nsbereich Instances aus. 3. Wählen Sie die Amazon Linux 2-Demo-Instance und dann Connect aus. 4. Klicken Sie auf Session Manager. 5. Wählen Sie Connect, um ein neues Terminalfenster zu öffnen. 6. Führen Sie den folgenden Befehl aus. `sudo su`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren und starten Sie Docker.	Gehen Sie wie folgt vor, um Docker in der Amazon EC2 EC2-Linux-Instance zu installieren und zu starten:
	1. Führen Sie den folgenden Befehl aus, um Docker zu installieren.
	`yum install -y docker`
	2. Führen Sie den folgenden Befehl aus, um den Docker-Dienst zu starten.
	`service docker start`
	3. Führen Sie den folgenden Befehl aus, um die Docker-Installation zu überprüfen.
	`docker info`
		App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installiere Git und klone das Repository.	Gehen Sie wie folgt vor, um Git auf der Amazon EC2 EC2-Linux-Instance zu installieren und das Repository von GitHub zu klonen.
	1. Führen Sie den folgenden Befehl aus, um Git zu installieren.
	`yum install git -y`
	2. Führen Sie den folgenden Befehl aus, um das Repository zu klonen.
	`git clone https://github.com/<username>/<repo-name>.git`
	3. Führen Sie den folgenden Befehl aus, um zur Dockerfile zu navigieren.
	`cd <repo-name>/DemoNetCoreWebAPI/`
		App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Docker-Container und führen Sie ihn aus.	Gehen Sie wie folgt vor, um das Docker-Image zu erstellen und den Container in der Amazon EC2 EC2-Linux-Instance auszuführen:
	1. Führen Sie den folgenden Befehl aus, um das Docker-Image zu erstellen.
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Führen Sie den folgenden Befehl aus, um alle Docker-Images anzuzeigen.
	`docker images`
	3. Führen Sie den folgenden Befehl aus, um den Container zu erstellen und auszuführen.
	`docker run -d -p 80:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
		App-Entwickler, AWS-Administrator, AWS DevOps

Testen Sie die Web-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Web-API mit dem Befehl curl.	Führen Sie den folgenden Befehl aus, um die Web-API zu testen. `curl -X GET "http://localhost/WeatherForecast" -H  "accept: text/plain"` Überprüfen Sie die API-Antwort. Hinweis: Sie können die curl-Befehle für jeden Endpunkt von Swagger abrufen, wenn Sie ihn lokal ausführen.	App-Developer

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle Ressourcen.	Löschen Sie den Stapel, um alle Ressourcen zu entfernen . Dadurch wird sichergestellt, dass Ihnen keine Dienste in Rechnung gestellt werden, die Sie nicht nutzen.	AWS-Administrator, AWS DevOps

Zugehörige Ressourcen

- Stellen Sie mithilfe von PuTTY von Windows aus eine Connect zu Ihrer Linux-Instance her
- Erstellen Sie eine Web-API mit ASP.NET Core

- Auf dem Weg zu einer Welt ohne Bastionen

Ausführen von nachrichtengesteuerten Workloads in großem Umfang mithilfe von AWS Fargate

Erstellt von Stan Zubarev (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices; Messaging und Kommunikation; Datenbanken	AWS-Services: AWS Fargate; Amazon SQS; Amazon DynamoDB

Übersicht

Dieses Muster zeigt, wie nachrichtengesteuerte Workloads in der AWS Cloud mithilfe von Containern und AWS Fargate in großem Umfang ausgeführt werden.

Die Verwendung von Containern zur Verarbeitung von Daten kann hilfreich sein, wenn die Datenmenge, die eine Anwendung verarbeitet, die Einschränkungen von funktionsbasierten Serverless-Computing-Services überschreitet. Wenn eine Anwendung beispielsweise mehr Rechenkapazität oder Verarbeitungszeit benötigt, als AWS Lambda bietet, kann die Verwendung von Fargate die Leistung verbessern.

Im folgenden Beispiel wird das AWS Cloud Development Kit (AWS CDK) in TypeScript verwendet, um die folgenden Ressourcen in der AWS Cloud zu konfigurieren und bereitzustellen:

- Ein Fargate-Service
- Eine Amazon Simple Queue Service (Amazon SQS)-Warteschlange
- Eine Amazon-DynamoDB-Tabelle.
- Ein Amazon CloudWatch -Dashboard

Der Fargate-Service empfängt und verarbeitet Nachrichten aus der Amazon SQS-Warteschlange und speichert sie dann in der Amazon-DynamoDB-Tabelle. Sie können mithilfe des CloudWatch Dashboards überwachen, wie viele Amazon SQS-Nachrichten verarbeitet werden und wie viele DynamoDB-Elemente von Fargate erstellt werden.

Hinweis: Sie können auch den Beispielcode dieses Musters verwenden, um komplexere Datenverarbeitungs-Workloads in ereignisgesteuerten Serverless-Architekturen zu erstellen. Weitere

Informationen finden Sie unter Ausführen von ereignisgesteuerten und geplanten Workloads in großem Umfang mit AWS Fargate .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die neueste Version der AWS Command Line Interface (AWS CLI), die auf Ihrem lokalen Computer installiert und konfiguriert ist
- Git , auf Ihrem lokalen Computer installiert und konfiguriert
- Das AWS-CDK , das auf Ihrem lokalen Computer installiert und konfiguriert ist
- Go , auf Ihrem lokalen Computer installiert und konfiguriert
- Docker , auf Ihrem lokalen Computer installiert und konfiguriert

Architektur

Zieltechnologie-Stack

- Amazon SQS
- AWS Fargate
- Amazon DynamoDB

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Ausführung von nachrichtengesteuerten Workloads in der AWS Cloud mithilfe von Fargate:

Das Diagramm zeigt den folgenden Workflow:

1. Der Fargate-Service verwendet Amazon SQS-Langabfragen, um Nachrichten aus einer Amazon SQSWarteschlange zu empfangen.
2. Der Fargate-Service verarbeitet dann die Amazon SQS-Nachrichten und speichert sie in einer DynamoDB-Tabelle.

Automatisierung und Skalierung

Um die Skalierung Ihrer Fargate-Aufgabenanzahl zu automatisieren, können Sie Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling konfigurieren. Es hat sich bewährt, die Skalierungsrichtlinie basierend auf der Anzahl der sichtbaren Nachrichten in der Amazon SQS-Warteschlange Ihrer Anwendung zu konfigurieren.

Weitere Informationen finden Sie unter Skalierung basierend auf Amazon SQS im Benutzerhandbuch für Amazon EC2 Auto Scaling.

Tools

AWS-Services

- AWS Fargate unterstützt Sie beim Ausführen von Containern, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2)-Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.

Code

Der Code für dieses Muster ist im GitHub sqs-fargate-ddb-cdk-go-Repository verfügbar.

Polen

Erstellen und Bereitstellen der Ressourcen mithilfe des AWS-CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub sqs-fargate-ddb-cdk-go-Repository auf Ihren lokalen Computer,	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samples/sqs-fargate-ddb-cdk-go.git`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die AWS CLI für das richtige AWS-Konto konfiguriert ist und dass das AWS-CDK über die erforderlichen Berechtigungen verfügt.	Um zu überprüfen, ob Ihre AWS CLI-Konfigurations einstellungen korrekt sind, können Sie den folgenden Amazon Simple Storage Service (Amazon S3) ls-Befehl ausführen: `aws s3 ls` Dieses Verfahren erfordert auch, dass das AWS-CDK über Berechtigungen zur Bereitstellung der Infrastru ktur in Ihrem AWS-Konto verfügt. Um die erforderl ichen Berechtigungen zu erteilen, müssen Sie ein benanntes AWS-Profil in AWS CLI erstellen und es als AWS_PROFILE-Umgebung svariable exportieren. Hinweis: Wenn Sie das AWS-CDK noch nicht in Ihrem AWS-Konto verwendet haben, müssen Sie zuerst die erforderlichen AWS-CDK-Ressourcen bereitstellen. Weitere Informationen finden Sie unter Bootstrapping im AWS CDK v2-Entwicklerhandb uch.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den AWS-CDK-Stack in Ihrem AWS-Konto bereit.	1. Erstellen Sie ein Container-Image, indem Sie den folgenden AWS CLI-Befehl ausführen:
	`docker build -t go-fargate .`
	2. Öffnen Sie das AWS-CDK-Verzeichnis, indem Sie den folgenden Befehl ausführen:
	`cd cdk`
	3. Installieren Sie die erforderlichen npm-Module, indem Sie den folgenden Befehl ausführen:
	`npm i`
	4. Stellen Sie das AWS-CDK-Muster in Ihrem AWS-Konto bereit, indem Sie den folgenden Befehl ausführen:
	`cdk deploy --profile ${AWS_PROFILE}`
		App-Developer

Testen der Einrichtung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie eine Testnachricht an die Amazon SQS-Warteschlange.	Anweisungen finden Sie unter Senden von Nachrichten an eine Warteschlange (Konsole) im Amazon SQS-Entwicklerhandbuch.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispiel für das Testen einer Amazon SQS-Nachricht `{ "message": "hello, Fargate" }`	
Stellen Sie sicher, dass die Testnachricht in den CloudWatch Protokollen des Fargate-Service angezeigt wird.	Folgen Sie den Anweisungen unter Anzeigen von CloudWatch Protokollen im Amazon-ECS-Entwicklerhandbuch. Stellen Sie sicher, dass Sie die Protokolle für die go-fargate-service Protokollgruppe im go-service-cluster ECS-Cluster überprüfen.	App-Developer
Stellen Sie sicher, dass die Testnachricht in der DynamoDB-Tabelle angezeigt wird.	1. Öffnen Sie die DynamoDB-Konsole. 2. Wählen Sie im linken Navigationsbereich Tables (Tabellen) aus. Wählen Sie dann die folgende Tabelle aus der Liste aus: sqs-fargate-ddb-table. 3. Wählen Sie Explore Table Items (Tabellenelemente erkudnen) aus. 4. Stellen Sie sicher, dass die Testnachricht in der Liste Zurückgegebene Elemente angezeigt wird.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass der Fargate-Service Nachrichten an - CloudWatch Protokolle sendet.	1. Öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im linken Navigationsbereich Dashboards aus. 3. Wählen Sie in der Liste Benutzerdefinierte Dashboards das Dashboard mit dem Namen ausgo-service-dashboard. 4. Stellen Sie sicher, dass die Testnachricht in den Protokollen angezeigt wird. Hinweis: Das AWS-CDK erstellt das CloudWatch Dashboard in Ihrem AWS-Konto automatisch.	App-Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den AWS-CDK-Stack.	1. Öffnen Sie Ihr AWS-CDK-Verzeichnis in der AWS CLI, indem Sie den folgenden Befehl ausführen: `cd cdk` 2. Löschen Sie den AWS-CDK-Stack, indem Sie den folgenden Befehl ausführen:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk destroy --profile ${AWS_PROFILE}`	
Überprüfen Sie, ob der AWS-CDK-Stack gelöscht wurde.	Führen Sie den folgenden Befehl aus, um sicherzustellen, dass der Stack gelöscht wurde: `aws cloudformation list-stacks --query \ "StackSummaries[?contains(StackName,'SqsFargate')].StackStatus" \ --profile ${AWS_PROFILE}` Der in der Befehlsausgabe zurückgegebene `StackStatus` Wert ist `DELETE_COMPLETE`, wenn der Stack gelöscht wird. Weitere Informationen finden Sie unter Beschreiben und Auflisten Ihrer Stacks im AWS-CloudFormation Benutzerhandbuch.	App-Developer

Zugehörige Ressourcen

- Konfigurieren der AWS CLI (AWS CLI-Benutzerhandbuch für Version 2)
- API-Referenz (AWS-CDK-API-Referenz)
- AWS SDK for Go v2 (Go-Dokumentation)

Führen Sie zustandsbehaftete Workloads mit persistenter Datenspeicherung aus, indem Sie Amazon EFS auf Amazon EKS mit AWS Fargate verwenden

Erstellt von Ricardoais (AWS), Bolr Bersa (AWS) und Lucio PereSpeed (AWS)

Code-Repository: Amazon EKS mit Fargate und Amazon EFS	Umgebung: PoC oder Pilotprojekt	Technologien: Container und Microservices; Speicher und Backup
Workload: Open-Source	AWS-Services: Amazon EFS; Amazon EKS; AWS Fargate	

Übersicht

Dieses Muster bietet Anleitungen zur Aktivierung von Amazon Elastic File System (Amazon EFS) als Speichergerät für Container, die auf Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden, indem AWS Fargate zur Bereitstellung Ihrer Rechenressourcen verwendet wird.

Die in diesem Muster beschriebene Einrichtung folgt bewährten Sicherheitsmethoden und bietet standardmäßig Sicherheit im Ruhezustand und Sicherheit während der Übertragung. Um Ihr Amazon EFS-Dateisystem zu verschlüsseln, verwendet es einen AWS Key Management Service (AWS KMS)-Schlüssel. Sie können jedoch auch einen Schlüsselalias angeben, der den Prozess der Erstellung eines KMS-Schlüssels versendet.

Sie können die Schritte in diesem Muster ausführen, um einen Namespace und ein Fargate-Profil für eine proof-of-concept (PoC)-Anwendung zu erstellen, den Amazon EFS Container Storage Interface (CSI)-Treiber zu installieren, der zur Integration des Kubernetes-Clusters in Amazon EFS verwendet wird, die Speicherklasse zu konfigurieren und die PoC-Anwendung bereitzustellen. Diese Schritte führen zu einem Amazon-EFS-Dateisystem, das von mehreren Kubernetes-Workloads gemeinsam genutzt wird und über Fargate ausgeführt wird. Das Muster wird von Skripts begleitet, die diese Schritte automatisieren.

Sie können dieses Muster verwenden, wenn Sie Datenpersistenz in Ihren containerisierten Anwendungen wünschen und Datenverlust während Skalierungsvorgängen vermeiden möchten. Beispielsweise:

- -DevOps Tools – Ein häufiges Szenario ist die Entwicklung einer CI/CD-Strategie (Continuous Integration and Continuous Delivery). In diesem Fall können Sie Amazon EFS als gemeinsam genutztes Dateisystem verwenden, um Konfigurationen zwischen verschiedenen Instances des CI/CD-Tools oder einen Cache (z. B. ein Apache-Maven-Repository) für Pipeline-Phasen zwischen verschiedenen Instances des CI/CD-Tools zu speichern.
- Webserver – Ein häufiges Szenario ist die Verwendung von Apache als HTTP-Webserver. Sie können Amazon EFS als gemeinsam genutztes Dateisystem verwenden, um statische Dateien zu speichern, die von verschiedenen Instances des Webservers gemeinsam genutzt werden. In diesem Beispielszenario werden Änderungen direkt auf das Dateisystem angewendet, anstatt statische Dateien in ein Docker-Image einzubinden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein vorhandener Amazon-EKS-Cluster mit Kubernetes-Version 1.17 oder höher (getestet bis Version 1.27)
- Ein vorhandenes Amazon-EFS-Dateisystem, um ein Kubernetes zu binden StorageClass und Dateisysteme dynamisch bereitzustellen
- Cluster-Verwaltungsberechtigungen
- Kontext, der so konfiguriert ist, dass er auf den gewünschten Amazon-EKS-Cluster verweist

Einschränkungen

- Bei der Verwendung von Amazon EKS mit Fargate sind einige Einschränkungen zu berücksichtigen. Beispielsweise wird die Verwendung einiger Kubernetes-Konstrukte, wie z. B. DaemonSets und privilegierte Container, nicht unterstützt. Weitere Informationen zu Fargate-Einschränkungen finden Sie in den Überlegungen zu AWS Fargate in der Amazon EKS-Dokumentation.
- Der mit diesem Muster bereitgestellte Code unterstützt Workstations, auf denen Linux oder macOS ausgeführt wird.

Produktversionen

- AWS Command Line Interface (AWS CLI) Version 2 oder höher
- Amazon-EFS-CSI-Treiberversion 1.0 oder höher (getestet bis Version 2.4.8)
- eksctl Version 0.24.0 oder höher (getestet bis Version 0.158.0)
- jq Version 1.6 oder höher
- kubectl Version 1.17 oder höher (getestet bis Version 1.27)
- Kubernetes Version 1.17 oder höher (getestet bis Version 1.27)

Architektur

Die Zielarchitektur besteht aus der folgenden Infrastruktur:

- Eine Virtual Private Cloud (VPC)
- Zwei Availability Zones
- Ein öffentliches Subnetz mit einem NAT-Gateway, das Internetzugang bietet
- Ein privates Subnetz mit einem Amazon-EKS-Cluster und Amazon-EFS-Mountingzielen (auch bekannt als Mountingpunkte)
- Amazon EFS auf VPC-Ebene

Im Folgenden finden Sie die Umgebungsinfrastruktur für den Amazon-EKS-Cluster:

- AWS Fargate-Profile, die die Kubernetes-Konstrukte auf Namespace-Ebene aufnehmen
- Ein Kubernetes-Namespace mit:
  - Zwei Anwendungs-Pods, die auf Availability Zones verteilt sind
  - Ein persistenter Volume-Anspruch (PVC), der an ein persistentes Volume (PV) auf Cluster-Ebene gebunden ist
- Eine Cluster-weite PV, die an den microSD im Namespace gebunden ist und auf die Amazon-EFS-Mountingziele im privaten Subnetz außerhalb des Clusters verweist

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über die Befehlszeile mit AWS-Services interagieren können.
- Amazon Elastic File System (Amazon EFS) hilft Ihnen beim Erstellen und Konfigurieren freigegebener Dateisysteme in der AWS Cloud. In diesem Muster bietet es ein einfaches, skalierbares, vollständig verwaltetes und gemeinsam genutztes Dateisystem für die Verwendung mit Amazon EKS.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigenen Cluster installieren oder betreiben zu müssen.
- AWS Fargate ist eine Serverless-Compute-Engine für Amazon EKS. Es erstellt und verwaltet Rechenressourcen für Ihre Kubernetes-Anwendungen.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.

Andere Tools

- Docker ist eine Reihe von Platform as a Service (PaaS)-Produkten, die Virtualisierung auf Betriebssystemebene verwenden, um Software in Containern bereitzustellen.
- eksctl ist ein Befehlszeilen-Dienstprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.
- jq ist ein Befehlszeilen-Tool zum Analysieren von JSON.

Code

Der Code für dieses Muster wird in der GitHub Persistenzkonfiguration mit Amazon EFS in Amazon EKS unter Verwendung von AWS Fargate Repo bereitgestellt. Die Skripte sind nach Epics in den Ordnern `epic01` bis geordnet`epic06`, die der Reihenfolge im Abschnitt „PiCs“ in diesem Muster entsprechen.

Bewährte Methoden

Die Zielarchitektur umfasst die folgenden Services und Komponenten und folgt den bewährten Methoden des AWS Well-Architected Framework:

- Amazon EFS bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem. Dies wird als gemeinsam genutztes Dateisystem unter allen Replikationen der PoC-Anwendung verwendet, die in Pods ausgeführt werden, die in den privaten Subnetzen des ausgewählten Amazon-EKS-Clusters verteilt sind.
- Ein Amazon-EFS-Mountingziel für jedes private Subnetz. Dies bietet Redundanz pro Availability Zone innerhalb der Virtual Private Cloud (VPC) des Clusters.
- Amazon EKS, das die Kubernetes-Workloads ausführt. Sie müssen einen Amazon-EKS-Cluster bereitstellen, bevor Sie dieses Muster verwenden, wie im Abschnitt Voraussetzungen beschrieben.
- AWS KMS, das eine Verschlüsselung im Ruhezustand für den Inhalt bietet, der im Amazon EFS-Dateisystem gespeichert ist.
- Fargate verwaltet die Rechenressourcen für die Container, sodass Sie sich auf die Geschäftsanforderungen statt auf den Infrastrukturaufwand konzentrieren können. Das Fargate-Profil wird für alle privaten Subnetze erstellt. Es bietet Redundanz pro Availability Zone innerhalb der Virtual Private Cloud (VPC) des Clusters.
- Kubernetes-Pods zur Validierung, dass Inhalte von verschiedenen Instances einer Anwendung gemeinsam genutzt, verbraucht und geschrieben werden können.

Sekunden

Bereitstellen eines Amazon-EKS-Clusters (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-EKS-Cluster.	Wenn Sie bereits einen Cluster bereitgestellt haben, fahren Sie mit der nächsten Ausgabe fort. Erstellen Sie einen Amazon EKS-Cluster in Ihrem vorhandenen AWS-Konto. Verwenden Sie im GitHub Repo-Verzeichnis eines der Muster, um einen Amazon-EKS-Cluster mithilfe von Terraform oder eksctl bereitzustellen. Weitere	AWS-Administrator, Terraform - oder eksctl-Administrator, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie unter Erstellen eines Amazon-EKS-Clusters in der Amazon-EKS-Dokumentation. Hinweis: Im Terraform-Muster gibt es auch Beispiele, die zeigen, wie Sie Fargate-Profile mit Ihrem Amazon-EKS-Cluster verknüpfen, ein Amazon-EFS-Dateisystem erstellen und Amazon-EFS-CSI-Treiber in Ihrem Amazon-EKS-Cluster bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Umgebungsvariablen.	Führen Sie das Skript env.sh aus. Dadurch werden die in den nächsten Schritten erforderlichen Informationen bereitgestellt.
	`source ./scripts/env.sh`
	`Inform the AWS Account ID: <13-digit-account-id>`
	`Inform your AWS Region: <aws-Region-code>`
	`Inform your Amazon EKS Cluster Name: <amazon-eks-cluster-name>`
	`Inform the Amazon EFS Creation Token: <self-genereated-uuid>`
	Falls noch nicht angegeben, können Sie alle oben angeforderten Informationen mit den folgenden CLI-Befehlen abrufen.
	`# ACCOUNT ID`
	`aws sts get-caller-identity --query "Account" --output text`
	`# REGION CODE`
	`aws configure get region`
	`# CLUSTER EKS NAME`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws eks list-clusters --query "clusters" --output text`
	
	`# GENERATE EFS TOKEN uuidgen`	

Erstellen eines Kubernetes-Namespace und eines verknüpften Fargate-Profils

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Kubernetes-Namespace und ein Fargate-Profil für Anwendungs-Workloads.	Erstellen Sie einen Namespace für den Empfang der Anwendungs-Workloads, die mit Amazon EFS interagieren. Führen Sie das `create-k8s-ns-and-linked-fargate-profile.sh` -Skript aus. Sie können einen benutzerdefinierten Namespace-Namen oder den standardmäßig bereitgestellten Namespace verwenden`poc-efs-eks-fargate` . Mit einem benutzerdefinierten Anwendungs-Namespace-Namen: `export $APP_NAMESPACE=<CUSTOM_NAME> ./scripts/epic01/create-k8s-ns-and`	Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`-linked-fargate-pr ofile.sh \ -c "$CLUSTER_NAME" -n "$APP_NAMESPACE"`
	
	Ohne einen benutzerdefinierte n Anwendungs-Namespace-Namen:
	
	`./scripts/epic01/c reate-k8s-ns-and-l inked-fargate-prof ile.sh \ -c "$CLUSTER_NAME"`
	
	wobei der Name Ihres Amazon-EKS-Clusters `$CLUSTER_NAME` ist. Der `-n <NAMESPACE>` Parameter ist optional. Wenn er nicht informiert wird, wird ein standardmäßig generierter Namespace-Name angegeben .	

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie ein eindeutig es Token.	Amazon EFS benötigt ein Erstellungstoken, um einen idempotenten Vorgang sicherzustellen (das Aufrufen des Vorgangs mit demselben Erstellungstoken hat keine	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Auswirkungen). Um diese Anforderung zu erfüllen, müssen Sie mithilfe einer verfügbaren Technik ein eindeutiges Token generiere n. Sie können beispielsweise einen Universally Unique Identifier (UUID) generiere n, der als Erstellungstoken verwendet werden soll.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	Erstellen Sie das Dateisyst em für den Empfang der Datendateien, die von den Anwendungs-Workloads gelesen und geschrieben werden. Sie können ein verschlüsseltes oder nicht verschlüsseltes Dateisyst em erstellen. (Als bewährte Methode erstellt der Code für dieses Muster ein verschlüs seltes System, um die standardmäßige Verschlüs selung im Ruhezustand zu aktivieren.) Sie können einen eindeutigen, symmetris chen AWS KMS-Schlüssel verwenden, um Ihr Dateisyst em zu verschlüsseln. Wenn kein benutzerdefinierter Schlüssel angegeben ist, wird ein von AWS verwalteter Schlüssel verwendet. Verwenden Sie das create-ef s.sh-Skript, um ein verschlüs seltes oder nicht verschlüs seltes Amazon-EFS-Dateisy stem zu erstellen, nachdem Sie ein eindeutiges Token für Amazon EFS generiert haben. Mit Verschlüsselung im Ruhezustand, ohne KMS-Schlüssel:	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"`
	
	wobei `$CLUSTER_NAME` der Name Ihres Amazon-EKS-Clusters und ein eindeutiges Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist.
	
	Mit Verschlüsselung im Ruhezustand, mit einem KMS-Schlüssel:
	
	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"`
	
	wobei `$CLUSTER_NAME` der Name Ihres Amazon-EKS-Clusters`$EFS_CREATION_TOKEN`, ein eindeutiges Erstellungstoken für das Dateisystem und der Alias für den KMS-Schlüssel `$KMS_KEY_ALIAS` ist.
	
	Ohne Verschlüsselung:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`./scripts/epic02/create-efs.sh -d \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"` wobei der Name Ihres Amazon-EKS-Cluster s`$CLUSTER_NAME` , ein eindeutiges Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist und die Verschlüsselung im Ruhezustand `-d` deaktiviert.	
Erstellen einer Sicherheitsgruppe.	Erstellen Sie eine Sicherheitsgruppe, damit der Amazon-EKS-Cluster auf das Amazon-EFS-Dateisystem zugreifen kann.	AWS-Systemadministrator
Aktualisieren Sie die eingehende Regel für die Sicherheitsgruppe.	Aktualisieren Sie die Regeln für eingehenden Datenverkehr der Sicherheitsgruppe, um eingehenden Datenverkehr für die folgenden Einstellungen zuzulassen: • TCP-Protokoll – Port 2049 • Quelle – CIDR-Blockbereiche für die privaten Subnetze in der VPC, die den Kubernetes-Cluster enthält	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie für jedes private Subnetz ein Mount-Ziel hinzu.	Erstellen Sie für jedes private Subnetz des Kubernetes-Clusters ein Mountingziel für das Dateisystem und die Sicherheitsgruppe.	AWS-Systemadministrator

Installieren von Amazon-EFS-Komponenten im Kubernetes-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Amazon-EFS-CSI-Treiber bereit.	Stellen Sie den Amazon-EFS-CSI-Treiber im Cluster bereit. Der Treiber stellt Speicher gemäß den persistenten Volume-Ansprüchen bereit, die von Anwendungen erstellt wurden. Führen Sie das `create-k8s-efs-csi-sc.sh` Skript aus, um den Amazon-EFS-CSI-Treiber und die Speicherklasse im Cluster bereitzustellen. `./scripts/epic03/create-k8s-efs-csi-sc.sh` Dieses Skript verwendet das `kubectl` Dienstprogramm . Stellen Sie daher sicher, dass der Kontext konfiguriert wurde und auf den gewünschten Amazon-EKS-Cluster verweist.	Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Speicherklasse bereit.	Stellen Sie die Speicherklasse im Cluster für den Amazon-EFS-Provisioner bereit (efs.csi.aws.com).	Kubernetes-Benutzer mit gewährten Berechtigungen

Installieren der PoC-Anwendung im Kubernetes-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das persistente Volume bereit.	Stellen Sie das persistente Volume bereit und verknüpfen Sie es mit der erstellten Speicherklasse und der ID des Amazon-EFS-Dateisystems. Die Anwendung verwendet das persistente Volume zum Lesen und Schreiben von Inhalten. Sie können eine beliebige Größe für das persistente Volume im Speicherfeld angeben. Kubernetes erfordert dieses Feld, aber da Amazon EFS ein elastisches Dateisystem ist, erzwingt es keine Dateisystemkapazität. Sie können das persistente Volume mit oder ohne Verschlüsselung bereitstellen. (Der Amazon-EFS-CSI-Treiber aktiviert standardmäßig die Verschlüsselung als bewährte Methode.) Führen Sie das `deploy-poc-app.sh` Skript aus, um	Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	das persistente Volume, den persistenten Volume-Anspruch und die beiden Workloads bereitzustellen.
	
	Bei Verschlüsselung während der Übertragung:
	
	`./scripts/epic04/deploy-poc-app.sh \ -t "$EFS_CREATION_TOKEN"`
	
	wobei das eindeutige Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist.
	
	Ohne Verschlüsselung während der Übertragung:
	
	`./scripts/epic04/deploy-poc-app.sh -d \ -t "$EFS_CREATION_TOKEN"`
	
	wobei das eindeutige Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist und die Verschlüsselung während der Übertragung `-d` deaktiviert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den von der Anwendung angeforderten persistenten Volume-Anspruch bereit.	Stellen Sie den von der Anwendung angeforderten persistenten Volume-Anspruch bereit und verknüpfen Sie ihn mit der Speicherklasse . Verwenden Sie denselben Zugriffsmodus wie das persistente Volume, das Sie zuvor erstellt haben. Sie können eine beliebige Größe für den persistenten Volume-Anspruch im Speicherfeld angeben. Kubernetes erfordert dieses Feld, aber da Amazon EFS ein elastisches Dateisyst em ist, erzwingt es keine Dateisystemkapazität.	Kubernetes-Benutzer mit gewährten Berechtigungen
Stellen Sie Workload 1 bereit.	Stellen Sie den Pod bereit, der Workload 1 der Anwendung darstellt. Dieser Workload schreibt Inhalte in die Datei `/data/out1.txt` .	Kubernetes-Benutzer mit gewährten Berechtigungen
Stellen Sie Workload 2 bereit.	Stellen Sie den Pod bereit, der Workload 2 der Anwendung darstellt. Dieser Workload schreibt Inhalte in die Datei `/data/out2.txt` .	Kubernetes-Benutzer mit gewährten Berechtigungen

Überprüfen der Persistenz, Haltbarkeit und Gemeinsamkeit des Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status von `PersistentVolume` .	Geben Sie den folgenden Befehl ein, um den Status der zu überprüfen`PersistentVolume` . `kubectl get pv` Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen.	Kubernetes-Benutzer mit gewährten Berechtigungen
Überprüfen Sie den Status von `PersistentVolumeClaim` .	Geben Sie den folgenden Befehl ein, um den Status der zu überprüfen`PersistentVolumeClaim` . `kubectl -n poc-efs-eks-fargate get pvc` Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen.	Kubernetes-Benutzer mit gewährten Berechtigungen
Überprüfen Sie, ob Workload 1 in das Dateisystem schreiben kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 1 in schreibt`/data/out1.txt` . `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -f /data/out1.txt`	Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Die Ergebnisse ähneln den folgenden:
	`...`
	`Thu Sep  3 15:25:07 UTC 2023 - PoC APP 1`
	`Thu Sep  3 15:25:12 UTC 2023 - PoC APP 1`
	`Thu Sep  3 15:25:17 UTC 2023 - PoC APP 1`
	`...`	

Überprüfen Sie, ob Workload 2 in das Dateisystem schreiben kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 2 in schreibt `/data/out2.txt` .
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -f /data/out2.txt`
	Die Ergebnisse ähneln den folgenden:
	`...`
	`Thu Sep  3 15:26:48 UTC 2023 - PoC APP 2`
	`Thu Sep  3 15:26:53 UTC 2023 - PoC APP 2`
	`Thu Sep  3 15:26:58 UTC 2023 - PoC APP 2`
	`...`
		Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie, ob Workload 1 die von Workload 2 geschriebene Datei lesen kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 1 die von Workload 2 geschriebene `/data/out2.txt` Datei lesen kann.
	`kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -n 3 /data/out2.txt`
	Die Ergebnisse ähneln den folgenden:
	`... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ...`
		Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie, ob Workload 2 die von Workload 1 geschriebene Datei lesen kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 2 die von Workload 1 geschriebene `/data/out1.txt` Datei lesen kann.
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -n 3 /data/out1.txt`
	Die Ergebnisse ähneln den folgenden:
	`... Thu Sep 3 15:29:22 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:27 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:32 UTC 2023 - PoC APP 1 ...`
		Kubernetes-Benutzer mit gewährten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie, ob Dateien aufbewahrt werden, nachdem Sie Anwendungskomponenten entfernt haben.	Als Nächstes verwenden Sie ein Skript, um die Anwendungskomponenten (persistentes Volume, persistenter Volume-Anspruch und Pods) zu entfernen und zu überprüfen, ob die Dateien `/data/out1.txt` und im Dateisystem aufbewahrt `/data/out2.txt` werden. Führen Sie das Skript `validate-efs-content.sh` mit dem folgenden Befehl aus.
	`./scripts/epic05/validate-efs-content.sh \`
	`-t "$EFS_CREATION_TOKEN"`
	wobei das eindeutige Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist.
	Die Ergebnisse ähneln den folgenden:
	`pod/poc-app-validation created`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
		Kubernetes-Benutzer mit gewährten Berechtigungen, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Results from execution of 'find /data' on validation process pod: /data /data/out2.txt /data/out1.txt`	

Überwachen von -Operationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie Anwendung sprotokolle.	Senden Sie im Rahmen eines Vorgangs vom zweiten Tag die Anwendungsprotokolle CloudWatch zur Überwachung an Amazon.	AWS-Systemadministrator, Kubernetes-Benutzer mit gewährten Berechtigungen
Überwachen Sie Amazon-EKS- und Kubernetes-Container mit Container Insights.	Überwachen Sie im Rahmen eines Vorgangs vom zweiten Tag die Systeme Amazon EKS und Kubernetes mithilfe von Amazon CloudWatch Container Insights. Dieses Tool sammelt, aggregiert und fasst Metriken aus containerisierten Anwendungen auf verschiedenen Ebenen und Dimensionen zusammen. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	AWS-Systemadministrator, Kubernetes-Benutzer mit gewährten Berechtigungen
Überwachen Sie Amazon EFS mit CloudWatch.	Überwachen Sie im Rahmen eines Vorgangs vom zweiten Tag die Dateisysteme mit	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon CloudWatch, das Rohdaten von Amazon EFS sammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit vorliegen. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie alle erstellten Ressourcen für das Muster.	Nachdem Sie dieses Muster abgeschlossen haben, bereinigen Sie alle Ressourcen, damit keine AWS-Gebühren anfallen. Führen Sie das `clean-up-resources.sh` Skript aus, um alle Ressourcen zu entfernen, nachdem Sie die Verwendung der PoC-Anwendung abgeschlossen haben. Führen Sie eine der folgenden Optionen aus. Mit Verschlüsselung im Ruhezustand, mit einem KMS-Schlüssel: `./scripts/epic06/clean-up-resources.sh \`	Kubernetes-Benutzer mit gewährten Berechtigungen, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>-c "$CLUSTER_NAME" \
	-t "$EFS_CREATION_TOKEN" \
	-k "$KMS_KEY_ALIAS"</pre>
	wobei `$CLUSTER_NAME` der Name Ihres Amazon-EKS-Clusters`$EFS_CREATION_TOKEN` , das Erstellungstoken für das Dateisystem und der Alias für den KMS-Schlüssel `$KMS_KEY_ALIAS` ist.
	
	Ohne Verschlüsselung im Ruhezustand:
	
	<pre>./scripts/epic06/clean-up-resources.sh \
	-c "$CLUSTER_NAME" \
	-t "$EFS_CREATION_TOKEN"</pre>
	wobei `$CLUSTER_NAME` der Name Ihres Amazon-EKS-Clusters und das Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist.	

Zugehörige Ressourcen

Referenzen

- AWS Fargate für Amazon EKS unterstützt jetzt Amazon EFS (Ankündigung)
- So erfassen Sie Anwendungsprotokolle bei Verwendung von Amazon EKS auf AWS Fargate (Blogbeitrag)
- Verwenden von Container Insights (Amazon- CloudWatch Dokumentation)
- Einrichten von Container Insights in Amazon EKS und Kubernetes (Amazon- CloudWatch Dokumentation)
- Metriken von Amazon EKS und Kubernetes Container Insights (Amazon- CloudWatch Dokumentation)
- Überwachen von Amazon EFS mit Amazon CloudWatch (Amazon-EFS-Dokumentation)

GitHub -Tutorials und -Beispiele

- Statische Bereitstellung
- Verschlüsselung während der Übertragung
- Zugreifen auf das Dateisystem von mehreren Pods aus
- Nutzung von Amazon EFS in StatefulSets
- Mounting von Unterpfaden
- Verwenden von Amazon-EFS-Zugriffspunkten
- Amazon-EKS-Blueprints für Terraform

Erforderliche Tools

- Installieren der AWS CLI Version 2
- Installieren von eksctl
- Installieren von kubectl
- Installieren von jq

Zusätzliche Informationen

Im Folgenden finden Sie eine Beispielausgabe des `kubectl get pv` Befehls .

```
NAME         CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
           STORAGECLASS   REASON   AGE
```

```
poc-app-pv   1Mi        RWX            Retain           Bound    poc-efs-eks-fargate/
poc-app-pvc   efs-sc                   3m56s
```

Im Folgenden finden Sie eine Beispielausgabe des `kubectl -n poc-efs-eks-fargate get pvc` Befehls .

```
NAME          STATUS   VOLUME       CAPACITY   ACCESS MODES   STORAGECLASS   AGE
poc-app-pvc   Bound    poc-app-pv   1Mi        RWX            efs-sc         4m34s
```

Mehr Muster

- Bewerten Sie die Anwendungsbereitschaft für die Migration in die AWS Cloud mithilfe von CAST Highlight
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mit AWS CDK
- Erstellen und pushen Sie Docker-Images mithilfe von GitHub Aktionen und Terraform auf Amazon ECR
- Containerisieren Sie Mainframe-Workloads, die von Clari Age modernisiert wurden
- Erstellen eines benutzerdefinierten Protokollparsers für Amazon ECS mithilfe eines Firelens-Protokollrouters
- Bereitstellen einer CI/CD-Pipeline für Java-Microservices auf Amazon ECS
- Bereitstellen eines Amazon EKS-Clusters aus AWS Cloud9 mithilfe eines EC2-Instance-Profils
- Bereitstellen einer Umgebung für containerisierte Clari Age-Anwendungen mithilfe von Terraform
- Bereitstellen von Vorverarbeitungslogik in einem ML-Modell in einem einzigen Endpunkt mithilfe einer Inferenz-Pipeline in Amazon SageMaker
- Verwalten Sie Blau/Grün-Bereitstellungen von Microservices für mehrere Konten und Regionen mithilfe von AWS-Codeservices und AWS KMS-Schlüsseln für mehrere Regionen
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS
- Überwachen von Amazon ECR-Repositorys auf Platzhalterberechtigungen mit AWS CloudFormation und AWS Config
- Einrichten einer CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere mithilfe von AWS CDK und GitLab
- Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein
- ???
- Einrichten der end-to-end Verschlüsselung für Anwendungen in Amazon EKS mit cert-manager und Let's Encrypt
- Vereinfachen Sie die Bereitstellung von Amazon-EKS-Anwendungen mit mehreren Mandanten mithilfe von Flux

- Strukturieren eines Python-Projekts in hexaffinaler Architektur mit AWS Lambda
- Trainieren und implementieren Sie ein benutzerdefiniertes GPU-unterstütztes ML-Modell auf Amazon SageMaker

Bereitstellung von Inhalten

Themen

- Senden Sie AWS-WAF-Protokolle mithilfe von AWS Firewall Manager und Amazon Data Firehose an Splunk
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Mehr Muster

Senden Sie AWS-WAF-Protokolle mithilfe von AWS Firewall Manager und Amazon Data Firehose an Splunk

Erstellt von Michael Friedenthal (AWS), Aman Kaur Gandhi (AWS) und JJ Johnson (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Bereitstellung von Inhalten; Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Services: AWS Firewall Manager; Amazon Kinesis Data Firehose; AWS WAF		

Übersicht

In der Vergangenheit gab es zwei Möglichkeiten, Daten in Splunk zu verschieben: eine Push- oder eine Pull-Architektur. Eine Pull-Architektur bietet garantierte Lieferdaten durch Wiederholungsversuche, erfordert jedoch spezielle Ressourcen in Splunk, die Daten abfragen. Pull-Architekturen funktionieren aufgrund des Pollings in der Regel nicht in Echtzeit. Eine Push-Architektur hat in der Regel eine geringere Latenz, ist skalierbarer und reduziert die betriebliche Komplexität und die Kosten. Sie garantiert jedoch nicht die Lieferung und erfordert in der Regel Agenten.

Die Splunk-Integration mit Amazon Data Firehose liefert Streaming-Daten in Echtzeit über einen HTTP Event Collector (HEC) an Splunk. Diese Integration bietet die Vorteile von Push- und Pull-Architekturen: Sie garantiert die Datenlieferung durch Wiederholungsversuche, erfolgt nahezu in Echtzeit und zeichnet sich durch geringe Latenz und geringe Komplexität aus. Die HEC sendet Daten schnell und effizient über HTTP oder HTTPS direkt an Splunk. HECs sind tokenbasiert, wodurch die Notwendigkeit entfällt, Anmeldeinformationen in einer Anwendung oder in unterstützenden Dateien fest zu codieren.

In einer AWS Firewall Manager Manager-Richtlinie können Sie die Protokollierung für den gesamten AWS WAF WAF-Web-ACL-Verkehr in all Ihren Konten konfigurieren. Anschließend können Sie einen Firehose-Lieferstream verwenden, um diese Protokolldaten zur Überwachung, Visualisierung und Analyse an Splunk zu senden. Diese Lösung bietet die folgenden Vorteile:

- Zentrale Verwaltung und Protokollierung für den AWS WAF WAF-Web-ACL-Verkehr in all Ihren Konten
- Splunk-Integration mit einem einzigen AWS-Konto
- Skalierbarkeit
- Bereitstellung von Protokolldaten nahezu in Echtzeit
- Kostenoptimierung durch den Einsatz einer serverlosen Lösung, sodass Sie nicht für ungenutzte Ressourcen bezahlen müssen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto, das Teil einer Organisation in AWS Organizations ist.
- Sie benötigen die folgenden Berechtigungen, um die Protokollierung mit Firehose zu aktivieren:
  - `iam:CreateServiceLinkedRole`
  - `firehose:ListDeliveryStreams`
  - `wafv2:PutLoggingConfiguration`
- AWS WAF und seine Web-ACLs müssen konfiguriert sein. Anweisungen finden Sie unter Erste Schritte mit AWS WAF.
- AWS Firewall Manager muss eingerichtet sein. Anweisungen finden Sie unter Voraussetzungen für AWS Firewall Manager.
- Die Firewall Manager Manager-Sicherheitsrichtlinien für AWS WAF müssen konfiguriert sein. Anweisungen finden Sie unter Erste Schritte mit AWS Firewall Manager AWS WAF WAF-Richtlinien.
- Splunk muss mit einem öffentlichen HTTP-Endpunkt eingerichtet werden, der von Firehose erreicht werden kann.

Einschränkungen

- Die AWS-Konten müssen in einer einzigen Organisation in AWS Organizations verwaltet werden.
- Die Web-ACL muss sich in derselben Region wie der Lieferstream befinden. Wenn Sie Protokolle für Amazon erfassen CloudFront, erstellen Sie den Firehose-Lieferstream in der Region USA Ost (Nord-Virginia),`us-east-1`.

- Das Splunk-Add-on für Firehose ist für kostenpflichtige Splunk Cloud-Implementierungen, verteilte Splunk Enterprise-Bereitstellungen und Splunk Enterprise-Implementierungen mit einer einzigen Instanz verfügbar. Dieses Add-on wird für kostenlose Testversionen von Splunk Cloud nicht unterstützt.

Architektur

Zieltechnologie-Stack

- Firewall Manager
- Firehose
- Amazon S3
- AWS WAF
- Splunk

Zielarchitektur

Die folgende Abbildung zeigt, wie Sie mit Firewall Manager alle AWS-WAF-Daten zentral protokollieren und über Kinesis Data Firehose an Splunk senden können.

1. Die AWS WAF WAF-Web-ACLs senden Firewall-Protokolldaten an Firewall Manager.
2. Firewall Manager sendet die Protokolldaten an Firehose.
3. Der Firehose-Lieferstream leitet die Protokolldaten an Splunk und an einen S3-Bucket weiter. Der S3-Bucket dient als Backup im Falle eines Fehlers im Firehose-Lieferstream.

Automatisierung und Skalierung

Diese Lösung ist so konzipiert, dass sie alle AWS WAF WAF-Web-ALCs innerhalb des Unternehmens skaliert und unterstützt. Sie können alle Web-ACLs so konfigurieren, dass sie dieselbe Firehose-Instanz verwenden. Wenn Sie jedoch mehrere Firehose-Instanzen einrichten und verwenden möchten, können Sie dies tun.

Tools

AWS-Services

- AWS Firewall Manager ist ein Sicherheitsmanagement-Service, mit dem Sie Firewall-Regeln für Ihre Konten und Anwendungen in AWS Organizations zentral konfigurieren und verwalten können.
- Amazon Data Firehose unterstützt Sie bei der Bereitstellung von Echtzeit-Streaming-Daten an andere AWS-Services, benutzerdefinierte HTTP-Endpunkte und HTTP-Endpunkte, die von unterstützten Drittanbietern wie Splunk betrieben werden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS WAF ist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere Tools

- Splunk unterstützt Sie bei der Überwachung, Visualisierung und Analyse von Protokolldaten.

Epen

Splunk konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Splunk-App für AWS.	1. Melden Sie sich bei Ihrem Splunk Heavy Forwarder an. Die Standard-URL ist. `http://<IP address>:8000` 2. Wählen Sie in der linken Navigationsleiste neben Apps die Zahnradtaste aus. 3. Wähle Weitere Apps durchsuchen. 4. Suchen Sie nach aws. 5. Wählen Sie für Splunk App for AWS Install. 6. Geben Sie Ihre Splunk.com-Anmeldeinformationen	Sicherheitsadministrator, Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein, akzeptieren Sie die Allgemeinen Geschäfts bedingungen und wählen Sie dann Anmelden und Installieren. 7. Wählen Sie Erledigt aus.	
Installieren Sie das Add-on für AWS WAF.	Wiederholen Sie die vorherige n Anweisungen, um das AWS Web Application Firewall Add-on für Splunk zu installieren.	Sicherheitsadministrator, Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie das Splunk-Add-on für Firehose.	1. Installieren und konfiguri eren Sie das Splunk-Add-on für Firehose. Im Rahmen der Installation und Konfiguration richten Sie, falls dies für Ihre Splunk-Plattform erforderl ich ist, einen HTTP Event Collector ein und bereiten die Infrastruktur vor, um die Protokolldaten an Ihre Indexer zu senden. Sehen Sie sich die Anweisung en an, die Ihrer Splunk-Be reitstellung entsprechen: • Bereitstellung von Splunk Cloud (Splunk-D okumentation) • Verteilte Splunk Enterpris e-Bereitstellung (Splunk-Dokumentation) • Bereitstellung von Splunk Enterprise in einer einzigen Instanz (Splunk-Dokumentation) Wichtig: Beenden Sie diesen Vorgang, nachdem Sie das Splunk-Add-on installiert und konfiguriert haben. Fahren Sie nicht mit den Anweisungen zur Konfiguration von Firehose	Sicherheitsadministrator, Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für das Senden von Daten an die Splunk-Plattform fort. 2. Notieren Sie sich das HTTP-Event-Collector-Token und den HTTP-Endpunkt. Sie benötigen diesen Wert später, wenn Sie den Lieferstream konfigurieren.	

Erstellen Sie den Firehose-Lieferstream

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Firehose Zugriff auf ein Splunk-Ziel.	Konfigurieren Sie die Zugriffsrichtlinie, die es Firehose ermöglicht, auf ein Splunk-Ziel zuzugreifen und die Protokolldaten in einem S3-Bucket zu sichern. Weitere Informationen finden Sie unter Firehose Zugriff auf ein Splunk-Ziel gewähren.	Sicherheitsadministrator
Erstellen Sie einen Firehose-Lieferstream.	Erstellen Sie in demselben Konto, in dem Sie die Web-ACLs für AWS WAF verwalten, einen Lieferstream in Firehose. Sie müssen eine IAM-Rolle besitzen, wenn Sie einen Bereitstellungsdatenstrom erstellen. Firehose nimmt diese IAM-Rolle an und erhält Zugriff auf den angegebenen S3-Bucket.	Sicherheitsadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie unter Einen Lieferstream erstellen. Beachten Sie Folgendes: • Der Name des Lieferdatenstroms muss mit beginnen `aws-waf-logs-` . • Wählen Sie als Quelle Direct PUT aus. • Wählen Sie für den S3-Backup-Modus Alle Ereignisse sichern und wählen Sie dann einen vorhandenen Bucket aus oder erstellen Sie einen neuen. • Folgen Sie für das Ziel den Anweisungen unter Wählen Sie Splunk für Ihr Ziel in der Firehose-Dokumentation. Informationen zu den Werten für Splunk-Endpunkte und Endpunkttypen finden Sie unter Amazon Data Firehose konfigurieren in der Splunk-Dokumentation. Wiederholen Sie diesen Vorgang für jedes Token, das Sie im HTTP-Event-Collector konfiguriert haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Lieferstream.	Testen Sie den Lieferstr eam, um sicherzustellen, dass er richtig konfiguriert ist. Anweisungen finden Sie unter Testen mit Splunk als Ziel in der Firehose-Dokumentation.	Sicherheitsadministrator

Konfigurieren Sie den Firewall Manager für die Protokollierung von Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Firewall Manager Manager-Richtlinien.	Die Firewall Manager Manager-Richtlinien müssen so konfiguriert sein, dass sie die Protokollierung aktiviere n und Protokolle an den richtigen Firehose-Lieferstr eam weiterleiten. Weitere Informationen und Anweisung en finden Sie unter Konfigura tion der Protokollierung für eine AWS-WAF-Richtlinie.	Sicherheitsadministrator

Zugehörige Ressourcen

AWS-Ressourcen

- Protokollierung des Web-ACL-Datenverkehrs (AWS WAF WAF-Dokumentation)
- Konfiguration der Protokollierung für eine AWS-WAF-Richtlinie (AWS WAF WAF-Dokumentation)
- Tutorial: Mit Amazon Data Firehose VPC-Flow-Logs an Splunk senden (Firehose-Dokumentation)
- Wie übertrage ich VPC-Flow-Logs mit Amazon Data Firehose an Splunk? (AWS-Wissenszentrum)
- Optimieren Sie die Datenaufnahme in Splunk mithilfe von Amazon Data Firehose (AWS-Blogbeitrag)

Splunk-Dokumentation

- Splunk-Add-on für Amazon Data Firehose

Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront

Erstellt von Angel Emmanuel Hernandez Cebrian

Umgebung: PoC oder Pilotprojekt	Technologien: Bereitstellung von Inhalten; Netzwerke; Sicherheit, Identität, Compliance; Serverlos; Web- und mobile Apps	AWS-Services: Amazon CloudFront; Elastic Load Balancing (ELB); AWS Lambda

Übersicht

Wenn Sie statische Inhalte bereitstellen, die auf Amazon Web Services (AWS) gehostet werden, wird empfohlen, einen Amazon Simple Storage Service (S3) -Bucket als Quelle zu verwenden und Amazon für die Verteilung der Inhalte CloudFront zu verwenden. Diese Lösung bietet zwei Hauptvorteile: die Bequemlichkeit, statische Inhalte an Edge-Standorten zwischenzuspeichern, und die Möglichkeit, Web-Zugriffskontrolllisten (Web-ACLs) für die CloudFront Verteilung zu definieren, wodurch Sie Anfragen zu den Inhalten mit minimalem Konfigurations- und Verwaltungsaufwand sichern können.

Der empfohlene Standardansatz weist jedoch häufig eine architektonische Einschränkung auf. In einigen Umgebungen möchten Sie, dass virtuelle Firewall-Appliances, die in einer Virtual Private Cloud (VPC) bereitgestellt werden, den gesamten Inhalt überprüfen, einschließlich statischer Inhalte. Der Standardansatz leitet den Datenverkehr nicht zur Inspektion durch die VPC. Dieses Muster bietet eine alternative architektonische Lösung. Sie verwenden immer noch eine CloudFront Distribution, um statische Inhalte in einem S3-Bucket bereitzustellen, aber der Datenverkehr wird mithilfe eines Application Load Balancer über die VPC geleitet. Eine AWS-Lambda-Funktion ruft dann den Inhalt aus dem S3-Bucket ab und gibt ihn zurück.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Statischer Website-Inhalt, der in einem S3-Bucket gehostet wird.

Einschränkungen

- Die Ressourcen in diesem Muster müssen sich in einer einzigen AWS-Region befinden, sie können jedoch in verschiedenen AWS-Konten bereitgestellt werden.
- Es gelten Grenzwerte für die maximale Anfrage- und Antwortgröße, die die Lambda-Funktion empfangen bzw. senden kann. Weitere Informationen finden Sie unter Grenzwerte in Lambda-Funktionen als Ziele (Elastic Load Balancing Balancing-Dokumentation).
- Bei der Verwendung dieses Ansatzes ist es wichtig, ein ausgewogenes Verhältnis zwischen Leistung, Skalierbarkeit, Sicherheit und Kosteneffektivität zu finden. Trotz der hohen Skalierbarkeit von Lambda werden einige Anfragen gedrosselt, wenn die Anzahl gleichzeitiger Lambda-Aufrufe das maximale Kontingent überschreitet. Weitere Informationen finden Sie unter Lambda-Kontingente (Lambda-Dokumentation). Bei der Verwendung von Lambda müssen Sie auch die Preisgestaltung berücksichtigen. Um Lambda-Aufrufe zu minimieren, stellen Sie sicher, dass Sie den Cache für die Distribution richtig definieren. CloudFront Weitere Informationen finden Sie unter Optimierung von Caching und Verfügbarkeit (Dokumentation). CloudFront

Architektur

Zieltechnologie-Stack

- CloudFront
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer
- Lambda
- Amazon S3

Zielarchitektur

Die folgende Abbildung zeigt die vorgeschlagene Architektur, wenn Sie statische Inhalte aus einem S3-Bucket über eine VPC bereitstellen müssen. CloudFront

1. Der Client fordert die URL der CloudFront Verteilung an, um eine bestimmte Website-Datei im S3-Bucket abzurufen.

2. CloudFront sendet die Anfrage an AWS WAF. AWS WAF filtert die Anfrage mithilfe der Web-ACLs, die auf die CloudFront Verteilung angewendet wurden. Wenn sich herausstellt, dass die Anfrage gültig ist, wird der Ablauf fortgesetzt. Wenn sich herausstellt, dass die Anfrage ungültig ist, erhält der Client einen 403-Fehler.
3. CloudFront überprüft seinen internen Cache. Wenn es einen gültigen Schlüssel gibt, der der eingehenden Anfrage entspricht, wird der zugehörige Wert als Antwort an den Client zurückgesendet. Ist dies nicht der Fall, wird der Datenfluss fortgesetzt.
4. CloudFront leitet die Anfrage an die URL des angegebenen Application Load Balancer weiter.
5. Der Application Load Balancer hat einen Listener, der auf einer Lambda-Funktion einer Zielgruppe zugeordnet ist. Der Application Load Balancer ruft die Lambda-Funktion auf.
6. Die Lambda-Funktion stellt eine Verbindung zum S3-Bucket her, führt eine `GetObject` Operation darauf aus und gibt den Inhalt als Antwort zurück.

Automatisierung und Skalierung

Um die Bereitstellung statischer Inhalte mit diesem Ansatz zu automatisieren, erstellen Sie CI/CD-Pipelines zur Aktualisierung der Amazon S3 S3-Buckets, die Websites hosten.

Die Lambda-Funktion skaliert automatisch, um die gleichzeitigen Anfragen innerhalb der Kontingente und Einschränkungen des Dienstes zu verarbeiten. Weitere Informationen finden Sie unter Lambda-Funktionsskalierung und Lambda-Kontingente (Lambda-Dokumentation). Für die anderen AWS-Services und -Funktionen wie CloudFront den Application Load Balancer skaliert AWS diese automatisch.

Tools

- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. In diesem Muster verwenden Sie einen Application Load Balancer, der über Elastic Load Balancing bereitgestellt wird, um den Datenverkehr an die Lambda-Funktion weiterzuleiten.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Wird verwendet CloudFront , um statische Inhalte von Amazon S3 über eine VPC bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie eine VPC zum Hosten der in diesem Muster bereitgestellten Ressourcen, z. B. des Application Load Balancer und der Lambda-Funktion. Anweisungen finden Sie unter Erstellen einer VPC (Amazon VPC-Dokumentation).	Cloud-Architekt
Erstellen Sie eine AWS WAF WAF-Web-ACL.	Erstellen Sie eine AWS WAF WAF-Web-ACL. Später in diesem Muster wenden Sie diese Web-ACL auf die CloudFront Distribution an. Anweisungen finden Sie unter Erstellen einer Web-ACL (AWS-WAF-Dokumentation).	Cloud-Architekt
So erstellen Sie die Lambda-Funktion:	Erstellen Sie die Lambda-Funktion, die den im S3-Bucket gehosteten statischen Inhalt als Website bereitstellt. Verwenden Sie den Code, der im Abschnitt Zusätzliche Informationen dieses Musters	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereitgestellt wird. Passen Sie den Code an, um Ihren Ziel-S3-Bucket zu identifizieren.	
Laden Sie die Lambda-Funktion hoch.	Geben Sie den folgenden Befehl ein, um den Lambda-Funktionscode in ein ZIP-Dateiarchiv in Lambda hochzuladen. `aws lambda update-function-code \ --function-name \ --zip-file fileb://lambda-alb-s3-website.zip`	Allgemeines AWS
Erstellen Sie einen Application Load Balancer.	Erstellen Sie einen mit dem Internet verbundenen Application Load Balancer, der auf die Lambda-Funktion verweist. Anweisungen finden Sie unter Eine Zielgruppe für die Lambda-Funktion erstellen (Elastic Load Balancing Balancing-Dokumentation). Für eine Hochverfügbarkeitskonfiguration erstellen Sie den Application Load Balancer und fügen ihn privaten Subnetzen in verschiedenen Availability Zones hinzu.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFront Distribution.	Erstellen Sie eine CloudFront Verteilung, die auf den von Ihnen erstellten Application Load Balancer verweist. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFront Konsole unter https://console.aws.amazon.com/cloudfront/v3/home. 2. Wählen Sie Create Distribution. 3. Wählen Sie auf der ersten Seite des Assistenten Create Distribution Wizard im Abschnitt Web die Option Get Started. 4. Geben Sie die Einstellungen für Ihre Distribution an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren einer Verteilung angeben. Beachten Sie Folgendes: a. Legen Sie den Application Load Balancer als Ursprung fest. b. Wählen Sie in den Verteilungseinstellungen vorhandene Web-ACLs aus, die Sie über AWS WAF	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	anwenden möchten. Weitere Informationen finden Sie unter AWS WAF Web ACL. 5. Speichern Sie Ihre Änderungen. 6. Nachdem Sie Ihre Distribution CloudFront erstellt haben, ändert sich der Wert der Status-Spalte für Ihre Distribution von InProgress zu Deployed. Wenn Sie die Verteilung aktivieren, kann sie sofort Anfragen verarbeiten, nachdem der Status auf Deployed (Bereitgestellt) gewechselt hat.	

Zugehörige Ressourcen

AWS-Dokumentation

- Optimierung von Caching und Verfügbarkeit (CloudFront Dokumentation)
- Lambda-Funktionen als Ziele (Dokumentation zu Elastic Load Balancing)
- Lambda-Kontingente (Lambda-Dokumentation)

AWS-Servicewebsites

- Application Load Balancer
- Lambda
- CloudFront
- Amazon S3

- AWS WAF
- Amazon VPC

Zusätzliche Informationen

Code

Die folgende Lambda-Beispielfunktion ist in Node.js geschrieben. Diese Lambda-Funktion fungiert als Webserver, der eine `GetObject` Operation für einen S3-Bucket ausführt, der die Website-Ressourcen enthält.

```
/**

 * This is an AWS Lambda function created for demonstration purposes.

 * It retrieves static assets from a defined Amazon S3 bucket.

 * To make the content available through a URL, use an Application Load Balancer with a
 Lambda integration.
 *
 * Set the S3_BUCKET environment variable in the Lambda function definition.
 */

var AWS = require('aws-sdk');

exports.handler = function(event, context, callback) {

    var bucket = process.env.S3_BUCKET;
    var key = event.path.replace('/', '');

    if (key == '') {
        key = 'index.html';
    }

    // Fetch from S3
    var s3 = new AWS.S3();
    return s3.getObject({Bucket: bucket, Key: key},
       function(err, data) {

           if (err) {
               return err;
           }
```

```
            var isBase64Encoded = false;
            var encoding = 'utf8';

            if (data.ContentType.indexOf('image/') > -1) {
                isBase64Encoded = true;
                encoding = 'base64'
            }

            var resp = {
                statusCode: 200,
                headers: {
                    'Content-Type': data.ContentType,
                },
                body: new Buffer(data.Body).toString(encoding),
                isBase64Encoded: isBase64Encoded
            };

            callback(null, resp);
        }
    );
};
```

Mehr Muster

- Suchen Sie in einer CloudFront Amazon-Distribution nach Zugriffsprotokollierung, HTTPS- und TLS-Version
- Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu
- ???
- Stellen Sie die Lösung Security Automations für AWS WAF mithilfe von Terraform bereit
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen

Kostenmanagement

Themen

Erstellen detaillierter Kosten- und Nutzungsberichte für AWS Glue-Aufträge mithilfe von AWS Cost Explorer

Erstellt von Parijat Bhide (AWS) und Boll Raj Jayarajan (AWS)

Umgebung: Produktion	Technologien: Kostenmanagement; Analysen	AWS-Services: AWS Billing and Cost Management; AWS Glue

Übersicht

Dieses Muster zeigt, wie Sie die Nutzungskosten von AWS Glue-Datenintegrationsaufträgen verfolgen können, indem Sie benutzerdefinierte Kostenzuordnungs-Tags konfigurieren. Sie können diese Tags verwenden, um detaillierte Kosten- und Nutzungsberichte in AWS Cost Explorer für Aufträge über mehrere Dimensionen hinweg zu erstellen. Sie können beispielsweise die Nutzungskosten auf Team-, Projekt- oder Kostenstellenebene verfolgen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein oder mehrere AWS Glue-Aufträge, für die benutzerdefinierte Tags aktiviert sind

Architektur

Zieltechnologie-Stack

- AWS Glue
- AWS Cost Explorer

Das folgende Diagramm zeigt, wie Sie Tags anwenden können, um die Nutzungskosten für AWS Glue-Aufträge zu verfolgen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Dateningenieur oder AWS-Administrator erstellt benutzerdefinierte Kostenzuordnungs-Tags für die AWS Glue-Aufträge.
2. Ein AWS-Administrator aktiviert die Tags.
3. Die Tags melden Metadaten an AWS Cost Explorer .

Tools

- AWS Glue ist ein vollständig verwalteter ETL-Service (Extract, Transform, Load). Es hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Cost Explorer hilft Ihnen, Ihre AWS-Kosten und -Nutzung anzuzeigen und zu analysieren.

Polen

Erstellen und Aktivieren von Tags für Ihre AWS Glue-Aufträge

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerdefinierte Kostenzuordnungs-Tags für Ihre AWS Glue-Aufträge.	So fügen Sie einem vorhandenen AWS Glue-Auftrag Tags hinzu 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Glue-Konsole . 2. Wählen Sie im linken Navigationsbereich unter ETL die Option Aufträge aus. 3. Wählen Sie im Abschnitt Ihre Aufträge den Namen des Auftrags aus, den Sie markieren.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie die Registerkarte Job details (Auftragsdetails) aus. Erweitern Sie dann den Abschnitt Erweiterte Eigenschaften. 5. Wählen Sie für Tags die Option Neues Tag hinzufügen aus. 6. Geben Sie für Schlüssel einen Namen für Ihr Tag ein. 7. (Optional) Geben Sie unter Wert einen Wert ein, der dem Schlüssel zugeordnet werden soll. 8. (Optional) Wiederholen Sie die Schritte 5-7 für jedes Tag, das Sie für den Auftrag erstellen möchten. 9. Wählen Sie Speichern. So fügen Sie einem neuen AWS Glue-Auftrag Tags hinzu 1. Erstellen Sie einen neuen AWS Glue-Auftrag basierend auf Ihren Anwendungsfallanforderungen. Anweisungen finden Sie unter Arbeiten mit Aufträgen in der AWS Glue-Konsole im AWS Glue-Entwicklerhandbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wenn Sie die Einstellungen für Auftragsdetails konfigurieren, folgen Sie den Schritten 4-9 des Abschnitts So fügen Sie Tags zu einem vorhandenen AWS Glue-Auftrag dieser Aufgabe hinzu. Hinweis: Weitere Informationen finden Sie unter AWS-Tags in AWS Glue im AWS Glue-Entwicklerhandbuch.	
Aktivieren Sie die benutzerdefinierten Kostenzuordnungs-Tags.	Folgen Sie den Anweisungen unter Aktivieren benutzerdefinierter Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.	AWS-Administrator

Erstellen von Kosten- und Nutzungsberichten für Ihre AWS Glue-Aufträge

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Kosten- und Nutzungsberichte für Ihre AWS Glue-Aufträge mithilfe von Tag-Filtern in AWS Cost Explorer .	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-Kostenmanagementkonsole . 2. Wählen Sie im linken Navigationsbereich Berichte aus. 3. Wählen Sie Neuen Bericht erstellen aus.	Allgemeines AWS, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie unter Berichtstyp auswählen die Option Kosten und Nutzung aus (empfohlen). Wählen Sie dann Bericht erstellen aus. 5. Wählen Sie für Filter die Option Service aus. Das Dropdown-Menü Service wird angezeigt. 6. Aktivieren Sie die Kontrollkästchen neben Glue . Wählen Sie dann Filter anwenden aus. 7. Wählen Sie fürFilters die Option Tag aus. Das Dropdown-Menü Tag wird angezeigt. 8. Wählen Sie Team . Aktivieren Sie dann die Kontrollkästchen neben den Teams, denen Sie Tags zugewiesen haben. Schließen Sie alle Teams aus, denen Sie keine Tags zugewiesen haben. Wählen Sie dann Filter anwenden aus. 9. Wählen Sie oben im Diagramm Tag aus. Wählen Sie dann die Tags für die AWS Glue-Aufträge aus, für die Sie einen Bericht erstellen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Wählen Sie oben im Diagramm die Dropdownliste Letzte 3 Monate und wählen Sie den Zeitrahmen aus, den der Bericht abdecken soll. Wählen Sie dann die Dropdownliste Monatlich und wählen Sie aus, wie die Einzelposten im Bericht basierend auf dem Zeitrahmen aggregiert werden sollen. 11. Wählen Sie Save as (Speichern unter) aus. Geben Sie dann einen Titel für Ihren Bericht ein. 12. Wählen Sie Bericht speichern aus. Weitere Informationen finden Sie unter Erkunden Ihrer Daten mit Cost Explorer im AWS-Kostenmanagement-Benutzerhandbuch.	

Erstellen detaillierter Kosten- und Nutzungsberichte für Amazon EMR-Cluster mithilfe von AWS Cost Explorer

Erstellt von Parijat Bhide (AWS) und Boll Raj Jayarajan (AWS)

Umgebung: Produktion	Technologien: Kostenmanagement; Analytik; Big Data	AWS-Services: AWS Billing and Cost Management; Amazon EMR

Übersicht

Dieses Muster zeigt, wie Sie die Nutzungskosten von Amazon-EMR-Clustern verfolgen können, indem Sie benutzerdefinierte Kostenzuordnungs-Tags konfigurieren. Sie können diese Tags verwenden, um detaillierte Kosten- und Nutzungsberichte in AWS Cost Explorer für Cluster über mehrere Dimensionen hinweg zu erstellen. Sie können beispielsweise die Nutzungskosten auf Team-, Projekt- oder Kostenstellenebene verfolgen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein oder mehrere EMR-Cluster, für die benutzerdefinierte Tags aktiviert sind

Architektur

Zieltechnologie-Stack

- Amazon EMR
- AWS Cost Explorer

Zielarchitektur

Das folgende Diagramm zeigt, wie Sie Tags anwenden können, um die Nutzungskosten für bestimmte Amazon-EMR-Cluster zu verfolgen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Dateningenieur oder AWS-Administrator erstellt benutzerdefinierte Kostenzuordnungs-Tags für die Amazon EMR-Cluster.
2. Ein AWS-Administrator aktiviert die Tags.
3. Die Tags melden Metadaten an AWS Cost Explorer .

Tools

Tools

- Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks in AWS vereinfacht, um große Datenmengen zu verarbeiten und zu analysieren.
- AWS Cost Explorer hilft Ihnen, Ihre AWS-Kosten und -Nutzung anzuzeigen und zu analysieren.

Polen

Erstellen und Aktivieren von Tags für Ihre Amazon-EMR-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerd efinierte Kostenzuordnungs-Tags für Ihre Amazon-EMR-Cluster.	So fügen Sie einem vorhandenen Amazon-EMR-Cluster Tags hinzu Folgen Sie den Anweisungen unter Hinzufügen von Tags zu einem vorhandenen Cluster im Amazon-EMR-Verwalt ungshandbuch. So fügen Sie einem neuen Amazon-EMR-Cluster Tags hinzu	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Folgen Sie den Anweisungen unter Hinzufügen von Tags zu einem neuen Cluster im Verwaltungshandbuch für Amazon EMR. Weitere Informationen zum Einrichten eines Amazon-EMR-Clusters finden Sie unter Cluster planen und konfigurieren im Verwaltungshandbuch für Amazon EMR.	
Aktivieren Sie die benutzerdefinierten Kostenzuordnungs-Tags.	Folgen Sie den Anweisungen unter Aktivieren benutzerdefinierter Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.	AWS-Administrator

Erstellen von Kosten- und Nutzungsberichten für Ihre Amazon-EMR-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Kosten- und Nutzungsberichte für Ihre Amazon EMR-Cluster mithilfe von Tag-Filtern in AWS Cost Explorer .	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-Kostenmanagementkonsole . 2. Wählen Sie im linken Navigationsbereich Berichte aus. 3. Wählen Sie Neuen Bericht erstellen aus.	Allgemeines AWS, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie unter Berichtstyp auswählen die Option Kosten und Nutzung aus (empfohlen). Wählen Sie dann Bericht erstellen aus. 5. Wählen Sie für Filter die Option Service aus. Das Dropdown-Menü Service wird angezeigt. 6. Aktivieren Sie die Kontrollkästchen neben EMR (Elastic MapReduce) und EC2-Instances (Elastic Compute Cloud – Compute). Wählen Sie dann Filter anwenden aus. 7. Wählen Sie für Filter die Option Tag aus. Das Dropdown-Menü Tag wird angezeigt. 8. Wählen Sie Team aus. Aktivieren Sie dann die Kontrollkästchen neben den Teams, denen Sie Tags zugewiesen haben. Schließen Sie alle Teams aus, denen Sie keine Tags zugewiesen haben. Wählen Sie dann Filter anwenden aus. 9. Wählen Sie oben im Diagramm Tag aus. Wählen Sie dann die Tags für die Amazon-EMR-Cluster aus,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für die Sie einen Bericht erstellen möchten. 10. Wählen Sie oben im Diagramm die Dropdownliste Letzte 3 Monate und wählen Sie den Zeitrahmen aus, den der Bericht abdecken soll. Wählen Sie dann die Dropdownliste Monatlich und wählen Sie aus, wie die Einzelposten im Bericht basierend auf dem Zeitrahmen aggregiert werden sollen. 11. Wählen Sie Save as (Speichern unter) aus. Geben Sie dann einen Titel für Ihren Bericht ein. 12. Wählen Sie Bericht speichern aus. Weitere Informationen finden Sie unter Erkunden Ihrer Daten mit Cost Explorer im AWS-Kostenmanagement-Benutzerhandbuch.	

Mehr Muster

- Automatisieren der Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- ???
- Erstellen detaillierter Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora
- Löschen ungenutzter Amazon Elastic Block Store (Amazon EBS)-Volumes mithilfe von AWS Config und AWS Systems Manager
- Schätzen der Speicherkosten für eine Amazon-DynamoDB-Tabelle
- Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität

Data Lakes

Themen

Automatisieren Sie die Datenaufnahme aus AWS Data Exchange in Amazon S3

Erstellt von Adnan Alvee (AWS) und Manikanta Gona (AWS)

Technologien: Analytik; Datenseen	Umgebung: Produktion	AWS-Dienste: Amazon S3; Amazon CloudWatch; AWS Lambda; Amazon SNS

Übersicht

Dieses Muster stellt eine CloudFormation AWS-Vorlage bereit, mit der Sie Daten aus AWS Data Exchange automatisch in Ihren Data Lake in Amazon Simple Storage Service (Amazon S3) aufnehmen können.

AWS Data Exchange ist ein Service, der den sicheren Austausch dateibasierter Datensätze in der AWS-Cloud erleichtert. AWS Data Exchange Exchange-Datensätze basieren auf Abonnements. Als Abonnent können Sie auch auf Änderungen von Datensätzen zugreifen, wenn Anbieter neue Daten veröffentlichen.

Die CloudFormation AWS-Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS-Lambda-Funktion. Das Ereignis sucht nach Aktualisierungen des Datensatzes, den Sie abonniert haben. Wenn es ein Update gibt, CloudWatch initiiert eine Lambda-Funktion, die die Daten in den von Ihnen angegebenen S3-Bucket kopiert. Wenn die Daten erfolgreich kopiert wurden, sendet Lambda Ihnen eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Abonnement eines Datensatzes in AWS Data Exchange

Einschränkungen

- Die CloudFormation AWS-Vorlage muss für jeden abonnierten Datensatz in AWS Data Exchange separat bereitgestellt werden.

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon S3
- AWS Data Exchange
- Amazon CloudWatch
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation AWS-Vorlage mehrfach für die Datensätze verwenden, die Sie in den Data Lake aufnehmen möchten.

Tools

- AWS Data Exchange — Ein Service, der es AWS-Kunden leicht macht, dateibasierte Datensätze in der AWS-Cloud sicher auszutauschen. Als Abonnent können Sie Hunderte von Produkten qualifizierter Datenanbieter finden und abonnieren. Anschließend können Sie den Datensatz schnell herunterladen oder nach Amazon S3 kopieren, um ihn für eine Vielzahl von AWS-Analyse- und Machine-Learning-Services zu verwenden. Jeder mit einem AWS-Konto kann ein AWS Data Exchange-Abonnent sein.
- AWS Lambda — Ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die Rechenzeit, die Sie verbrauchen. Es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird. Mit AWS Lambda können Sie Code für praktisch jede Art von Anwendung oder Backend-Service ohne Verwaltungsaufwand ausführen. AWS Lambda führt Ihren Code auf einer

hochverfügbaren Recheninfrastruktur aus und verwaltet alle Rechenressourcen, einschließlich Server- und Betriebssystemwartung, Kapazitätsbereitstellung und automatische Skalierung, Codeüberwachung und Protokollierung.

- Amazon S3 — Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon CloudWatch Events — Liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben. Mithilfe einfacher Regeln, die Sie schnell einrichten können, können Sie Ereignisse zuordnen und sie an eine oder mehrere Zielfunktionen oder Streams weiterleiten. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten. Es reagiert auf diese betrieblichen Änderungen und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst. Sie können CloudWatch Ereignisse auch verwenden, um mithilfe von Cron - oder Rate-Ausdrücken automatisierte Aktionen zu planen, die zu bestimmten Zeiten von selbst ausgelöst werden.
- Amazon SNS — Ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen. Amazon SNS bietet Themen (Kommunikationskanäle) für Push-basiertes Messaging mit hohem Durchsatz. many-to-many Mithilfe von Amazon SNS SNS-Themen können Herausgeber Nachrichten zur parallel Verarbeitung an eine große Anzahl von Abonnenten verteilen, einschließlich Amazon Simple Queue Service (Amazon SQS) -Warteschlangen, AWS Lambda Lambda-Funktionen und HTTP/S-Webhooks. Sie können Amazon SNS auch verwenden, um Benachrichtigungen per Push, SMS und E-Mail an Endbenutzer zu senden.

Epen

Abonnieren Sie einen Datensatz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie einen Datensatz.	Abonnieren Sie in der AWS Data Exchange Exchange-Konsole einen Datensatz . Anweisungen finden Sie unter dem Link im Abschnitt „Verwandte Ressourcen“.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich die Attribute des Datensatzes.	Notieren Sie sich die AWS-Region, ID und Revision-ID für den Datensatz. Sie benötigen dies für die CloudFormation AWS-Vorlage im nächsten Schritt.	Allgemeines AWS

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket und einen Ordner.	Wenn Sie bereits über einen Data Lake in Amazon S3 verfügen, erstellen Sie einen Ordner zum Speichern der Daten, die aus AWS Data Exchange aufgenommen werden sollen. Wenn Sie die Vorlage zu Testzwecken bereitstellen, erstellen Sie einen neuen S3-Bucket und notieren Sie sich den Bucket-Namen und das Ordnerpräfix für den nächsten Schritt.	Allgemeines AWS
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie die CloudFormation AWS-Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Konfigurieren Sie die folgenden Parameter so, dass sie Ihren AWS-Konto-, Datensatz- und S3-Bucket-Einstellungen entsprechen: AWS-	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dataset-Region, Datensatz -ID, Revision-ID, S3-Bucket -Name (z. B. DOC-EXAMP LE-BUCKET), Ordnerprä fix (zum Beispiel myfolder/) und E-Mail für SNS-Benac hrichtigung. Sie können den Parameter Dataset Name auf einen beliebigen Namen setzen. Wenn Sie die Vorlage bereitstellen, führt sie eine Lambda-Funktion aus, um automatisch den ersten im Datensatz verfügbaren Datensatz aufzunehmen. Die nachfolgende Aufnahme erfolgt dann automatisch, sobald neue Daten in den Datensatz aufgenommen werden.	

Zugehörige Ressourcen

- Abonnieren von Datenprodukten auf AWS Data Exchange (AWS Data Exchange Exchange-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen einer Datenpipeline zur Aufnahme, Transformation und Analyse von Google Analytics-Daten mit dem AWS DataOps Development Kit

Erstellt von Anton Kukushkin (AWS) und Rudy Puig (AWS)

Code-Repository: AWS DDK-Beispiele – Analysieren von Google Analytics-Daten mit Amazon AppFlow, Amazon Athena und AWS DataOps Development Kit	Umgebung: PoC oder Pilotprojekt	Technologien: Data Lakes; Analytik DevOps; Infrastruktur
Workload: Open-Source	AWS-Services: Amazon AppFlow; Amazon Athena ; AWS CDK; AWS Lambda ; Amazon S3	

Übersicht

Dieses Muster beschreibt, wie Sie eine Datenpipeline erstellen, um Google Analytics-Daten mithilfe des AWS DataOps Development Kit (DDK) und anderer AWS-Services aufzunehmen, zu transformieren und zu analysieren. Das AWS DDK ist ein Open-Source-Entwicklungs-Framework, mit dem Sie Datenworkflows und eine moderne Datenarchitektur in AWS erstellen können. Eines der Hauptziele des AWS DDK besteht darin, Ihnen Zeit und Mühe zu sparen, die in der Regel für arbeitsintensive Datenpipeline-Aufgaben aufgewendet werden, z. B. für die Orchestrierung von Pipelines, den Aufbau der Infrastruktur und die Erstellung der DevOps hinter dieser Infrastruktur. Sie können diese arbeitsintensiven Aufgaben auf AWS DDK auslagern, sodass Sie sich auf das Schreiben von Code und anderen wichtigen Aktivitäten konzentrieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Ein konfigurierter Amazon AppFlow -Konnektor für Google Analytics
- Python und pip (Paketmanager von Python)
- Git, installiert und konfiguriert
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- AWS Cloud Development Kit (AWS CDK), installiert

Produktversionen

- Python 3.7 oder höher
- pip 9.0.3 oder höher

Architektur

Technologie-Stack

- Amazon AppFlow
- Amazon Athena
- Amazon CloudWatch
- Amazon EventBridge
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Queue Service (Amazon SQS)
- AWS DataOps Development Kit (DDK)
- AWS Lambda

Zielarchitektur

Das folgende Diagramm zeigt den ereignisgesteuerten Prozess, der Google Analytics-Daten aufnimmt, transformiert und analysiert.

Das Diagramm zeigt den folgenden Workflow:

1. Eine von Amazon CloudWatch geplante Ereignisregel ruft Amazon auf AppFlow.

2. Amazon AppFlow nimmt Google Analytics-Daten in einen S3-Bucket auf.
3. Nachdem die Daten vom S3-Bucket erfasst wurden, EventBridge werden Ereignisbenachrichtigungen in generiert, von einer CloudWatch Ereignisregel erfasst und dann in eine Amazon SQS-Warteschlange gestellt.
4. Eine Lambda-Funktion verbraucht Ereignisse aus der Amazon SQS-Warteschlange, liest die jeweiligen S3-Objekte, wandelt die Objekte in das Apache Parquet-Format um, schreibt die transformierten Objekte in den S3-Bucket und erstellt oder aktualisiert dann die Tabellendefinition des AWS Glue Data Catalog.
5. Eine Athena-Abfrage wird für die Tabelle ausgeführt.

Tools

AWS-Tools

- Amazon AppFlow ist ein vollständig verwalteter Integrationsservice, mit dem Sie Daten sicher zwischen Software-as-a-Service (SaaS)-Anwendungen austauschen können.
- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen AWS-Konten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Cloud Development Kit (CDK) ist ein Framework für die Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS CloudFormation.

- AWS DataOps Development Kit (DDK) ist ein Open-Source-Entwicklungs-Framework, das Sie beim Erstellen von Datenworkflows und einer modernen Datenarchitektur in AWS unterstützt.

Code

Der Code für dieses Muster ist im GitHub AWS DataOps Development Kit (DDK) und unter Analysieren von Google Analytics-Daten mit Amazon AppFlow, Amazon Athena und AWS DataOps Development Kit-Repositorys verfügbar.

Sekunden

Vorbereiten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie den Quellcode.	Führen Sie den folgenden Befehl aus, um den Quellcode zu klonen: `git clone https://github.com/aws-samples/aws-ddk-examples.git`	DevOps Techniker
Erstellen Sie eine virtuelle Umgebung.	Navigieren Sie zum Quellcodeverzeichnis und führen Sie dann den folgenden Befehl aus, um eine virtuelle Umgebung zu erstellen: `cd google-analytics-data-using-appflow/ python && python3 -m venv .venv`	DevOps Techniker
Installieren Sie die Abhängigkeiten.	Führen Sie den folgenden Befehl aus, um die virtuelle Umgebung zu aktivieren und	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Abhängigkeiten zu installieren: `source .venv/bin/activate && pip install -r requirements.txt`	

Bereitstellen der Anwendung, die Ihre Datenpipeline verwendet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrappen Sie die Umgebung.	1. Vergewissern Sie sich, dass die AWS CLI mit gültigen Anmeldeinformationen für Ihr AWS-Konto eingerichtet ist. Weitere Informationen finden Sie unter Verwenden benannter Profile in der AWS CLI-Dokumentation. 2. Führen Sie den Befehl `cdk bootstrap --profile [AWS_PROFILE]` aus.	DevOps Techniker
Stellen Sie die Daten bereit.	Um die Datenpipeline bereitzustellen, führen Sie den `cdk deploy --profile [AWS_PROFILE]` Befehl aus.	DevOps Techniker

Testen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Stack-Status.	1. Öffnen Sie die AWS-CloudFormation Konsole .	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Vergewissern Sie sich auf der Seite Stacks, dass der Status des Stacks `DdkAppflowAthenaStack` lautet `CREATE_COMPLETE` .	

Fehlerbehebung

Problem	Lösung
Die Bereitstellung schlägt während der Erstellung einer -`AWS::AppFlow::Flow` Ressource fehl und Sie erhalten den folgenden Fehler: `Connector Profile with name ga-connection does not exist`	Vergewissern Sie sich, dass Sie einen Amazon- AppFlow Konnektor für Google Analytics erstellt und benannt haben`ga-connection` . Anweisungen finden Sie unter Google Analytics in der Amazon- AppFlow Dokumentation.

Zugehörige Ressourcen

- AWS DataOps Development Kit (DDK) (GitHub)
- AWS DDK-Beispiele (GitHub)

Zusätzliche Informationen

AWS DDK-Datenpipelines bestehen aus einer oder mehreren Phasen. In den folgenden Codebeispielen verwenden Sie , `AppFlowIngestionStage` um Daten aus Google Analytics aufzunehmen, `SqsToLambdaStage` Datentransformation `AthenaSQLStage` zu verarbeiten und die Athena-Abfrage auszuführen.

Zunächst werden die Datentransformations- und Aufnahmephasen erstellt, wie das folgende Codebeispiel zeigt:

```
        appflow_stage = AppFlowIngestionStage(
            self,
            id="appflow-stage",
            flow_name=flow.flow_name,
        )
        sqs_lambda_stage = SqsToLambdaStage(
            self,
            id="lambda-stage",
            lambda_function_props={
                "code": Code.from_asset("./ddk_app/lambda_handlers"),
                "handler": "handler.lambda_handler",
                "layers": [
                    LayerVersion.from_layer_version_arn(
                        self,
                        id="layer",
                        layer_version_arn=f"arn:aws:lambda:
{self.region}:336392948345:layer:AWSDataWrangler-Python39:1",
                    )
                ],
                "runtime": Runtime.PYTHON_3_9,
            },
        )
        # Grant lambda function S3 read & write permissions
        bucket.grant_read_write(sqs_lambda_stage.function)
        # Grant Glue database & table permissions
        sqs_lambda_stage.function.add_to_role_policy(
            self._get_glue_db_iam_policy(database_name=database.database_name)
        )
        athena_stage = AthenaSQLStage(
            self,
            id="athena-sql",
            query_string=[
                (
                    "SELECT year, month, day, device, count(user_count) as cnt "
                    f"FROM {database.database_name}.ga_sample "
                    "GROUP BY year, month, day, device "
                    "ORDER BY cnt DESC "
                    "LIMIT 10; "
                )
            ],
            output_location=Location(
                bucket_name=bucket.bucket_name, object_key="query-results/"
            ),
```

```
            additional_role_policy_statements=[
                self._get_glue_db_iam_policy(database_name=database.database_name)
            ],
        )
```

Als Nächstes wird das `DataPipeline`Konstrukt verwendet, um die Phasen mithilfe von EventBridge Regeln zusammenzufassen, wie das folgende Codebeispiel zeigt:

```
        (
            DataPipeline(self, id="ingestion-pipeline")
            .add_stage(
                stage=appflow_stage,
                override_rule=Rule(
                    self,
                    "schedule-rule",
                    schedule=Schedule.rate(Duration.hours(1)),
                    targets=appflow_stage.targets,
                ),
            )
            .add_stage(
                stage=sqs_lambda_stage,
                # By default, AppFlowIngestionStage stage emits an event after the flow
run finishes successfully
                # Override rule below changes that behavior to call the the stage when
data lands in the bucket instead
                override_rule=Rule(
                    self,
                    "s3-object-created-rule",
                    event_pattern=EventPattern(
                        source=["aws.s3"],
                        detail={
                            "bucket": {"name": [bucket.bucket_name]},
                            "object": {"key": [{"prefix": "ga-data"}]},
                        },
                        detail_type=["Object Created"],
                    ),
                    targets=sqs_lambda_stage.targets,
                ),
            )
            .add_stage(stage=athena_stage)
        )
```

Weitere Codebeispiele finden Sie im GitHub Repository Analysieren von Google Analytics-Daten mit Amazon AppFlow, Amazon Athena und AWS DataOps Development Kit.

Konfigurieren Sie den kontoübergreifenden Zugriff auf einen gemeinsamen AWS Glue Glue-Datenkatalog mit Amazon Athena

Erstellt von Denis Avdonin (AWS)

Umgebung: Produktion	Technologien: Datenseen; Analytik; Große Datenmengen	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon Athena; AWS Glue		

Übersicht

Dieses Muster enthält step-by-step Anweisungen, einschließlich Richtlinienbeispielen für AWS Identity and Access Management (IAM), um die kontoübergreifende gemeinsame Nutzung eines in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeicherten Datensatzes mithilfe des AWS Glue Glue-Datenkatalogs zu konfigurieren. Sie können den Datensatz in einem S3-Bucket speichern. Die Metadaten werden von einem AWS Glue Glue-Crawler gesammelt und in den AWS Glue Glue-Datenkatalog aufgenommen. Der S3-Bucket und der AWS Glue Glue-Datenkatalog befinden sich in einem AWS-Konto, das als Datenkonto bezeichnet wird. Sie können den Zugriff auf IAM-Prinzipale in einem anderen AWS-Konto gewähren, das als Verbraucherkonto bezeichnet wird. Benutzer können die Daten im Verbraucherkonto mithilfe der serverlosen Amazon Athena Athena-Abfrage-Engine abfragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten
- Ein S3-Bucket in einem der AWS-Konten
- Athena-Engine-Version 2
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert (oder AWS CloudShell für die Ausführung von AWS-CLI-Befehlen)

Produktversionen

Dieses Muster funktioniert nur mit Athena-Engine-Version 2 und Athena-Engine-Version 3. Wir empfehlen Ihnen, auf Athena-Engine-Version 3 zu aktualisieren. Wenn Sie kein Upgrade von Athena-Engine-Version 1 auf Athena-Engine-Version 3 durchführen können, folgen Sie dem Ansatz für den kontoübergreifenden Zugriff auf den AWS Glue-Datenkatalog mit Amazon Athena im AWS Big Data-Blog.

Architektur

Zieltechnologie-Stack

- Amazon Athena
- Amazon-Simple-Storage-Service (Amazon-S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)

Das folgende Diagramm zeigt eine Architektur, die IAM-Berechtigungen verwendet, um Daten in einem S3-Bucket in einem AWS-Konto (Datenkonto) mit einem anderen AWS-Konto (Verbraucherkonto) über den AWS Glue-Datenkatalog zu teilen.

Das Diagramm zeigt den folgenden Workflow:

1. Die S3-Bucket-Richtlinie im Datenkonto gewährt Berechtigungen für eine IAM-Rolle im Verbraucherkonto und für die AWS Glue Glue-Crawler-Servicerolle im Datenkonto.
2. Die AWS KMS KMS-Schlüsselrichtlinie im Datenkonto gewährt Berechtigungen für die IAM-Rolle im Verbraucherkonto und für die AWS Glue Glue-Crawler-Servicerolle im Datenkonto.
3. Der AWS Glue Glue-Crawler im Datenkonto erkennt das Schema der Daten, die im S3-Bucket gespeichert sind.
4. Die Ressourcenrichtlinie des AWS Glue Glue-Datenkatalogs im Datenkonto gewährt Zugriff auf die IAM-Rolle im Verbraucherkonto.
5. Ein Benutzer erstellt mithilfe eines AWS-CLI-Befehls eine benannte Katalogreferenz im Verbraucherkonto.
6. Eine IAM-Richtlinie gewährt einer IAM-Rolle im Verbraucherkonto Zugriff auf Ressourcen im Datenkonto. Die Vertrauensrichtlinie der IAM-Rolle ermöglicht es Benutzern im Verbraucherkonto, die IAM-Rolle zu übernehmen.

7. Ein Benutzer im Verbraucherkonto übernimmt die IAM-Rolle und greift mithilfe von SQL-Abfragen auf Objekte im Datenkatalog zu.
8. Die serverlose Athena Engine führt die SQL-Abfragen aus.

Hinweis: Bewährte IAM-Methoden empfehlen, einer IAM-Rolle Berechtigungen zu erteilen und einen Identitätsverbund zu verwenden.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel zum Schutz Ihrer Daten.

Epen

Richten Sie Berechtigungen im Datenkonto ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff auf Daten im S3-Bucket.	Erstellen Sie eine S3-Bucket-Richtlinie auf der Grundlage der folgenden Vorlage und weisen Sie die Richtlinie dem Bucket zu, in dem die Daten gespeichert sind. `{`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	"Version":
	"2012-10-17",
	"Statement": [
	{
	"Effect":
	"Allow",
	"Principa
	l": {
	"AWS": [
	
	"arn:aws:iam::<con
	sumer account id>:role/
	<role name>",
	
	"arn:aws:iam::<dat
	a account id>:role/
	service-role/AWSGl
	ueServiceRole-data-
	bucket-crawler"
	]
	},
	"Action":
	"s3:GetObject",
	"Resource":
	"arn:aws:s3:::data-
	bucket/*"
	},
	{
	"Effect":
	"Allow",
	"Principa
	l": {
	"AWS": [
	
	"arn:aws:iam::<con
	sumer account id>:role/
	<role name>",
	
	"arn:aws:iam::<dat
	a account id>:role/
	service-role/AWSGl</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ueServiceRole-data-bucket-crawler"] }, "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }] } Die Bucket-Richtlinie gewährt Berechtigungen für die IAM-Rolle im Verbraucherkonto und für die AWS Glue Glue-Crawler-Servicerolle im Datenkonto.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Falls erforderlich) Gewähren Sie Zugriff auf den Datenverschlüsselungsschlüssel.	Wenn der S3-Bucket mit einem AWS-KMS-Schlüssel verschlüsselt ist, `kms:Decrypt` erteilen Sie der IAM-Rolle im Verbraucherkonto und der AWS Glue Glue-Crawler-Servicerolle im Datenkonto die Erlaubnis für den Schlüssel. Aktualisieren Sie die Schlüsselrichtlinie mit der folgenden Aussage: `{ "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie dem Crawler Zugriff auf die Daten.	Fügen Sie der Servicerolle des Crawlers die folgende IAM-Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" } ] }`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Falls erforderlich) Gewähren Sie dem Crawler Zugriff auf den Datenverschlüsselungsschlüssel.	Wenn der S3-Bucket mit einem AWS-KMS-Schlüssel verschlüsselt ist, erteilen Sie der Service-Rolle des Crawlers die `kms:Decrypt` Erlaubnis für den Schlüssel, indem Sie ihm die folgende Richtlinie anhängen: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie der IAM-Rolle im Verbraucherkonto und dem Crawler Zugriff auf den Datenkatalog.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Einstellungen aus. 3. Fügen Sie im Abschnitt Berechtigungen die folgende Anweisung hinzu, und wählen Sie dann Speichern aus. `{ "Version" : "2012-10-17", "Statement" : [ { "Effect" : "Allow", "Principal" : { "AWS" : [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, ...`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Action" : "glue:*", "Resource" : ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Diese Richtlinie erlaubt alle AWS Glue Glue-Aktionen für alle Datenbanken und Tabellen im Datenkonto. Sie können die Richtlinie so anpassen, dass den Benutzerprinzipalen nur die erforderlichen Berechtigungen gewährt werden. Sie können beispielsweise schreibgeschützten Zugriff auf bestimmte Tabellen oder Ansichten in einer Datenbank gewähren.	

Greifen Sie über das Verbraucherkonto auf Daten zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine benannte Referenz für den Datenkata log.	Um eine benannte Datenkata logreferenz zu erstellen, verwenden Sie CloudShel loder eine lokal installierte AWS-CLI, um den folgenden Befehl auszuführen: `aws athena create-da ta-catalog --name <shared catalog name> --type GLUE --paramet ers catalog-id=<data account id>`	Cloud-Administrator
Gewähren Sie der IAM-Rolle im Verbraucherkonto Zugriff auf die Daten.	Fügen Sie der IAM-Rolle im Verbraucherkonto die folgende Richtlinie hinzu, um der Rolle kontoübergreifenden Zugriff auf die Daten zu gewähren: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow",`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }, { "Effect": "Allow", "Action": "glue:*", "Resource": ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Verwenden Sie als Nächstes die folgende Vorlage, um anzugeben, welche Benutzer die IAM-Rolle in ihrer Vertrauensrichtlinie akzeptieren können: <pre>{ "Version": "2012-10-17",</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	    "Statement": [
	       {
	            "Effect":
	 "Allow",
	            "Principa
	l": {
	                "AWS":
	 "arn:aws:iam::<con
	sumer account id>:user/
	<IAM user>"
	            },
	            "Action":
	 "sts:AssumeRole"
	        }
	    ]
	}</pre> Erteilen Sie den Benutzern abschließend Berechtigungen zur Übernahme der IAM-Rolle, indem Sie dieselbe Richtlinie an die Benutzergruppe anhängen, zu der sie gehören.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Falls erforderlich) Gewähren Sie der IAM-Rolle im Verbraucherkonto Zugriff auf den Datenverschlüsselungsschlüssel.	Wenn der S3-Bucket mit einem AWS-KMS-Schlüssel verschlüsselt ist, erteilen Sie der IAM-Rolle im Verbrauch erkonto die `kms:Decrypt` Erlaubnis für den Schlüssel , indem Sie ihm die folgende Richtlinie anhängen: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Cloud-Administrator
Wechseln Sie im Verbrauch erkonto zur IAM-Rolle, um auf Daten zuzugreifen.	Wechseln Sie als Datenverbraucher zur IAM-Rolle, um auf Daten im Datenkonto zuzugreifen.	Datenverbraucher

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Greifen Sie auf die Daten zu.	Fragen Sie Daten mit Athena ab. Öffnen Sie beispielsweise den Athena-Abfrage-Editor und führen Sie die folgende Abfrage aus:
	
	`SELECT * FROM <shared catalog name>.<database name>.<table name>`
	
	Anstatt eine benannte Katalogreferenz zu verwenden, können Sie auch anhand seines Amazon-Ressourcennamens (ARN) auf den Katalog verweisen.
	
	Hinweis: Wenn Sie eine dynamische Katalogreferenz in einer Abfrage oder Ansicht verwenden, setzen Sie den Verweis in doppelte Anführungszeichen (\“). Beispielsweise:
	
	`SELECT * FROM \"glue:arn:aws:glue:<region>:<data account id>:catalog\".<database name>.<table name>`
	
	Weitere Informationen finden Sie unter Kontoübergreifender Zugriff auf AWS Glue Glue-
		Datenverbraucher

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datenkataloge im Amazon Athena Athena-Benutzerhandbuch.	

Zugehörige Ressourcen

- Kontoübergreifender Zugriff auf AWS Glue Glue-Datenkataloge (Athena-Dokumentation)
- (AWS CLI) create-data-catalog (AWS CLI-Befehlsreferenz)
- Kontoübergreifender Zugriff auf den AWS Glue-Datenkatalog mit Amazon Athena (AWS Big Data Blog)
- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)

Zusätzliche Informationen

Verwendung von Lake Formation als Alternative für kontenübergreifendes Teilen

Sie können AWS Lake Formation auch verwenden, um den Zugriff auf AWS Glue Glue-Katalogobjekte für mehrere Konten gemeinsam zu nutzen. Lake Formation bietet eine detaillierte Zugriffskontrolle auf Spalten- und Zeilenebene, Tag-basierte Zugriffskontrolle, gesteuerte Tabellen für ACID-Transaktionen und andere Funktionen. Lake Formation ist zwar gut in Athena integriert, erfordert jedoch eine zusätzliche Konfiguration im Vergleich zum reinen IAM-Ansatz dieses Musters. Wir empfehlen Ihnen, die Entscheidung, Lake Formation oder reine IAM-Zugriffskontrollen zu verwenden, im breiteren Kontext Ihrer gesamten Lösungsarchitektur zu berücksichtigen. Zu den Überlegungen gehören auch, um welche anderen Dienste es sich handelt und wie sie sich in beide Ansätze integrieren lassen.

Kontoübergreifende Automatisierung der Datenfreigabe

Erstellt von Issam Habibi (AWS), Bol Hourcade (AWS) und Bolalena Calvo (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Data Lakes; Analytik	Workload: Alle anderen Workloads
AWS-Services: AWS Glue; AWS Lake Formation; AWS RAM; Amazon Athena		

Übersicht

Mehrere unabhängige Geschäftsbereiche (BUs) innerhalb einer Organisation zu haben bedeutet, dass eine strenge Kontrolle über die Data-Lake-Zugriffsberechtigungen oberste Priorität haben sollte und dass jede Geschäftseinheit nur auf ihre eigenen Daten zugreifen darf. Die Workloads einer Geschäftseinheit könnten jedoch eine andere Geschäftseinheit für Analysezwecke interessieren, was mit einer differenzierten Berechtigungskontrolle das Interesse am Thema der BU-übergreifenden Datenfreigabe wecken würde.

In dieser Version nehmen wir an, dass eine Geschäftseinheit einem AWS-Konto zugeordnet ist, das seine Daten hostet (von Glue gecrawlte Datenbanken aus S3), und dass die bereichsübergreifende Datenfreigabe daher zu einem Problem mit der kontoübergreifenden AWS-Datenfreigabe wird.
Wir bieten eine automatisierte Möglichkeit, bestimmte Tabellen einer Glue-Datenbank mit einem Prinzipal eines externen AWS-Kontos mithilfe von Lake Formation gemeinsam zu nutzen. Diese Automatisierung ermöglicht es den Datenbesitzern, externen BUs das Recht zu gewähren, Analyseabfragen (z. B. mit Athena) für definierte Tabellen auszuführen.

Sie können diese automatisierte Lösung verwenden, um einen typischen Anwendungsfall zu erfüllen, z. B.:

Das Personaldatenteam wird in einem AWS-Quellkonto gehostet, das die Tabelle mit den Gehältern für das AWS-Zielkonto des Datenanalystenteams teilt, das mit Athena weiter abgefragt werden soll.

Voraussetzungen und Einschränkungen

Voraussetzungen

Für diese Bereitstellung benötigen Sie:

- zwei AWS-Konten (Quellkonto und Zielkonto) mit ausreichenden Berechtigungen zum Bereitstellen von AWS-Ressourcen, die in diesem Code verpackt sind
- aws-cdk: global installiert (npm-Installation -g aws-cdk)
- Git-Client
- Mindestens eine durchsuchte -Glue-Datenbank mit Tabellen darin .
- Wenige manuelle Lake-Formation-Konfigurationen, die im Abschnitt „Epics“ dargestellt werden

Einschränkungen

- Diese Lösung erfordert bereits durchsuchte Glue-Datenbanken im AWS-Quellkonto.

- Diese Lösung bietet noch keine automatisierte Möglichkeit, die erteilten Berechtigungen zu widerrufen. Sobald Sie Daten von einem Quellkonto für ein Zielkonto freigegeben haben, sollte der Zugriff manuell in der Lake-Formation-Konsole widerrufen werden.

Architektur

Übersicht über die Lösung

Dieser CDK-Code stellt die im folgenden Diagramm zusammengefasste Architektur bereit

Sie umfasst insbesondere:

Quellkonto-Stack:

- DynamoDb Tabelle : Diese Tabelle enthält die Freigabeberechtigungsdefinitionen, die ein Benutzer hochlädt. Es sind DynamoDb Streams aktiviert und löst für jedes der Tabelle hinzugefügte Freigabeberechtigungselement ein Lambda aus.
- Eine Lambda-Funktion : erteilt einem externen Prinzipal die angegebenen Berechtigungen für eine Tabelle.

Zielkonto-Stack:

- Resource Access Manager (RAM): Nimmt Einladungen von Lake Formation an. Eine Einladung sollte angenommen werden, um Zugriff auf die freigegebenen Daten zu erhalten.
- Amazon SQS : empfängt Nachrichten vom Quellkonto, die darauf hinweisen, dass eine Freigabeprozedur gestartet wurde
- EventBridge Regel : Diese Regel wird ausgelöst, sobald eine RAM-Einladung akzeptiert wird.
- Zwei Lambda-Funktionen: eine, die von der SQS-Warteschlange ausgelöst wird, die automatisch die RAM-Einladungen akzeptiert, und eine zweite Funktion, die von der EventBridge Regel ausgelöst wird, die die lokale gemeinsam genutzte Datenbank erstellt und die Ressource verweist auf die gemeinsam genutzten Ressourcen. Diese Ressourcenlinks könnten mit Athena weiter abgefragt werden.

Der Prozess könnte in den folgenden Schritten zusammengefasst werden:

1 – Benutzer lädt das Freigabedefinitionselement in die dynamoDb-Tabelle im Quellkonto hoch.

2- DynamoDb Streams lösen das Quellkonto Lambda aus, das die Tabelle der im Freigabedefinitionselement angegebenen Datenbank mithilfe von Lake Formation mit dem Zielkonto teilt. Diese Freigabe sendet automatisch eine RAM-Einladung an das Zielkonto.

3 – Das Quellkonto Lambda sendet auch eine Nachricht an eine SQS-Warteschlange im Zielkonto, die es über den Beginn des Freigabevorgangs informiert.

4 – Auf dem Zielkonto löst die SQS-Warteschlange ein Lambda aus, das die empfangene RAM-Einladung akzeptiert.

5 – Nach Annahme der Einladung löst eine - EventBridge Regel eine Lamdba aus, die eine lokale Datenbank erstellt, und einen Ressourcenlink, der die freigegebene Tabelle enthält. Dieses Lambda erteilt dem Zielprinzipal auch Berechtigungen für die freigegebenen Daten.

6 – Der Prinzipal kann Daten mit Athena abfragen.

Tools

Code-Repository

Der Code für dieses Muster ist auf Gitlab verfügbar

Bewährte Methoden

- Es ist obligatorisch, wie bereits erwähnt, dass Sie über eine bereits von Glue gecrawlte Datenbank in Ihrem Konto verfügen.
- Die Datenbanknamen und Tabellennamen sollten mit denen in der durch Glue gecrawlten Datenbank übereinstimmen.
- Das Freigabeeingabeelement, das in dynamoDb eingefügt werden soll, sollte wie folgt aussehen:

Polen

Klonen Sie das Repository und konfigurieren Sie die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen des Repositorys	Klonen des Gitlab-Repositorys auf Ihrem Computer
	`git clone git@ssh.gitlab.aws.dev:ihabibi/cross-account-data-sharing.git`
	`cd cross-account-data-sharing`
		Allgemeines AWS

Konfigurieren Ihrer Bereitstellung	Bearbeiten Sie die `resources.py` Datei mit Informationen über die Region, die von Ihnen verwendeten Quell-/Zielkonten und den Zielprinzipal-ARN
	`AWS_REGION = 'eu-west-1'`
	`AWS_SOURCE_ACCOUNT_ID = '111111111111'`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AWS_TARGET_ACCOUNT_ID = '222222222222' TARGET_PRINCIPAL_ARN = 'arn:aws:iam::222222222222:role/admin'`	

Bootstrappen Sie Ihr AWS-Konto und stellen Sie den Code bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrapping Ihres AWS-Quellkontos	Falls noch nicht geschehen, müssen Sie Ihre AWS-Umgebung bootstrappen, bevor Sie diese CDK-Anwendung bereitstellen. Führen Sie die folgenden Befehle mit den AWS-Anmeldeinformationen Ihres AWS-Quellkontos aus: `cdk bootstrap aws://<source-account-id>/<aws-region>`	Allgemeines AWS
Bereitstellen des Quell-CDK-Stacks	Nachdem Ihr AWS-Quellkonto gestartet wurde und Sie Ihre Bereitstellung konfiguriert haben, können Sie die CDK-Anwendung mit dem folgenden Befehl bereitstellen: (stellen Sie sicher, dass Sie sich im Verzeichnis cross-account-data-sharing/ befinden)	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk deploy SourceAccountStack`	
Bootstrap Ihres AWS-Zielkontos	Falls noch nicht geschehen, müssen Sie Ihre AWS-Umgebung booten, bevor Sie diese CDK-Anwendung bereitstellen. Führen Sie die folgenden Befehle mit den AWS-Anmeldeinformationen Ihres AWS-Zielkontos aus: `cdk bootstrap aws://<target-account-id>/<aws-region>`	Allgemeines AWS
Bereitstellen des Ziel-CDK-Stacks	Nachdem Ihr AWS-Zielkonto gestartet und Ihre Bereitstellung konfiguriert wurde, können Sie die CDK-Anwendung mit dem folgenden Befehl bereitstellen: (stellen Sie sicher, dass Sie sich im Verzeichnis cross-account-data-sharing/ befinden) `cdk deploy TargetAccountStack`	Allgemeines AWS

Einrichten von Lake Formation auf dem Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichten von Lake Formation auf dem Quellkonto	• Melden Sie sich im Quellkonto bei der Lake-Formation-Konsole an und navigieren Sie zu Registrie ren und Erfassen —> Data-Lake-Standorte. Registrie ren Sie den S3-Speicherort Ihrer Daten. • Gehen Sie zu Berechtig ungen —> Data-Lake-Berechtigungen. Widerrufen Sie alle IAM-AllowedGroup Berechtigungen.	

Testen der kontoübergreifenden Freigabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Freigeben einer Tabelle von der Quelle für das Zielkonto	• Melden Sie sich bei der Konsole Ihres Quellkont os an DynamoDb und suchen Sie nach der Tabelle „permissions_table“ und fügen Sie ein Element nach diesem Schema ein. Sie können auch AWS CLI verwenden `{ "share_id": "1", "table_name": "sample_data",`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"database_name": "database-ohio", "permissions": "DESCRIBE,SELECT", "source_acc_id": "111111111111", "target_acc_id": "222222222222" }</pre> Sobald das Element in die Tabelle eingefügt wurde, löst es den gesamten Prozess aus und die Tabelle sollte innerhalb weniger Sekunden im Zielkonto abgefragt werden können. • Beachten Sie, dass die möglichen Berechtigungen DESCRIBE, SELECT sind. Sie sollten durch ein Komma getrennt werden.	
Abfragen der Tabelle auf dem Zielkonto	• Melden Sie sich bei der Konsole Ihres Zielkontos an. Sie werden feststellen, dass Lake Formation die freigegebene Tabelle bereits erkennt und Sie sie mit Athena abfragen können.	

Zugehörige Ressourcen

Code in Gitlab

Zusätzliche Informationen

Dokumentation der wichtigsten verwendeten Services:

Amazon DynamoDb

AWS Lambda

AWS Lake Formation

AWS Glue

AWS Resource Access Manager

Amazon SQS

Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden

Umgebung: Produktion	Technologien: Datenseen; Analytik; Serverlos; DevOps	Arbeitslast: Alle anderen Workloads
AWS-Services: Amazon S3; Amazon SQS; AWS; AWS Glue CloudForm ation; Amazon; AWS Lambda CloudWatch; AWS Step Functions; Amazon DynamoDB		

Übersicht

Dieses Muster beschreibt, wie Serverless Computing und Infrastructure as Code (IaC) verwendet werden, um einen Data Lake in der Amazon Web Services (AWS) -Cloud zu implementieren und zu verwalten. Dieses Muster basiert auf dem von AWS entwickelten Workshop zum Serverless Data Lake Framework (SDLF).

SDLF ist eine Sammlung wiederverwendbarer Ressourcen, die die Bereitstellung von Unternehmensdatenseen in der AWS-Cloud beschleunigen und zu einer schnelleren Bereitstellung in der Produktion beitragen. Es wird verwendet, um die grundlegende Struktur eines Data Lakes unter Befolgung bewährter Methoden zu implementieren.

SDLF implementiert einen CI/CD-Prozess (Continuous Integration/Continuous Deployment) während der gesamten Code- und Infrastrukturbereitstellung mithilfe von AWS-Services wie AWS CodePipeline, AWS und AWS CodeBuild. CodeCommit

Dieses Muster verwendet mehrere serverlose AWS-Services, um das Data Lake-Management zu vereinfachen. Dazu gehören Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB für die Speicherung, AWS Lambda und AWS Glue für die Datenverarbeitung sowie Amazon CloudWatch Events, Amazon Simple Queue Service (Amazon SQS) und AWS Step Functions für die Orchestrierung.

AWS CloudFormation - und AWS-Code-Services fungieren als IaC-Schicht und bieten reproduzierbare und schnelle Bereitstellungen mit einfachem Betrieb und einfacher Verwaltung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert.
- Ein Git-Client, installiert und konfiguriert.
- Der SDLF-Workshop wird in einem Webbrowser-Fenster geöffnet und ist sofort einsatzbereit.

Architektur

Das Architekturdiagramm veranschaulicht einen ereignisgesteuerten Prozess mit den folgenden Schritten.

1. Nachdem eine Datei zum Rohdaten-S3-Bucket hinzugefügt wurde, wird eine Amazon S3 S3-Ereignisbenachrichtigung in eine SQS-Warteschlange gestellt. Jede Benachrichtigung wird als JSON-Datei zugestellt, die Metadaten wie den S3-Bucket-Namen, den Objektschlüssel oder den Zeitstempel enthält.
2. Diese Benachrichtigung wird von einer Lambda-Funktion verarbeitet, die das Ereignis auf der Grundlage der Metadaten an den richtigen Extraktions-, Transformations- und Ladeprozess (ETL) weiterleitet. Die Lambda-Funktion kann auch kontextbezogene Konfigurationen verwenden, die in einer Amazon DynamoDB-Tabelle gespeichert sind. Dieser Schritt ermöglicht die Entkopplung und Skalierung auf mehrere Anwendungen im Data Lake.
3. Das Ereignis wird an die erste Lambda-Funktion im ETL-Prozess weitergeleitet, die Daten transformiert und aus dem Rohdatenbereich in den Staging-Bereich für den Data Lake verschiebt. Der erste Schritt besteht darin, den umfassenden Katalog zu aktualisieren. Dies ist eine DynamoDB-Tabelle, die alle Dateimetadaten des Data Lake enthält. Jede Zeile in dieser Tabelle enthält Betriebsmetadaten zu einem einzelnen Objekt, das in Amazon S3 gespeichert ist. Es wird synchron eine Lambda-Funktion aufgerufen, die eine leichte Transformation für das S3-Objekt durchführt. Dabei handelt es sich um einen rechenintensiven Vorgang (z. B. das Konvertieren

einer Datei von einem Format in ein anderes). Da dem Staging-S3-Bucket ein neues Objekt hinzugefügt wurde, wird der umfassende Katalog aktualisiert und eine Nachricht an die SQS-Warteschlange gesendet, in der auf die nächste ETL-Phase gewartet wird.

4. Eine CloudWatch Ereignisregel löst alle 5 Minuten eine Lambda-Funktion aus. Diese Funktion prüft, ob Nachrichten aus der vorherigen ETL-Phase an die SQS-Warteschlange zugestellt wurden. Wenn eine Nachricht zugestellt wurde, startet die Lambda-Funktion die zweite Funktion von AWS Step Functions im ETL-Prozess.
5. Anschließend wird eine umfangreiche Transformation auf einen Stapel von Dateien angewendet. Diese umfangreiche Transformation ist ein rechenintensiver Vorgang, z. B. ein synchroner Aufruf eines AWS Glue-Jobs, einer AWS Fargate-Aufgabe, eines Amazon EMR-Schritts oder eines Amazon-Notebooks. SageMaker Tabellenmetadaten werden mithilfe eines AWS Glue-Crawlers, der den AWS Glue-Katalog aktualisiert, aus den Ausgabedateien extrahiert. Dateimetadaten werden auch der umfassenden Katalogtabelle in DynamoDB hinzugefügt. Schließlich wird auch ein Datenqualitätsschritt ausgeführt, der Deequ nutzt.

Technologie-Stack

- CloudWatch Amazon-Veranstaltungen
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- Amazon-DynamoDB
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SQS
- AWS Step Functions

Tools

- Amazon CloudWatch Events — CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.

- AWS CloudFormation — CloudFormation hilft bei der vorhersehbaren und wiederholten Erstellung und Bereitstellung von AWS-Infrastrukturbereitstellungen.
- AWS CodeBuild — CodeBuild ist ein vollständig verwalteter Build-Service, der Ihren Quellcode kompiliert, Komponententests durchführt und Artefakte erzeugt, die sofort einsatzbereit sind.
- AWS CodeCommit — CodeCommit ist ein von AWS gehosteter Service zur Versionskontrolle, mit dem Sie Ressourcen (wie Quellcode und Binärdateien) privat speichern und verwalten können.
- AWS CodePipeline — CodePipeline ist ein Continuous Delivery Service, mit dem Sie die Schritte modellieren, visualisieren und automatisieren können, die für die kontinuierliche Veröffentlichung Ihrer Softwareänderungen erforderlich sind.
- Amazon DynamoDB — DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit Skalierbarkeit bietet.
- AWS Glue — AWS Glue ist ein vollständig verwalteter ETL-Service, der das Aufbereiten und Laden von Daten für Analysen erleichtert.
- AWS Lambda — Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice. Amazon S3 kann für eine Vielzahl von Speicherlösungen verwendet werden, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- AWS Step Functions — AWS Step Functions ist ein serverloser Funktionsorchestrator, der es einfach macht, AWS Lambda Lambda-Funktionen und mehrere AWS-Services in geschäftskritischen Anwendungen zu sequenzieren.
- Amazon SQS — Amazon Simple Queue Service (Amazon SQS) ist ein vollständig verwalteter Message Queuing-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln und skalieren können.
- Deequ — Deequ ist ein Tool, das Ihnen dabei hilft, Datenqualitätskennzahlen für große Datenmengen zu berechnen, Datenqualitätsbeschränkungen zu definieren und zu überprüfen und über Änderungen bei der Datenverteilung auf dem Laufenden zu bleiben.

Code

Der Quellcode und die Ressourcen für das SDLF sind im AWS GitHub Labs-Repository verfügbar.

Epen

Richten Sie die CI/CD-Pipeline für die Bereitstellung von IaC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die CI/CD-Pipeline ein, um IaC für den Data Lake zu verwalten.	Melden Sie sich bei der AWS-Managementkonsole an und folgen Sie den Schritten aus dem Abschnitt Ersteinrichtung des SDLF-Workshops. Dadurch werden die ersten CI/CD-Ressourcen wie CodeCommit Repositorys, CodeBuild Umgebungen und CodePipeline Pipelines erstellt, die IaC für den Data Lake bereitstellen und verwalten.	DevOps Ingenieur

Versionskontrolle des IaC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das CodeCommit Repository auf Ihrem lokalen Computer.	Folgen Sie den Anweisungen aus dem Abschnitt Einführung der Grundlagen des SDLF-Workshops. Auf diese Weise können Sie das Git-Repository, das IaC hostet, in Ihre lokale Umgebung klonen. Weitere Informationen finden Sie in der Dokumentation unter Verbindung zu	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommit Repositorys herstellen. CodeCommit	
Ändern Sie die CloudFormation Vorlagen.	Verwenden Sie Ihre lokale Workstation und einen Code-Editor, um die CloudFormation Vorlagen an Ihre Anwendungsfälle oder Anforderungen anzupassen. Übergeben Sie sie in das lokal geklonte Git-Repository. Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation unter Arbeiten mit CloudFormation AWS-Vorlagen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Änderungen in das CodeCommit Repository.	Ihr Infrastrukturcode unterliegt jetzt der Versionskontrolle und Änderungen an Ihrer Codebasis werden nachverfolgt. Wenn Sie eine Änderung per Push in das CodeCommit Repository übertragen, CodePipeline wird sie automatisch auf Ihre Infrastruktur angewendet und an diese weitergeleitet CodeBuild. Wichtig: Wenn Sie die AWS SAM-CLI in verwenden CodeBuild, führen Sie die `sam deploy` Befehle `sam package` und aus. Wenn Sie die AWS-CLI verwenden, führen Sie die `aws cloudformation deploy` Befehle `aws cloudformation package` und aus.	DevOps Ingenieur

Zugehörige Ressourcen

Richten Sie die CI/CD-Pipeline für die Bereitstellung von IaC ein

- SDLF-Workshop — Erste Einrichtung

Versionskontrolle des IaC

- SDLF-Workshop — Bereitstellung der Grundlagen
- Verbindung zu Repositorien herstellen CodeCommit
- Arbeiten mit CloudFormation AWS-Vorlagen

Sonstige Ressourcen

- Referenzarchitektur für die serverlose Datenanalyse-Pipeline von AWS
- SDLF-Dokumentation

Kostengünstige Aufnahme von IoT-Daten direkt in Amazon S3 mit AWS IoT Greengrass

Erstellt von Sebastian Viviani (AWS) und Rizwan Syed (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Data Lakes; Analytik; IoT	Workload: Open-Source
AWS-Services: AWS IoT Greengrass; Amazon S3; Amazon Athena		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Internet of Things (IoT)-Daten mithilfe eines AWS IoT Greengrass Version 2-Geräts direkt in einen Amazon Simple Storage Service (Amazon S3)-Bucket aufnehmen können. Das Gerät führt eine benutzerdefinierte Komponente aus, die die IoT-Daten liest und die Daten im persistenten Speicher (d. h. auf einem lokalen Datenträger oder Volume) speichert. Anschließend komprimiert das Gerät die IoT-Daten in eine Apache-Parquet-Datei und lädt die Daten regelmäßig in einen S3-Bucket hoch.

Die Menge und Geschwindigkeit der IoT-Daten, die Sie aufnehmen, wird nur durch Ihre Edge-Hardware-Funktionen und Netzwerkbandbreite begrenzt. Sie können Amazon Athena verwenden, um Ihre aufgenommenen Daten kostengünstig zu analysieren. Athena unterstützt komprimierte Apache-Parquet-Dateien und Datenvisualisierung mithilfe von Amazon Managed Grafana .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Edge-Gateway, das auf AWS IoT Greengrass Version 2 ausgeführt wird und Daten von Sensoren sammelt (die Datenquellen und der Datenerfassungsprozess liegen außerhalb des Geltungsbereichs dieses Musters, aber Sie können fast jede Art von Sensordaten verwenden. Dieses Muster verwendet einen lokalen MQTT-Broker mit Sensoren oder Gateways, die Daten lokal veröffentlichen.)

- AWS IoT Greengrass-Komponente , Rollen und SDK-Abhängigkeiten
- Eine Stream-Manager-Komponente zum Hochladen der Daten in den S3-Bucket
- AWS SDK for Java , AWS SDK for JavaScript oder AWS SDK for Python (Boto3) zum Ausführen der APIs

Einschränkungen

- Die Daten in diesem Muster werden nicht in Echtzeit in den S3-Bucket hochgeladen. Es gibt einen Verzögerungszeitraum, und Sie können den Verzögerungszeitraum konfigurieren. Daten werden vorübergehend auf dem Edge-Gerät gepuffert und dann nach Ablauf des Zeitraums hochgeladen.
- Das SDK ist nur in Java, Node.js und Python verfügbar.

Architektur

Zieltechnologie-Stack

- Amazon S3
- AWS IoT Greengrass
- MQTT-Broker
- Stream-Manager-Komponente

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur, die darauf ausgelegt ist, IoT-Sensordaten aufzunehmen und diese Daten in einem S3-Bucket zu speichern.

Das Diagramm zeigt den folgenden Workflow:

1. Mehrere Sensoren (z. B. Temperatur und Temperatur) werden auf einem lokalen MQTT-Broker veröffentlicht.
2. Das Parquet-Dateifragment, das diese Sensoren abonniert hat, aktualisiert Themen und erhält diese Updates.
3. Die Parquet-Datei speichert die Updates lokal.

4. Nach Ablauf des Zeitraums werden die gespeicherten Dateien in Parquet-Dateien komprimiert und an den Stream-Manager übergeben, um in den angegebenen S3-Bucket hochgeladen zu werden.
5. Der Stream-Manager lädt die Parquet-Dateien in den S3-Bucket hoch.

Hinweis: Der Stream-Manager (`StreamManager`) ist eine verwaltete Komponente. Beispiele für den Export von Daten nach Amazon S3 finden Sie unter Stream Manager in der AWS IoT Greengrass-Dokumentation. Sie können einen lokalen MQTT-Broker als Komponente oder einen anderen Broker wie Eclipse Mosquitto verwenden.

Tools

AWS-Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS IoT Greengrass ist ein Open-Source-IoT-Edge-Laufzeit- und Cloud-Service, mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können.

Andere Tools

- Apache Parquet ist ein spaltenorientiertes Open-Source-Datendateiformat, das für die Speicherung und den Abruf entwickelt wurde.
- MQTT (Message Queuing Telemetry Transport) ist ein leichtgewichtiges Messaging-Protokoll, das für eingeschränkte Geräte entwickelt wurde.

Bewährte Methoden

Verwenden Sie das richtige Partitionsformat für hochgeladene Daten

Es gibt keine spezifischen Anforderungen für die Root-Präfixnamen im S3-Bucket (z. B. `"myAwesomeDataSet/"` oder `"dataFromSource"`), aber wir empfehlen Ihnen, eine aussagekräftige Partition und ein aussagekräftiges Präfix zu verwenden, damit der Zweck des Datensatzes leicht verständlich ist.

Wir empfehlen außerdem, die richtige Partitionierung in Amazon S3 zu verwenden, damit die Abfragen optimal für den Datensatz ausgeführt werden. Im folgenden Beispiel werden die Daten im HIVE-Format partitioniert, sodass die von jeder Athena-Abfrage gescannte Datenmenge optimiert wird. Dies verbessert die Leistung und senkt die Kosten.

```
s3://<ingestionBucket>/<rootPrefix>/year=YY/month=MM/day=DD/
HHMM_<suffix>.parquet
```

Polen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Erstellen Sie einen S3-Bucket oder verwenden Sie einen vorhandenen Bucket. 2. Erstellen Sie ein aussagekräftiges Präfix für den S3-Bucket, in den Sie die IoT-Daten aufnehmen möchten (z. B. `s3:\\<bucket>\<prefix>`). 3. Notieren Sie Ihr Präfix zur späteren Verwendung.	App-Developer
Fügen Sie dem S3-Bucket IAM-Berechtigungen hinzu.	Um Benutzern Schreibzugriff auf den S3-Bucket und das zuvor erstellte Präfix zu gewähren, fügen Sie Ihrer AWS IoT Greengrass-Rolle die folgende IAM-Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	"Sid": "S3DataUpload",
	"Effect": "Allow",
	"Action": [
	"s3:List*",
	"s3:Put*"
	],
	"Resource": [
	"arn:aws:s3:::<ingestionBucket>",
	"arn:aws:s3:::<ingestionBucket>/<prefix>/*"
	]
	}
	]
	}</pre>
	Weitere Informationen finden Sie unter Erstellen einer IAM-Richtlinie für den Zugriff auf Amazon S3-Ressourcen in der Aurora-Dokumentation.
	
	Aktualisieren Sie als Nächstes die Ressourcenrichtlinie (falls erforderlich) für den S3-Bucket, um Schreibzugriff mit den richtigen AWS-Prinzipalen zu ermöglichen.	

Erstellen und Bereitstellen der AWS IoT Greengrass-Komponente

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie das Rezept der Komponente.	Aktualisieren Sie die Komponentenkonfiguration, wenn Sie eine Bereitstellung basierend auf dem folgenden Beispiel erstellen: `{ "region": "<region>", "parquet_period": <period>, "s3_bucket": "<s3Bucket>", "s3_key_prefix": "<s3prefix>" }` Ersetzen Sie `<region>` durch Ihre AWS-Region, `<period>` durch Ihr periodisches Intervall , `<s3Bucket>` durch Ihren S3-Bucket und `<s3prefix>` durch Ihr Präfix.	App-Developer
Erstellen Sie die Komponente.	Führen Sie eine der folgenden Aktionen aus: • Erstellen Sie die Komponente . • Fügen Sie die Komponente der CI/CD-Pipeline hinzu (falls vorhanden). Kopieren Sie das Artefakt aus dem Artefakt-Repository in den AWS IoT Greengrass	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Artefakt-Bucket. Erstellen oder aktualisieren Sie dann Ihre AWS IoT Greengrass-Komponente. • Fügen Sie den MQTT-Broker als Komponente hinzu oder fügen Sie ihn später manuell hinzu. Hinweis: Diese Entscheidung wirkt sich auf das Authentifizierungsschema aus, das Sie mit dem Broker verwenden können. Das manuelle Hinzufügen eines Brokers entkoppelt den Broker von AWS IoT Greengrass und aktiviert jedes unterstützte Authentifizierungsschema des Brokers. Die von AWS bereitgestellten Broker-Komponenten haben vordefinierte Authentifizierungsschemata. Weitere Informationen finden Sie unter MQTT-3.1.1-Broker (Moquette) und MQTT-5-Broker (EMQX).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den MQTT-Client.	Der Beispielcode verwendet keine Authentifizierung, da die Komponente lokal eine Verbindung zum Broker herstellt. Wenn sich Ihr Szenario unterscheidet, aktualisieren Sie den Abschnitt MQTT-Client nach Bedarf. Führen Sie außerdem die folgenden Schritte aus: 1. Aktualisieren Sie die MQTT-Themen im Abonnement. 2. Aktualisieren Sie den MQTT-Nachrichtenparser nach Bedarf, da sich Nachrichten aus jeder Quelle unterscheiden können.	App-Developer

Hinzufügen der Komponente zum AWS IoT Greengrass Version 2 Core-Gerät

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Bereitstellung des Core-Geräts.	Wenn die Bereitstellung des AWS IoT Greengrass Version 2 Core-Geräts bereits vorhanden ist, ändern Sie die Bereitstellung . Wenn die Bereitstellung nicht vorhanden ist, erstellen Sie eine neue Bereitstellung .	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um der Komponente den richtigen Namen zu geben, aktualisieren Sie die Protokoll manager-Konfiguration für die neue Komponente (falls erforderlich) basierend auf den folgenden Schritten: `{ "logsUploaderConfiguration": { "systemLogsConfiguration": { ... }, "componentLogsConfigurationMap": { "<com.iot.ingest.parquet>": { "minimumLogLevel": "INFO", "diskSpaceLimit": "20", "diskSpaceLimitUnit": "MB", "deleteLogFileAfterCloudUpload": "false" } ... } }, "periodicUploadIntervalSec": "300" }` Schließen Sie abschließend die Revision der Bereitstellung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für Ihr AWS IoT Greengrass-Kerngerät ab.	

Überprüfen der Datenaufnahme in den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokolle für das AWS IoT Greengrass-Volume.	Überprüfen Sie Folgendes: • Der MQTT-Client ist erfolgreich mit dem lokalen MQTT-Broker verbunden. • Der MQTT-Client hat die richtigen Themen abonniert. • Meldungen zur Sensorakt ualisierung werden an den Broker zu den MQTT-Them en gesendet. • Die Parquet-Komprimierung erfolgt in jedem periodisc hen Intervall.	App-Developer
Überprüfen Sie den S3-Bucket .	Überprüfen Sie, ob die Daten in den S3-Bucket hochgelad en werden. Sie können die Dateien, die hochgeladen werden, in jedem Zeitraum sehen. Sie können auch überprüfen, ob die Daten in den S3-Bucket hochgeladen werden, indem Sie die Daten im nächsten Abschnitt abfragen.	App-Developer

Einrichten der Abfrage von Athena

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenbank und eine Tabelle.	1. Erstellen Sie eine AWS Glue-Datenbank (falls erforderlich). 2. Erstellen Sie manuell eine Tabelle in AWS Glue https://docs.aws.amazon.com/glue/latest/dg/tables-described.html oder indem Sie einen Acrawler in AWS Glue ausführen.	App-Developer
Gewähren Sie Athena Zugriff auf die Daten.	1. Aktualisieren Sie die Berechtigungen, damit Athena auf den S3-Bucket zugreifen kann. Weitere Informationen finden Sie unter Differenzierter Zugriff auf Datenbanken und Tabellen im AWS Glue Data Catalog in der Athena-Dokumentation. 2. Fragen Sie die Tabelle in Ihrer Datenbank ab.	App-Developer

Fehlerbehebung

Problem	Lösung
Der MQTT-Client kann keine Verbindung herstellen	• Validieren Sie die Berechtigungen für den MQTT-Broker. Wenn Sie einen MQTT-Broker von AWS haben, finden Sie weitere Informati

Problem	Lösung
	onen unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX). • Validieren Sie die Anmeldeinformationen auf dem MQTT-Client. Wenn Sie einen MQTT-Broker von AWS haben, finden Sie weitere Informationen unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX).
MQTT-Client kann nicht abonniert werden	Validieren Sie die Berechtigungen für den MQTT-Broker. Wenn Sie einen MQTT-Broker von AWS haben, finden Sie weitere Informati onen unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX).
Parquet-Dateien werden nicht erstellt	• Überprüfen Sie, ob die MQTT-Themen korrekt sind. • Stellen Sie sicher, dass die MQTT-Nach richten von den Sensoren das richtige Format haben.
Objekte werden nicht in den S3-Bucket hochgeladen	• Stellen Sie sicher, dass Sie über Internetk onnektivität und Endpunktkonnektivität verfügen. • Überprüfen Sie, ob die Ressourcenrichtlinie für Ihren S3-Bucket korrekt ist. • Überprüfen Sie die Berechtigungen für die AWS IoT Greengrass Version 2 Core-Gerä terolle.

Zugehörige Ressourcen

- DataFrame (P Bols-Dokumentation)
- Apache Parquet-Dokumentation (Parquet-Dokumentation)

- Entwickeln von AWS IoT Greengrass-Komponenten (AWS IoT Greengrass Developer Guide, Version 2)
- Bereitstellen von AWS IoT Greengrass-Komponenten auf Geräten (AWS IoT Greengrass Developer Guide, Version 2)
- Interagieren mit lokalen IoT-Geräten (AWS IoT Greengrass Developer Guide, Version 2)
- MQTT 3.1.1 Broker (Moquette) (AWS IoT Greengrass-Entwicklerhandbuch, Version 2)
- MQTT 5 Broker (EMQX) (AWS IoT Greengrass-Entwicklerhandbuch, Version 2)

Zusätzliche Informationen

Kostenanalyse

Das folgende Kostenanalyseszenario zeigt, wie sich der in diesem Muster behandelte Ansatz zur Datenaufnahme auf die Datenaufnahmekosten in der AWS Cloud auswirken kann. Die Preisbeispiele in diesem Szenario basieren auf den Preisen zum Zeitpunkt der Veröffentlichung. Die Preise sind freibleibend. Darüber hinaus können Ihre Kosten je nach AWS-Region, AWS-Servicekontingenten und anderen Faktoren im Zusammenhang mit Ihrer Cloud-Umgebung variieren.

Eingabesignalsatz

Diese Analyse verwendet den folgenden Satz von Eingabesignalen als Grundlage für den Vergleich der IoT-Aufnahmekosten mit anderen verfügbaren Alternativen.

Anzahl der Signale	Frequency (Frequenz)	Daten pro Signal
125	25 Hz	8 Bytes

In diesem Szenario empfängt das System 125 Signale. Jedes Signal beträgt 8 Byte und tritt alle 40 Millisekunden (25 Hz) auf. Diese Signale können einzeln oder in einer gemeinsamen Nutzlast gruppiert sein. Sie haben die Möglichkeit, diese Signale je nach Bedarf aufzuteilen und zu packen. Sie können auch die Latenz bestimmen. Latenz besteht aus dem Zeitraum für den Empfang, das Ansammeln und die Aufnahme der Daten.

Zu Vergleichszwecken basiert der Aufnahmevorgang für dieses Szenario in der `us-east-1` AWS-Region. Der Kostenvergleich gilt nur für AWS-Services. Andere Kosten, wie Hardware oder Konnektivität, werden bei der Analyse nicht berücksichtigt.

Kostenvergleiche

Die folgende Tabelle zeigt die monatlichen Kosten in USD (USD) für jede Aufnahmemethode.

Methode	Monatliche Kosten
AWS IoT SiteWise*	331,77 USD
AWS IoT SiteWise Edge mit Datenverarbeitungspaket (alle Daten bleiben am Edge erhalten)	200 USD
AWS IoT Core- und Amazon S3-Regeln für den Zugriff auf Rohdaten	84,54 USD
Parquet-Dateikomprimierung am Edge und Hochladen in Amazon S3	0,5 USD

*Daten müssen aussortiert werden, um die Service Quotas zu erfüllen. Das bedeutet, dass es bei dieser Methode zu Datenverlusten kommt.

Alternative Methoden

Dieser Abschnitt zeigt die entsprechenden Kosten für die folgenden alternativen Methoden:

- AWS IoT SiteWise – Jedes Signal muss in einer einzelnen Nachricht hochgeladen werden. Daher beträgt die Gesamtzahl der Nachrichten pro Monat 125×25×3600×24×30 oder 8,1 Milliarden Nachrichten pro Monat. AWS IoT SiteWise kann jedoch nur 10 Datenpunkte pro Sekunde und Eigenschaft verarbeiten. Unter der Annahme, dass die Daten auf 10 Hz herabgestuft werden, wird die Anzahl der Nachrichten pro Monat auf 125 × 10 × 3600 × 24 × 30 oder 3,24 Milliarden reduziert. Wenn Sie die Herausgeberkomponente verwenden, die Messungen in Gruppen von 10 (bei 1 USD pro Million Nachrichten) verpackt, erhalten Sie monatliche Kosten von 324 USD pro Monat. Angenommen, jede Nachricht hat 8 Byte (1 KB/125), d. h. 25,92 GB Datenspeicher. Dadurch fallen monatliche Kosten von 7,77 USD pro Monat an. Die Gesamtkosten für den ersten Monat betragen 331,77 USD und steigen jeden Monat um 7,77 USD.
- AWS IoT SiteWise Edge mit Datenverarbeitungspaket, einschließlich aller Modelle und Signale, die am Edge vollständig verarbeitet werden (d. h. keine Cloud-Erfassung) – Sie können das Datenverarbeitungspaket als Alternative verwenden, um die Kosten zu senken und alle Modelle

zu konfigurieren, die am Edge berechnet werden. Dies kann nur für die Speicherung und Visualisierung funktionieren, auch wenn keine echte Berechnung durchgeführt wird. In diesem Fall ist es erforderlich, leistungsstarke Hardware für das Edge-Gateway zu verwenden. Es fallen Fixkosten von 200 USD pro Monat an.

- Direkte Aufnahme in AWS IoT Core durch MQTT und eine IoT-Regel zum Speichern der Rohdaten in Amazon S3 – Unter der Annahme, dass alle Signale in einer gemeinsamen Nutzlast veröffentlicht werden, beträgt die Gesamtzahl der in AWS IoT Core veröffentlichten Nachrichten 25×3600×24×30 oder 64,8 Millionen pro Monat. Bei 1 USD pro Million Nachrichten entspricht dies einem monatlichen Preis von 64,8 USD pro Monat. Bei 0,15 USD pro Million Regelaktivierungen und mit einer Regel pro Nachricht, die monatliche Kosten von 19,44 USD pro Monat hinzufügt. Für Kosten von 0,023 USD pro GB Speicher in Amazon S3, wodurch weitere 1,5 USD pro Monat hinzugefügt werden (zunahme jeden Monat, um die neuen Daten widerzuspiegeln). Die Gesamtkosten für den ersten Monat betragen 84,54 USD und steigen jeden Monat um 1,5 USD.
- Komprimieren von Daten am Edge in einer Parquet-Datei und Hochladen in Amazon S3 (vorgeschlagene Methode) – Das Komprimierungsverhältnis hängt von der Art der Daten ab. Wenn dieselben industriellen Daten für MQTT getestet wurden, betragen die Gesamtausgabedaten für einen ganzen Monat 1,2 GB. Dies kostet 0,03 USD pro Monat. Die in anderen Benchmarks beschriebenen Komprimierungsraten (mit Zufallsdaten) liegen in der Reihenfolge von 66 Prozent (naher an einem Worst-Case-Szenario). Die Gesamtdaten betragen 21 GB und kosten 0,5 USD pro Monat.

Parquet-Dateigenerator

Das folgende Codebeispiel zeigt die Struktur eines Parquet-Dateigenerators, der in Python geschrieben ist. Das Codebeispiel dient nur zur Veranschaulichung und funktioniert nicht, wenn es in Ihre Umgebung eingefügt wird.

```
import queue
import paho.mqtt.client as mqtt
import pandas as pd

#queue for decoupling the MQTT thread
messageQueue = queue.Queue()
client = mqtt.Client()
streammanager = StreamManagerClient()

def feederListener(topic, message):
    payload = {
```

```
        "topic" : topic,
        "payload" : message,
    }
    messageQueue.put_nowait(payload)

def on_connect(client_instance, userdata, flags, rc):
    client.subscribe("#",qos=0)

def on_message(client, userdata, message):
    feederListener(topic=str(message.topic),
 message=str(message.payload.decode("utf-8")))


filename = "tempfile.parquet"
streamname = "mystream"
destination_bucket= "mybucket"
keyname="mykey"
period= 60

client.on_connect = on_connect
client.on_message = on_message
streammanager.create_message_stream(
            MessageStreamDefinition(name=streamname,
 strategy_on_full=StrategyOnFull.OverwriteOldestData)
        )


while True:
   try:
       message = messageQueue.get(timeout=myArgs.mqtt_timeout)
   except (queue.Empty):
       logger.warning("MQTT message reception timed out")

   currentTimestamp = getCurrentTime()
   if currentTimestamp >= nextUploadTimestamp:
       df = pd.DataFrame.from_dict(accumulator)
       df.to_parquet(filename)
       s3_export_task_definition = S3ExportTaskDefinition(input_url=filename,
 bucket=destination_bucket, key=key_name)
       streammanager.append_message(streamname,
 Util.validate_and_serialize_to_json_bytes(s3_export_task_definition))
       accumulator = {}
       nextUploadTimestamp += period
   else:
```

```
        accumulator.append(message)
```

Migrieren Sie Hadoop-Daten mithilfe von LiveData WANdisco Migrator zu Amazon S3

Quelle: Lokaler Hadoop-Cluster	Ziel: Amazon S3	R-Typ: Rehost
Umgebung: Produktion	Technologien: Datenseen; Große Datenmengen; Hybrid-Cloud; Migration	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon S3		

Übersicht

Dieses Muster beschreibt den Prozess für die Migration von Apache Hadoop-Daten von einem Hadoop Distributed File System (HDFS) zu Amazon Simple Storage Service (Amazon S3). Es verwendet WANdisco LiveData Migrator, um den Datenmigrationsprozess zu automatisieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Hadoop-Cluster-Edge-Knoten, auf dem LiveData Migrator installiert wird. Der Knoten sollte die folgenden Anforderungen erfüllen:
  - Mindestspezifikation: 4 CPUs, 16 GB RAM, 100 GB Speicher.
  - Netzwerk mit mindestens 2 Gbit/s.
  - Port 8081, auf den auf Ihrem Edge-Knoten zugegriffen werden kann, um auf die WANdisco-Benutzeroberfläche zuzugreifen.
  - Java 1.8 64-Bit.
  - Auf dem Edge-Knoten installierte Hadoop-Clientbibliotheken.
  - Möglichkeit, sich als HDFS-Superuser zu authentifizieren (z. B. „hdfs“).
  - Wenn Kerberos auf Ihrem Hadoop-Cluster aktiviert ist, muss auf dem Edge-Knoten ein gültiger Keytab verfügbar sein, der einen geeigneten Principal für den HDFS-Superuser enthält.
  - Eine Liste der unterstützten Betriebssysteme finden Sie in den Versionshinweisen.

- Ein aktives AWS-Konto mit Zugriff auf einen S3-Bucket.
- Eine AWS Direct Connect, die zwischen Ihrem lokalen Hadoop-Cluster (insbesondere dem Edge-Knoten) und AWS hergestellt wird.

Produktversionen

- LiveData Migrator 1.8.6
- WANDisco-Benutzeroberfläche (eine Benutzeroberfläche) 5.8.0

Architektur

Quelltechnologie-Stack

- Lokaler Hadoop-Cluster

Zieltechnologie-Stack

- Amazon S3

Architektur

Das folgende Diagramm zeigt die Architektur der LiveData Migrator-Lösung.

Der Workflow besteht aus vier Hauptkomponenten für die Datenmigration von lokalem HDFS zu Amazon S3.

- LiveData Migrator — Automatisiert die Migration von Daten von HDFS zu Amazon S3 und befindet sich auf einem Edge-Knoten des Hadoop-Clusters.
- HDFS — Ein verteiltes Dateisystem, das Zugriff auf Anwendungsdaten mit hohem Durchsatz ermöglicht.
- Amazon S3 — Ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.
- AWS Direct Connect — Ein Service, der eine dedizierte Netzwerkverbindung von Ihren lokalen Rechenzentren zu AWS herstellt.

Automatisierung und Skalierung

In der Regel erstellen Sie mehrere Migrationen, sodass Sie bestimmte Inhalte aus Ihrem Quelldateisystem nach Pfad oder Verzeichnis auswählen können. Sie können Daten auch in mehrere unabhängige Dateisysteme gleichzeitig migrieren, indem Sie mehrere Migrationsressourcen definieren.

Epen

Amazon S3 S3-Speicher in Ihrem AWS-Konto konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei Ihrem AWS-Konto an.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3.	AWS-Erfahrung
Erstellen Sie einen S3-Bucket.	Wenn Sie noch keinen vorhandenen S3-Bucket haben, den Sie als Zielspeicher verwenden können, wählen Sie in der Amazon S3 S3-Konsole die Option „Bucket erstellen“ und geben Sie einen Bucket-Namen, eine AWS-Region und Bucket-Einstellungen für den Block Public Access an. AWS und WANdisco empfehlen, dass Sie die Optionen zum Blockieren des öffentlichen Zugriffs für den S3-Bucket aktivieren und die Richtlinien für den Bucket-Zugriff und die Benutzerberechtigungen	AWS-Erfahrung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	so einrichten, dass sie den Anforderungen Ihrer Organisation entsprechen. Ein AWS-Beispiel finden Sie unter https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example1.html.	

Installieren Sie LiveData Migrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das LiveData Migrator-Installationsprogramm herunter.	Laden Sie das LiveData Migrator-Installationsprogramm herunter und laden Sie es auf den Hadoop Edge-Knoten hoch. Sie können eine kostenlose Testversion von LiveData Migrator unter https://www2.wandisco.com/ldm-trial herunterladen. Zugriff auf LiveData Migrator erhalten Sie auch über den AWS Marketplace unter https://aws.amazon.com/marketplace/pp/B07B8SZND9.	Hadoop-Administrator, Besitzer der Anwendung
Installieren Sie LiveData Migrator.	Verwenden Sie das heruntergeladene Installationsprogramm und installieren Sie LiveData Migrator als HDFS-Superuser auf einem Edge-Knoten in Ihrem Hadoop-Cluster. Die Installationsbefehle finden	Hadoop-Administrator, Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie im Abschnitt „Zusätzliche Informationen“.	
Überprüfen Sie den Status von LiveData Migrator und anderen Diensten.	Überprüfen Sie den Status von LiveData Migrator, Hive Migrator und WANdisco UI mithilfe der Befehle im Abschnitt „Zusätzliche Informationen“.	Hadoop-Administrator, Besitzer der Anwendung

Konfigurieren Sie den Speicher über die WANdisco-Benutzeroberfläche

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie Ihr LiveData Migrator-Konto.	Melden Sie sich über einen Webbrowser auf Port 8081 (auf dem Hadoop-Edge-Knoten) bei der WANdisco-Benutzeroberfläche an und geben Sie Ihre Daten für die Registrierung ein. Wenn Sie LiveData Migrator beispielsweise auf einem Host namens myldmhost.example.com ausführen, lautet die URL: http://myldmhost.example.com:8081	Besitzer der Anwendung
Konfigurieren Sie Ihren HDFS-Quellspeicher.	Geben Sie die Konfigurationsdetails an, die für Ihren HDFS-Quellspeicher erforderlich sind. Dazu gehören der Wert „fs.defaultFS“ und ein benutzerdefinierter Speichername. Wenn	Hadoop-Administrator, Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kerberos aktiviert ist, geben Sie den Principal- und den Keytab-Speicherort an, den Migrator verwenden soll. LiveData Wenn NameNode HA auf dem Cluster aktiviert ist, geben Sie einen Pfad zu den Dateien core-site.xml und hdfs-site.xml auf dem Edge-Knoten an.	
Konfigurieren Sie Ihren Amazon S3 S3-Zielspeicher.	Fügen Sie Ihren Zielspeicher als Typ S3a hinzu. Geben Sie den benutzerdefinierten Speichernamen und den S3-Bucket-Namen an. Geben Sie „org.apache.hadoop.fs.s3a.simpleAWSCredentialsProvider“ für die Option Credentials Provider ein und geben Sie den AWS-Zugriff und die geheimen Schlüssel für den S3-Bucket ein. Zusätzliche S3a-Eigenschaften werden ebenfalls benötigt. Einzelheiten finden Sie im Abschnitt „S3a-Eigenschaften“ in der LiveData Migrator-Dokumentation unter https://docs.wandisco.com/live-data-migrator/docs/command-reference/#filesystem-add-s3a.	AWS, Inhaber der Anwendung

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Ausnahmen hinzu (falls erforderlich).	Wenn Sie bestimmte Datensätze von der Migration ausschließen möchten, fügen Sie Ausnahmen für den HDFS-Quellspeicher hinzu. Diese Ausnahmen können auf der Dateigröße, den Dateinamen (basierend auf Regex-Mustern) und dem Änderungsdatum basieren.	Hadoop-Administrator, Besitzer der Anwendung

Erstellen und starten Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie die Migration.	Erstellen Sie eine Migration im Dashboard der WANdisco-Benutzeroberfläche. Wählen Sie Ihre Quelle (HDFS) und Ihr Ziel (den S3-Bucket). Fügen Sie neue Ausnahmen hinzu, die Sie im vorherigen Schritt definiert haben. Wählen Sie entweder die Option „Überschreiben“ oder die Option „Überspringen, wenn die Größe übereinstimmt“. Erstellen Sie die Migration, wenn alle Felder vollständig sind.	Hadoop-Administrator, Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Migration.	Wählen Sie im Dashboard die Migration aus, die Sie erstellt haben. Klicken Sie hier, um die Migration zu starten. Sie können eine Migration auch automatisch starten, indem Sie bei der Erstellung der Migration die Option Autostart auswählen.	Besitzer der Anwendung

Bandbreite verwalten (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie ein Netzwerkb andbreitenlimit zwischen Quelle und Ziel fest.	Wählen Sie in der Speicherl iste auf dem Dashboard Ihren Quellspeicher aus und wählen Sie in der Gruppierungsliste „Bandbreitenverwaltung“ aus. Deaktivieren Sie die Option „Unbegrenzt“ und definieren Sie das maximale Bandbreit enlimit und die maximale Bandbreiteneinheit. Wählen Sie „Anwenden“.	Inhaber der Anwendung, Netzwerk

Überwachen und verwalten Sie Migrationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie Migrationsinformat ionen mithilfe der WANdisco-Benutzeroberfläche an.	Verwenden Sie die WANdisco-Benutzeroberfläche, um Lizenz-, Bandbreiten-,	Hadoop-Administrator, Anwendungsbesitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Speicher- und Migration sinformationen anzuzeige n. Die Benutzeroberfläche bietet auch ein Benachric htigungssystem, sodass Sie Benachrichtigungen über Fehler, Warnungen oder wichtige Meilensteine Ihrer Nutzung erhalten können.	
Migrationen beenden, fortsetzen und löschen.	Sie können verhindern, dass bei einer Migration Inhalte an das Ziel übertragen werden, indem Sie sie in den Status STOPPED versetzen . Gestoppte Migrationen können wieder aufgenomm en werden. Migrationen im Status STOPPED können auch gelöscht werden.	Hadoop-Administrator, Besitzer der Anwendung

Zugehörige Ressourcen

- LiveData Migrator-Dokumentation
- LiveData Migrator im AWS Marketplace
- WanDisco-Support-Community
- Vorführung von WANdisco LiveData Migrator (Video)

Zusätzliche Informationen

Installation von Migrator LiveData

Sie können LiveData Migrator mit den folgenden Befehlen installieren, vorausgesetzt, das Installationsprogramm befindet sich in Ihrem Arbeitsverzeichnis:

```
su - hdfs
chmod +x livedata-migrator.sh && sudo ./livedata-migrator.sh
```

Überprüfen Sie den Status von LiveData Migrator und anderen Diensten nach der Installation

Verwenden Sie die folgenden Befehle, um den Status von LiveData Migrator, Hive Migrator und WANdisco UI zu überprüfen:

```
service livedata-migrator status
service hivemigrator status
service livedata-ui status
```

Mehr Muster

- Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden
- ???
- Sicherstellen, dass ein Amazon-Redshift-Cluster bei der Erstellung verschlüsselt wird
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Migrieren von Daten in die AWS Cloud mithilfe von Starburst
- Optimieren Sie die ETL-Erfassung der Eingabedateigröße auf AWS
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- ???
- Übertragen Sie umfangreiche Db2-z/OS-Daten in CSV-Dateien an Amazon S3
- Stellen Sie sicher, dass neue Amazon-Redshift-Cluster über erforderliche SSL-Endpunkte verfügen
- Visualisieren von Amazon-Redshift-Prüfungsprotokollen mit Amazon Athena und Amazon QuickSight

Datenbanken

Themen

- Verarbeiten überlasteter Oracle-Funktionen in Aurora PostgreSQL – kompatibel
- Helfen Sie mit, DynamoDB-Tagging durchzusetzen
- Implementieren Sie regionsübergreifende Notfallwiederherstellung mit AWS DMS und Amazon Aurora
- Migrieren von Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten zu PostgreSQL
- Migrieren von DB-Instances von Amazon RDS für Oracle zu anderen Konten, die AMS verwenden
- Migrieren von Oracle-OUT-Bindungsvariablen in eine PostgreSQL-Datenbank
- Migrieren Sie SAP HANA zu AWS mithilfe von SAP HSR mit demselben Hostnamen
- Migrieren von SQL Server zu AWS mithilfe verteilter Verfügbarkeitsgruppen
- Migrieren von Oracle 8i oder 9i zu Amazon RDS für Oracle mit SharePlex und AWS DMS
- Überwachen von Amazon Aurora auf Instances ohne Verschlüsselung
- Überwachen von Oracle- GoldenGate Protokollen mithilfe von Amazon CloudWatch
- Plattformwechsel von Oracle Database Enterprise Edition auf Standard Edition 2 auf Amazon RDS für Oracle
- Replizieren von Mainframe-Datenbanken in AWS mithilfe von Precisely Connect
- Planen von Aufträgen für Amazon RDS for PostgreSQL und Aurora PostgreSQL mithilfe von Lambda und Secrets Manager
- Sichern und optimieren Sie den Benutzerzugriff in einer Db2-Verbunddatenbank in AWS mithilfe vertrauenswürdiger Kontexte
- Senden von Benachrichtigungen für eine Datenbank-Instance von Amazon RDS für SQL Server mithilfe eines On-Premises-SMTP-Servers und Database Mail
- Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten
- Einrichten einer HA/DR-Architektur für Oracle E-Business Suite in Amazon RDS Custom mit einer aktiven Standby-Datenbank
- Einrichten der Datenreplikation zwischen Amazon RDS für MySQL und MySQL auf Amazon EC2 mithilfe von GTID
- Übergangsrollen für eine Oracle- PeopleSoft Anwendung in Amazon RDS Custom für Oracle
- Datenbankmigrationsmuster nach Workload
- Mehr Muster

Zugriff auf lokale Microsoft SQL Server-Tabellen von Microsoft SQL Server auf Amazon EC2 über verknüpfte Server

Erstellt von Tirumala Dasari (AWS) und Eduardoentim (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken	Workload: Microsoft

Übersicht

Dieses Muster beschreibt den Zugriff auf lokale Microsoft SQL Server-Datenbanktabellen, die unter Microsoft Windows ausgeführt werden, von Microsoft SQL Server-Datenbanken, die auf Amazon Elastic Compute Cloud (Amazon EC2)-Windows- oder Linux-Instances ausgeführt oder gehostet werden, mithilfe verknüpfter Server.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon EC2 mit Microsoft SQL Server auf Amazon Linux AMI (Amazon Machine Image)
- AWS Direct Connect zwischen dem lokalen Microsoft SQL Server (Windows)-Server und der Windows- oder Linux EC2-Instance

Produktversionen

- SQL Server 2016 oder höher

Architektur

Quelltechnologie-Stack

- On-Premises Microsoft SQL Server-Datenbank unter Windows
- Amazon EC2 mit Microsoft SQL Server unter Windows AMI oder Linux AMI

Zieltechnologie-Stack

- Amazon EC2 mit Microsoft SQL Server unter Amazon Linux AMI
- Amazon EC2 mit Microsoft SQL Server unter Windows AMI

Quell- und Zieldatenbankarchitektur

Tools

- Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung einer SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Polen

Ändern des Authentifizierungsmodus in Windows für SQL Server in Windows SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über SSMS eine Verbindung zu Windows SQL Server her.		DBA
Ändern Sie den Authentif izierungsmodus in SQL Server über das Kontextmenü (rechte Maustaste) für die Windows SQL Server-Instance in Windows.		DBA

Starten Sie den Windows-MSSQL-Service neu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den SQL-Service neu.	1. Wählen Sie im SSMS Object Explorer die SQL Server-Instance aus. 2. Öffnen Sie das Kontextmenü (rechte Maustaste). 3. Wählen Sie Neustart aus.	DBA

Erstellen Sie eine neue Anmeldung und wählen Sie Datenbanken aus, auf die in Windows SQL Server zugegriffen werden soll

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie auf der Registerkarte Sicherheit das Kontextmenü (rechte Maustaste) für Anmeldung und wählen Sie eine neue Anmeldung aus.		DBA
Wählen Sie auf der Registerkarte Allgemein die Option SQL Server-Authentifizierung aus, geben Sie einen Benutzernamen ein, geben Sie das Passwort ein, bestätigen Sie dann das Passwort und deaktivieren Sie die Option zum Ändern des Passworts bei der nächsten Anmeldung.		DBA
Wählen Sie auf der Registerkarte Serverrollen die Option Öffentlich aus.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie auf der Registerkarte Benutzerzuordnung die Datenbank und das Schema aus, auf die Sie zugreifen möchten, und markieren Sie dann die Datenbank, um Datenbankrollen auszuwählen.	Wählen Sie public und db_datareader aus, um auf Daten aus den Datenbanktabellen zuzugreifen.	DBA
Wählen Sie OK, um einen Benutzer zu erstellen.		DBA

Hinzufügen von Windows SQL Server-IP zur Linux SQL Server-Hostdatei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über das Terminalfenster eine Verbindung mit dem Linux SQL Server-Feldher.		DBA
Öffnen Sie die Datei /etc/hosts und fügen Sie die IP-Adresse des Windows-Computers mit SQL Server hinzu.		DBA
Speichern Sie die Hosts-Datei.		DBA

Erstellen eines verknüpften Servers auf Linux SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen verknüpften Server mithilfe der gespeicherten Prozeduren	Weitere Informationen zur Verwendung dieser gespeicherten Prozeduren finden Sie im	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
master.sys.sp_addlinkedserver und master.dbo.sp_addlinkedsrvlogin.	Abschnitt Zusätzliche Informationen.	

Überprüfen des erstellten verknüpften Servers und der Datenbanken in SSMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie in Linux SQL Server in SSMS zu Verknüpfte Server und aktualisieren Sie .		DBA
Erweitern Sie die erstellten verknüpften Server und Kataloge im linken Bereich.	Sie sehen die ausgewählten SQL Server-Datenbanken mit Tabellen und Ansichten.	DBA

Stellen Sie sicher, dass Sie auf Windows SQL Server-Datenbanktabellen zugreifen können

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie im SSMS-Abfragefenster die Abfrage aus: „Wählen Sie die Top 3 * aus [sqllin].dms_sample_win.dbo.mlb_data“.	Beachten Sie, dass die FROM-Klausel eine vierteilige Syntax verwendet: computer.database.schema.table (z. B. SELECT-Name „SQL2 databases“ FROM [sqllin].master.sys.databases). In unserem Beispiel haben wir einen Alias für SQL2 in der Hosts-Datei erstellt, sodass Sie den tatsächlichen NetBIOS-Namen nicht zwischen den eckigen Klammern eingeben müssen.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie die tatsächlichen NetBIOS-Namen verwenden , beachten Sie, dass AWS standardmäßig NetBIOS-N amen wie Win-xxxx verwendet und SQL Server eckige Klammern für Namen mit Bindestrichen erfordert.	

Zugehörige Ressourcen

- Versionshinweise für SQL Server unter Linux

Zusätzliche Informationen

Verwenden von gespeicherten Prozeduren zum Erstellen von verknüpften Servern

SSMS unterstützt die Erstellung verknüpfter Server für Linux SQL Server nicht, daher müssen Sie diese gespeicherten Prozeduren verwenden, um sie zu erstellen:

```
EXEC master.sys.sp_addlinkedserver @server= N'SQLLIN' , @srvproduct= N'SQL Server'
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'SQLLIN',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassword='Te
```

Hinweis 1: Geben Sie die Anmeldeinformationen ein, die Sie zuvor in Windows SQL Server in der gespeicherten Prozedur erstellt haben`master.dbo.sp_addlinkedsrvlogin`.

Hinweis 2: `@server` Name `SQLLIN` und Name des Hostdateieintrags `172.12.12.4 SQLLIN` sollten identisch sein.

Sie können diesen Prozess verwenden, um verknüpfte Server für die folgenden Szenarien zu erstellen:

- Linux SQL Server mit Windows SQL Server über einen verknüpften Server (wie in diesem Muster angegeben)

- Windows SQL Server mit Linux SQL Server über einen verknüpften Server
- Linux SQL Server mit einem anderen Linux SQL Server über einen verknüpften Server

Hinzufügen von HA zu Oracle PeopleSoft auf Amazon RDS Custom mithilfe eines Lesereplikats

Erstellt von Sampath Kathirvel (AWS)

Umgebung: Produktion	Technologien: Datenbanken; Infrastruktur	Workload: Oracle
AWS-Services: Amazon RDS		

Übersicht

Um die Enterprise PeopleSoft Resource Planning (ERP)-Lösung von Oracle auf Amazon Web Services (AWS) auszuführen, können Sie Amazon Relational Database Service (Amazon RDS) oder Amazon RDS Custom für Oracle verwenden, das veraltete, benutzerdefinierte und verpackte Anwendungen unterstützt, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Wichtige Faktoren, die Sie bei der Planung einer Migration berücksichtigen sollten, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Ab diesem Schreiben unterstützt RDS Custom für Oracle nicht die Multi-AZ-Option, die für Amazon RDS für Oracle als HA-Lösung mit Speicherreplikation verfügbar ist. Stattdessen erreicht dieses Muster HA durch die Verwendung einer Standby-Datenbank, die eine physische Kopie der Primärdatenbank erstellt und verwaltet. Das Muster konzentriert sich auf die Schritte zum Ausführen einer PeopleSoft Anwendungsdatenbank auf Amazon RDS Custom mit HA, indem Oracle Data Guard verwendet wird, um ein Lesereplikat einzurichten.

Dieses Muster ändert auch das Lesereplikat in den schreibgeschützten Modus. Wenn sich Ihr Lesereplikat im schreibgeschützten Modus befindet, bietet dies zusätzliche Vorteile:

- Auslagern von schreibgeschützten Workloads aus der Primärdatenbank
- Aktivieren der automatischen Reparatur beschädigter Blöcke durch Abrufen fehlerfreier Blöcke aus der Standby-Datenbank mithilfe der Oracle Active Data Guard-Funktion
- Verwenden der Far Sync-Funktion, um die Remote-Standby-Datenbank synchron zu halten, ohne den Leistungsaufwand, der mit der Redo-Log-Übertragung über große Entfernungen verbunden ist.

Für die Verwendung eines Replikats im schreibgeschützten Modus ist die Option Oracle Active Data Guard erforderlich, die mit zusätzlichen Kosten verbunden ist, da es sich um eine separat lizenzierte Funktion von Oracle Database Enterprise Edition handelt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene PeopleSoft Anwendung auf Amazon RDS Custom. Wenn Sie keine Anwendung haben, lesen Sie das Muster Migrieren von Oracle PeopleSoft zu Amazon RDS Custom .
- Eine einzelne PeopleSoft Anwendungsebene. Sie können dieses Muster jedoch so anpassen, dass es mit mehreren Anwendungsebenen funktioniert.
- Amazon RDS Custom ist mit mindestens 8 GB Auslagerungsbereich konfiguriert.
- Eine Oracle Active Data Guard-Datenbanklizenz zum Konvertieren des Lesereplikats in den schreibgeschützten Modus und zum Auslagern von Berichtsaufgaben in den Standby-Modus. Weitere Informationen finden Sie in der kommerziellen Preisliste von Oracle Technology.

Einschränkungen

- Allgemeine Einschränkungen und nicht unterstützte Konfigurationen für RDS Custom für Oracle
- Einschränkungen im Zusammenhang mit Lesereplikaten von Amazon RDS Custom für Oracle

Produktversionen

- Informationen zu Oracle-Database-Versionen, die von Amazon RDS Custom unterstützt werden, finden Sie unter RDS Custom für Oracle.
- Informationen zu Oracle-Database-Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Unterstützung von DB-Instance-Klassen für RDS Custom für Oracle.

Architektur

Zieltechnologie-Stack

- Amazon RDS Custom für Oracle
- AWS Secrets Manager
- Oracle Active Data Guard

- Oracle- PeopleSoft Anwendung

Zielarchitektur

Das folgende Diagramm zeigt eine Amazon RDS Custom DB-Instance und ein Amazon RDS Custom Read Replica. Das Lesereplikat verwendet Oracle Active Data Guard, um in eine andere Availability Zone zu replizieren. Sie können das Lesereplikat auch verwenden, um Lesedatenverkehr in der Primärdatenbank auszulagern und zu Berichtszwecken.

Eine repräsentative Architektur mit Oracle PeopleSoft in AWS finden Sie unter Einrichten einer hochverfügbaren PeopleSoft Architektur in AWS .

Tools

AWS-Services

- Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen. In diesem Muster rufen Sie die Datenbankbenutzerpasswörter von Secrets Manager für `RDS_DATAGUARD` mit dem Secret-Namen `abdo-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Andere Tools

- Oracle Data Guard unterstützt Sie beim Erstellen, Verwalten und Überwachen von Standby-Datenbanken.

Bewährte Methoden

Um auf ein Ziel ohne Datenverlust (RPO=0) hinzuarbeiten, verwenden Sie den `MaxAvailability` Data-Guard-Schutzmodus mit der Redo-`SYNC+NOAFFIRM`Transporteinstellung für eine bessere Leistung. Weitere Informationen zur Auswahl des Datenbankschutzmodus finden Sie im Abschnitt Zusätzliche Informationen.

Polen

Erstellen des Lesereplikats

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Lesereplikat.	Um ein Lesereplikat der Amazon RDS Custom DB-Instance zu erstellen, folgen Sie den Anweisungen in der Amazon RDS-Dokumentation und verwenden Sie die Amazon RDS Custom DB-Instance, die Sie erstellt haben (siehe Abschnitt Voraussetzungen) als Quelldatenbank. Standardmäßig wird das Amazon RDS Custom Read Replica als physischer Standby erstellt und befindet sich im aufgespielten Zustand. Dies dient dazu, die Einhaltung der Oracle Active Data Guard-Lizenz sicherzustellen. Dieses Muster enthält Code zum Einrichten einer Multi-Tenant-Container-Datenbank (CDB) oder einer Nicht-CDB-Instance.	DBA

Ändern des Oracle Data Guard-Schutzmodus in MaxAvailability

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Data-Guard-Broker-Konfiguration in der Primärdatenbank zu.	In diesem Beispiel ist das Amazon RDS Custom Read Replica `RDS_CUSTOM_ORCL_D` für die Nicht-CDB-Instance und `RDS_CUSTOM_RDSCDB_B` für die CDB-Instance bestimmt. Die Datenbanken für Nicht-CDB sind `orcl_a` (primär) und `orcl_d` (Standby). Die Datenbanknamen für CDB sind `rdscdb_a` (primär) und `rdscdb_b` (Standby). Sie können sich direkt oder über die Primärdatenbank mit dem RDS Custom Read Replica verbinden. Sie finden den Netzdienstnamen für Ihre Datenbank in der `tnsnames.ora` Datei im `$ORACLE_HOME/network/admin` Verzeichnis . RDS Custom für Oracle füllt diese Einträge automatisch für Ihre Primärdatenbank und Ihre Lesereplikate aus. Das Passwort für den `RDS_DATAGUARD` Benutzer wird in AWS Secrets Manager mit dem Secret-Namen gespeichert`do-not-de`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`lete-rds-custom-+<<RDS Resource ID>>+-dg`. Weitere Informationen zum Herstellen einer Verbindung mit einer RDS Custom Instance mithilfe des von Secrets Manager abgerufenen SSH-Schlüssels (Secure Shell) finden Sie unter Herstellen einer Verbindung mit Ihrer RDS Custom DB-Instance mithilfe von SSH.
	
	Verwenden Sie den folgenden Code, um über die Data-Guard-Befehlszeile (`dgmgrl`) auf die Oracle-Data-Guard-Brokerkonfiguration zuzugreifen.
	
	Nicht-CDB
	
	`$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 22:44:49 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Connected to "ORCL_D" Connected as SYSDG. DGMGRL> DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 11.00 KByte/s Instance(s): ORCL SUCCESS DGMGRL>	
	CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 20:24:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Connected to "RDSCDB_B " Connected as SYSDG. DGMGRL> DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Einstellung für den Protokolltransport, indem Sie vom Primärkno ten aus eine Verbindung zu CCPMGRL herstellen.	Ändern Sie den Protokoll transportmodus in `FastSync`, entsprechend der Redo-Tran sporteinstellung `SYNC+NOAF FIRM` . Um sicherzustellen, dass Sie nach dem Rollenwec hsel über gültige Einstellu ngen verfügen, ändern Sie diese sowohl für die Primärdat enbank als auch für die Standby-Datenbank.
	
	Nicht-CDB
	
	`DGMGRL>`
	`DGMGRL> edit database orcl_d set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_d LogXptMode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL> edit database orcl_a set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_a logxptmode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL>`
	
	CDB
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DGMGRL> edit database rdscdb_b set property logxptmode=fastsyn c;DGMGRL> edit database rdscdb_b set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_b LogXptMode; LogXptMode = 'fastsync' DGMGRL> edit database rdscdb_a set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_a logxptmode; LogXptMode = 'fastsync' DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie den Schutzmodus auf MaxAvailability.	Ändern Sie den Schutzmodus in , `MaxAvailability` indem Sie vom Primärknoten DGMGRL aus eine Verbindung zu herstellen.
	
	Nicht-CDB
	
	`DGMGRL> edit configuration set protection mode as maxavailability;`
	`Succeeded.`
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 38 seconds ago)`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL>	

Ändern Sie den Replikatstatus von Mount auf schreibgeschützt und aktivieren Sie „Wiederherstellung anwenden“

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Wiederherstellung für die Standby-Datenbank.	Das Lesereplikat wird standardmäßig im -MOUNTModus erstellt. Um es im schreibgeschützten Modus zu öffnen, müssen Sie zuerst die Redo-Anwendung deaktivieren, indem Sie vom Primär- oder Standby-Knoten DGMGRL aus eine Verbindung zu herstellen. Nicht-CDB DGMGRL> show database orcl_dDGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 11.00 KByte/s Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> edit database orcl_d set state=app ly-off; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- OFF Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 42 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB DGMGRL> show configura tionDGMGRL> show configuration	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	    rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 57 seconds ago)
	DGMGRL> show database
	 rdscdb_b;
	Database - rdscdb_b
	  Role:
	 PHYSICAL STANDBY
	  Intended State:
	 APPLY-ON
	  Transport Lag:
	 0 seconds (computed 1
	 second ago)
	  Apply Lag:
	 0 seconds (computed 1
	 second ago)
	  Average Apply Rate:
	 2.00 KByte/s
	  Real Time Query:
	 OFF
	  Instance(s):
	    RDSCDB
	Database Status:
	SUCCESS
	DGMGRL> edit database
	 rdscdb_b set state=app
	ly-off;
	Succeeded.
	DGMGRL> show database
	 rdscdb_b;
	Database - rdscdb_b</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>Role:
	PHYSICAL STANDBY
	Intended State:
	APPLY-OFF
	Transport Lag:
	0 seconds (computed 1
	second ago)
	Apply Lag:
	0 seconds (computed 1
	second ago)
	Average Apply Rate:
	(unknown)
	Real Time Query:
	OFF
	Instance(s):
	RDSCDB
	Database Status:
	SUCCESS</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie die Leserepli kat-Instance im schreibge schützten Modus.	Stellen Sie mithilfe des TNS-Eintrags eine Verbindung mit der Standby-Datenbank her und öffnen Sie sie im schreibgeschützten Modus, indem Sie vom Primär- oder Standby-Knoten aus eine Verbindung zu ihr herstellen. Nicht-CDB `$ sqlplus RDS_DATAG UARD@RDS_CUSTOM_OR CL_D as sysdg -bash-4.2$ sqlplus RDS_DATAGUARD@RDS_ CUSTOM_ORCL_D as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Fri Sep 30 23:00:14 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2020, Oracle. All rights reserved. Enter password: Last Successful login time: Fri Sep 30 2022 22:48:27 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.10.0.0.0 SQL> select open_mode from v$database; OPEN_MODE -------------------- MOUNTED`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> alter database open read only; Database altered. SQL> select open_mode from v$database; OPEN_MODE -------------------- READ ONLY SQL> CDB -bash-4.2$ sqlplus C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Wed Jan 11 21:14:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2022, Oracle. All rights reserved. Enter password: Last Successful login time: Wed Jan 11 2023 21:12:05 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.16.0.0.0 SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ---------- RDSCDB MOUNTED	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> alter database open read only; Database altered. SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- RDSCDB READ ONLY SQL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktivieren Sie „Wiederherstellung anwenden“ auf der Lesereplikat-Instance.	Aktivieren Sie Redo Apply auf der Lesereplikat-Instance, indem Sie DGMGRL aus dem Primär- oder Standby-Knoten verwenden.
	
	Nicht-CDB
	
	`$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 23:02:16 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`DGMGRL>`
	`edit database orcl_d set state=apply-on;`
	`DGMGRL> edit database orcl_d set state=apply-on;`
	`Succeeded.`
	`DGMGRL> show database orcl_d`
	`Database - orcl_d`
	`Role: PHYSICAL STANDBY`
	`Intended State: APPLY-ON`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 496.00 KByte/s Real Time Query: ON Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 21:21:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DGMGRL> edit database rdscdb_b set state=app ly-on; Succeeded. DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 35.00 KByte/s Real Time Query: ON Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 16.00 KByte/s Real Time Query: ON Instance(s): RDSCDB	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Database Status:`
	`SUCCESS`
	`DGMGRL>`	

Zugehörige Ressourcen

- Konfigurieren von Amazon RDS als Oracle PeopleSoft -Datenbank (AWS-Whitepaper)
- Oracle Data Guard Broker-Handbuch (Oracle-Referenzdokumentation)
- Konzepte und Administration von Data Guard (Oracle-Referenzdokumentation)

Zusätzliche Informationen

Wählen Sie Ihren Datenbankschutzmodus

Oracle Data Guard bietet drei Schutzmodi, um Ihre Data-Guard-Umgebung basierend auf Ihren Verfügbarkeits-, Schutz- und Leistungsanforderungen zu konfigurieren. In der folgenden Tabelle sind diese drei Modi zusammengefasst.

Schutzmodus	Erneute Transporteinstellung	Beschreibung
MAXIMUM QUENKANCE	`ASYNC`	Bei Transaktionen in der Primärdatenbank werden Redo-Daten asynchron übertragen und in das Standby-Datenbank-Redo-Protokoll geschrieben. Daher sind die Auswirkungen auf die Leistung minimal. `MaxPerformance` kann RPO=0 aufgrund des asynchronen Versands von Protokollen nicht angeben.

MAXIMUM-VERBINDUNG	`SYNC+AFFIRM`	Bei Transaktionen in der Primärdatenbank werden Redo-Daten synchron übertragen und in das Standby-Datenbank-Redo-Protokoll auf der Festplatte geschrieben, bevor die Transaktion bestätigt wird. Wenn die Standby-Datenbank nicht verfügbar ist, fährt sich die Primärdatenbank selbst herunter, um sicherzustellen, dass Transaktionen geschützt sind.
MAXIMUM VERFÜGBARKEIT	`SYNC+AFFIRM`	Dies ähnelt dem `-MaxProtection` Modus, es sei denn, es wird keine Bestätigung von der Standby-Datenbank empfangen. In diesem Fall funktioniert es so, als wäre es im `MaxPerformance` Modus, um die Verfügbarkeit der Primärdatenbank beizubehalten, bis es seinen Redo-Stream erneut in eine synchronisierte Standby-Datenbank schreiben kann.

`SYNC+NOAFFIRM`	Bei Transaktionen in der Primärdatenbank wird Redo synchron an die Standby-D atenbank übertragen, und die Primärdatenbank wartet nur auf die Bestätigung, dass das Redo im Standby empfangen wurde, und nicht darauf, dass es auf den Standby-D atenträger geschrieben wurde. Dieser Modus, der auch als bezeichnet wird`FastSync`, kann einen Leistungsvorteil auf Kosten eines potenziellen Datenverlusts bei mehreren gleichzeitigen Ausfällen bieten.

Lesereplikate in RDS Custom für Oracle werden mit dem maximalen Leistungsschutzmodus erstellt, der auch der Standardschutzmodus für Oracle Data Guard ist. Der maximale Leistungsmodus bietet die geringsten Leistungsauswirkungen auf die Primärdatenbank, was Ihnen helfen kann, die in Sekunden gemessene Recovery Point Objective (RPO)-Anforderung zu erfüllen.

Um ein Ziel ohne Datenverlust (RPO=0) zu erreichen, können Sie den Schutzmodus von Oracle Data Guard auf `MaxAvailability` mit der `SYNC+NOAFFIRM` Einstellung für den Redo-Transport anpassen, um eine bessere Leistung zu erzielen. Da Commits in der Primärdatenbank erst bestätigt werden, nachdem die entsprechenden Redo-Vektoren erfolgreich an die Standby-Datenbank übertragen wurden, kann die Netzwerklatenz zwischen der primären Instance und dem Replikat für Commit-sensitive Workloads von entscheidender Bedeutung sein. Wir empfehlen, Lasttests für Ihren Workload durchzuführen, um die Leistungsauswirkungen zu bewerten, wenn das Lesereplikat für die Ausführung im -`MaxAvailability`Modus angepasst ist.

Die Bereitstellung des Lesereplikats in derselben Availability Zone wie die Primärdatenbank bietet eine geringere Netzwerklatenz als die Bereitstellung des Lesereplikats in einer anderen Availability Zone. Die Bereitstellung der Primär- und Lesereplikate in derselben Availability Zone erfüllt Ihre HA-Anforderungen jedoch möglicherweise nicht, da im unwahrscheinlichen Fall der Nichtverfügbarkeit der Availability Zone sowohl die primäre als auch die Lesereplikat-Instance betroffen sind.

Bewerten der Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas in AWS

Erstellt von Battulga Bolvragchaa (AWS), Krishnakumar Sa microSDanarayana (PeerIslands US Inc) und Bolbu Sivasan (MongoDB)

Umgebung: PoC oder Pilotprojekt	Quelle: Microsoft SQL Server	Ziel: MongoDB Atlas oder MongoDB Enterprise Advanced
R-Typ: Plattformwechsel	Workload: Microsoft	Technologien: Datenbanken; Migration

Übersicht

Dieses Muster bietet Anleitungen zum Laden von MongoDB mit nahezu realen Daten und zur Bewertung der MongoDB-Abfrageleistung, die so nah wie möglich am Produktionsszenario liegt. Die Bewertung bietet Eingaben, die Ihnen helfen, Ihre Migration zu MongoDB aus einer relationalen Datenbank zu planen. Das Muster verwendet PeerIslands Test Data Generator und Performance Analyzer, um die Abfrageleistung zu testen.

Dieses Muster ist besonders nützlich für die Migration von Microsoft SQL Server zu MongoDB, da das Ausführen von Schematransformationen und das Laden von Daten von aktuellen SQL Server-Instances zu MongoDB sehr komplex sein kann. Stattdessen können Sie nahezu realitätsnahe Daten in MongoDB laden, die MongoDB-Leistung verstehen und das Schemadesign optimieren, bevor Sie mit der eigentlichen Migration beginnen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Vertrautheit mit MongoDB Atlas
- MongoDB-Zielschema
- Typische Abfragemuster

Einschränkungen

- Die Ladezeiten und die Leistung der Daten werden durch die Größe der MongoDB-Cluster-Instance begrenzt. Wir empfehlen Ihnen, Instances zu wählen, die für den Produktionseinsatz empfohlen werden, um die reale Leistung zu verstehen.
- PeerIslands Test Data Generator und Performance Analyzer unterstützen derzeit nur Online-Datenladevorgänge und -abfragen. Die Offline-Batchverarbeitung (z. B. das Laden von Daten in MongoDB mithilfe von Spark-Konnektoren) wird noch nicht unterstützt.
- PeerIslands Test Data Generator und Performance Analyzer unterstützen Feldbeziehungen innerhalb einer Sammlung. Sie unterstützt keine Beziehungen zwischen Sammlungen.

Produkt-Editionen

- Dieses Muster unterstützt sowohl MongoDB Atlas als auch MongoDB Enterprise Advanced.

Architektur

Zieltechnologie-Stack

- MongoDB Atlas oder MongoDB Enterprise Advanced

Architektur

PeerIslands Test Data Generator und Performance Analyzer werden mithilfe von Java und Angular erstellt und speichern die generierten Daten im Amazon Elastic Block Store (Amazon EBS). Das Tool besteht aus zwei Workflows: Testdatengenerierung und Leistungstests.

- Bei der Testdatengenerierung erstellen Sie eine Vorlage, bei der es sich um die JSON-Darstellung des Datenmodells handelt, das generiert werden muss. Nachdem Sie die Vorlage erstellt haben, können Sie die Daten in einer Zielsammlung generieren, wie in der Konfiguration zur Lastgenerierung definiert.
- Bei Leistungstests erstellen Sie ein Profil. Ein Profil ist ein mehrstufiges Testszenario, in dem Sie CRUD-Operationen (Erstellen, Lesen, Aktualisieren und Löschen), Aggregationspipelines, die Gewichtung für jede Operation und die Dauer jeder Phase konfigurieren können. Nachdem

Sie das Profil erstellt haben, können Sie basierend auf der Konfiguration Leistungstests für die Zieldatenbank durchführen.

PeerIslands Test Data Generator und Performance Analyzer speichern ihre Daten auf Amazon EBS, sodass Sie Amazon EBS mit MongoDB verbinden können, indem Sie einen beliebigen von MongoDB unterstützten Verbindungsmechanismus verwenden, einschließlich Peering, Zulassungslisten und private Endpunkte. Standardmäßig enthält das Tool keine Betriebskomponenten. Es kann jedoch bei Bedarf mit Amazon Managed Service for Prometheus, Amazon Managed Grafana CloudWatch, Amazon und AWS Secrets Manager konfiguriert werden.

Tools

- PeerIslands Test Data Generator und Performance Analyzer enthalten zwei Komponenten. Die Test Data Generator-Komponente hilft Ihnen dabei, hoch kundenspezifische, reale Daten basierend auf Ihrem MongoDB-Schema zu generieren. Das Tool ist vollständig benutzeroberflächengesteuert und verfügt über eine umfangreiche Datenbibliothek und kann verwendet werden, um schnell Milliarden von Datensätzen auf MongoDB zu generieren. Das Tool bietet auch Funktionen zum Implementieren von Beziehungen zwischen Feldern im MongoDB-Schema. Die Performance Analyzer-Komponente hilft Ihnen dabei, hoch kundenspezifische Abfragen und Aggregationen zu generieren und realistische Leistungstests auf MongoDB durchzuführen. Sie können den Performance Analyzer verwenden, um die MongoDB-Leistung mit Rich-Load-Profilen und parametrisierten Abfragen für Ihren spezifischen Anwendungsfall zu testen.

Bewährte Methoden

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Bewährte Methoden für das MongoDB-Schemadesign (MongoDB-Entwicklerwebsite)
- Bewährte Methoden für die Bereitstellung von MongoDB Atlas in AWS (MongoDB-Website)
- Sicheres Verbinden von Anwendungen mit einer MongoDB-Atlas-Datenebene mit AWS PrivateLink (AWS-Blogbeitrag)
- Leitfaden für bewährte Methoden für MongoDB-Leistung (MongoDB-Website)

Polen

Verstehen Ihrer Quelldaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Machen Sie sich mit dem Datenbankbedarf der aktuellen SQL Server-Quelle vertraut.	Machen Sie sich mit Ihrem aktuellen SQL Server-Fußabdruck vertraut. Dies kann erreicht werden, indem Abfragen für das `INFORMATION` Schema der Datenbank ausgeführt werden. Bestimmen Sie die Anzahl der Tabellen und die Größe jeder Tabelle. Analysieren Sie den Index, der jeder Tabelle zugeordnet ist. Weitere Informationen zur SQL-Analyse finden Sie im Blogbeitrag SQL2Mongo: Data Migration Journey auf der - PeerIslands Website.	DBA
Machen Sie sich mit dem Quellschema vertraut.	Bestimmen Sie das Tabellenschema und die Geschäftsdarstellung der Daten (z. B. Postleitzahlen, Namen und Währung). Verwenden Sie Ihr vorhandenes Entity Relationship (ER)-Diagramm oder generieren Sie das ER-Diagramm aus der vorhandenen Datenbank. Weitere Informationen finden Sie im Blogbeitrag SQL2Mongo: Data Migration	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Journey auf der - PeerIslands Website.	
Verstehen von Abfragemu stern.	Dokumentieren Sie die 10 häufigsten SQL-Abfragen, die Sie verwenden. Sie können die Tabellen performan ce_schema.events_statements _summary_by_digest verwenden, die in der Datenbank verfügbar sind, um die wichtigsten Abfragen zu verstehen. Weitere Informati onen finden Sie im Blogbeitrag SQL2Mongo: Data Migration Journey auf der - PeerIslands Website.	DBA
Verstehen Sie SLA-Verpf lichtungen.	Dokumentieren Sie die Service Level Agreement s (SLAs) für Datenbank operationen. Zu den typischen Messwerten gehören die Abfragelatenz und Abfragen pro Sekunde. Die Maßnahmen und ihre Ziele sind in der Regel in Dokumenten mit nicht-funktionalen Anforderu ngen (NFR) verfügbar.	DBA

Definieren des MongoDB-Schemas

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie das Zielschema.	Definieren Sie verschiedene Optionen für das MongoDB-Zielschema. Weitere Informationen finden Sie unter Schemata in der MongoDB-Atlas-Dokumentation. MongoDB Berücksichtigen Sie die bewährten Methoden und Entwurfsmuster auf der Grundlage der Tabellenbeziehungen. Einzelheiten finden Sie unter Beispiele und Muster für Datenmodelle in der MongoDB-Dokumentation.	MongoDB-Techniker
Definieren Sie Zielabfragemuster.	Definieren Sie MongoDB-Abfragen und Aggregationspipelines. Diese Abfragen entsprechen den Top-Abfragen, die Sie für Ihren SQL Server-Workload erfasst haben. Informationen zum Erstellen von MongoDB-Aggregationspipelines finden Sie in der MongoDB-Dokumentation.	MongoDB-Techniker
Definieren Sie den MongoDB-Instance-Typ.	Bestimmen Sie die Größe der Instance, die Sie zum Testen verwenden möchten. Anleitungen finden Sie in der MongoDB-Dokumentation.	MongoDB-Techniker

Vorbereiten der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den MongoDB-Atlas-Cluster ein.	Um einen MongoDB-Cluster auf AWS einzurichten, folgen Sie den Anweisungen in der MongoDB-Dokumentation.	MongoDB-Techniker
Erstellen Sie Benutzer in der Zieldatenbank.	Konfigurieren Sie den MongoDB-Atlas-Cluster für den Zugriff und die Netzwerksicherheit, indem Sie den Anweisungen in der MongoDB-Dokumentation folgen.	MongoDB-Techniker
Erstellen Sie geeignete Rollen in AWS und konfigurieren Sie die rollenbasierte Zugriffskontrolle für Atlas.	Richten Sie bei Bedarf zusätzliche Benutzer ein, indem Sie den Anweisungen in der MongoDB-Dokumentation folgen. Konfigurieren Sie Authentifizierung und Autorisierung über AWS-Rollen.	MongoDB-Techniker
Richten Sie Compass für den MongoDB-Atlas-Zugriff ein.	Richten Sie das GUI-Dienstprogramm MongoDB Compass ein, um die Navigation und den Zugriff zu vereinfachen.	MongoDB-Techniker

Einrichten der Basislast mithilfe des Test Data Generators

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Test Data Generator.	Installieren Sie PeerIsland Test Data Generator in Ihrer Umgebung.	MongoDB-Techniker
Konfigurieren Sie Test Data Generator, um die entsprechenden Daten zu generieren.	Erstellen Sie eine Vorlage, indem Sie die Datenbibliothek verwenden, um spezifische Daten für jedes Feld im MongoDB-Schema zu generieren. Weitere Informationen finden Sie unter MongoDB Data Generator & Perf. Analyzer-Video.	MongoDB-Techniker
Skalieren Sie den Test Data Generator horizontal, um die erforderliche Last zu generieren.	Verwenden Sie die Vorlage, die Sie erstellt haben, um die Lastgenerierung anhand der Zielsammlung zu starten, indem Sie die erforderliche Parallelität konfigurieren. Bestimmen Sie die Zeitrahmen und Skalierung, um die erforderlichen Daten zu generieren.	MongoDB-Techniker
Validieren Sie die Last in MongoDB Atlas.	Überprüfen Sie die in MongoDB Atlas geladenen Daten.	MongoDB-Techniker
Generieren Sie die erforderlichen Indizes auf MongoDB .	Definieren Sie Indizes nach Bedarf, basierend auf Abfragemustern. Bewährte Methoden finden Sie in der MongoDB-Dokumentation.	MongoDB-Techniker

Leistungstests durchführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Ladeprofile in Performance Analyzer ein.	Erstellen Sie ein Leistungstestprofil in Performance Analyzer, indem Sie bestimmte Abfragen und die entsprechende Gewichtung, Dauer des Testlaufs und Stufen konfigurieren. Weitere Informationen finden Sie unter MongoDB Data Generator & Perf. Analyzer-Video.	MongoDB-Techniker
Führen Sie Leistungstests durch.	Verwenden Sie das von Ihnen erstellte Leistungstestprofil, um den Test anhand der Zielsammlung zu starten, indem Sie die erforderliche Parallelität konfigurieren. Skalieren Sie das Leistungstest-Tool horizontal, um Abfragen für MongoDB Atlas auszuführen.	MongoDB-Techniker
Zeichnen Sie die Testergebnisse auf.	Notieren Sie P95, P99-Latenz für die Abfragen.	MongoDB-Techniker
Optimieren Sie Ihr Schema und Ihre Abfragemuster.	Ändern Sie Indizes und Abfragemuster, um Leistungsprobleme zu beheben.	MongoDB-Techniker

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.	Löschen Sie alle temporäre n Ressourcen, die Sie für Test Data Generator und Performance Analyzer verwendet haben.	AWS-Administrator
Aktualisieren Sie die Leistungs testergebnisse.	Machen Sie sich mit der Leistung von MongoDB-A bfragen vertraut und vergleich en Sie sie mit Ihren SLAs. Optimieren Sie bei Bedarf das MongoDB-Schema und führen Sie den Prozess erneut aus.	MongoDB-Techniker
Schließen Sie das Projekt ab.	Schließen Sie das Projekt ab und geben Sie Feedback.	MongoDB-Techniker

Zugehörige Ressourcen

- GitHub -Repository: S3toAtlas
- Schema: MongoDB-Schemadesign
- Aggregationspipelines: MongoDB-Aggregationspipelines
- MongoDB-Atlas-Größe : Auswahl der Dimensionierungsstufe
- Video: MongoDB Data Generator und Perf. Analysator
- Referenzen: MongoDB-Dokumentation
- Tutorials: MongoDB-Entwicklerhandbuch, MongoDB Jumpstart
- AWS Marketplace: MongoDB Atlas auf AWS Marketplace
- AWS-Partnerlösungen: MongoDB Atlas in AWS-Referenzbereitstellung

Zusätzliche Ressourcen:

- SQL-Analyse
- MongoDB-Entwickler-Community-Foren
- Fragen zur MongoDB-Leistungsoptimierung
- Operative Analysen mit Atlas und Redshift
- Modernisierung von Anwendungen mit MongoDB Atlas und AWS Elastic Beanstalk

Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework

Erstellt von Jitendra Kumar (AWS), Oliver Francis (AWS) und Pavithra Balasubramanian (AWS)

aws-cross-region-drCode-Repository: -Datenbanken	Umgebung: Produktion	Technologien: Datenbanken; Infrastruktur; Migration; Modernisierung
AWS-Services: Amazon Aurora; AWS CloudFormation; Amazon ElastiCache; Amazon RDS; AWS Step Functions		

Übersicht

Dieses Muster beschreibt, wie DR Orchestrator Framework verwendet wird, um die manuellen, fehleranfälligen Schritte zur Durchführung der Notfallwiederherstellung in allen Amazon Web Services () -Regionen zu orchestrieren und zu automatisieren.AWS Das Muster deckt die folgenden Datenbanken ab:

- Amazon Relational Database Service (Amazon RDS) für MySQL, Amazon RDS for PostgreSQL oder Amazon RDS for MariaDB
- Amazon Aurora MySQL-Compatible Edition oder Amazon Aurora PostgreSQL-Compatible Edition (mit einer zentralisierten Datei)
- Amazon ElastiCache für Redis

Um die Funktionalität von DR Orchestrator Framework zu demonstrieren, erstellen Sie zwei DB-Instances oder Cluster. Die primäre befindet sich in der und AWS-Region `us-east-1` die sekundäre befindet sich in`us-west-2`. Um diese Ressourcen zu erstellen, verwenden Sie die AWS CloudFormation Vorlagen im `App-Stack` Ordner des GitHub Repositorys aws-cross-region-dr-databases.

Voraussetzungen und Einschränkungen

Allgemeine Voraussetzungen

- DR Orchestrator Framework wird sowohl primär als auch sekundär bereitgestellt AWS-Regionen
- Zwei Amazon Simple Storage Service-Buckets
- Eine virtuelle private Cloud (VPC) mit zwei Subnetzen und einer AWS Sicherheitsgruppe

Engine-spezifische Voraussetzungen

- Amazon Aurora — Mindestens eine globale Aurora-Datenbank muss in zwei verfügbar sein AWS-Regionen. Sie können `us-east-1` es als primäre Region und `us-west-2` als sekundäre Region verwenden.
- Amazon ElastiCache for Redis — Ein ElastiCache globaler Datenspeicher muss in zwei Einheiten verfügbar sein. AWS-Regionen Sie können `use us-east-1` es als primäre Region und `us-west-2` als sekundäre Region verwenden.

Einschränkungen von Amazon RDS

- DR Orchestrator Framework überprüft die Verzögerung bei der Replikation nicht, bevor ein Failover oder Failback durchgeführt wird. Die Replikationsverzögerung muss manuell überprüft werden.
- Diese Lösung wurde mit einer primären Datenbankinstanz mit einer Read Replica getestet. Wenn Sie mehr als eine Read Replica verwenden möchten, testen Sie die Lösung gründlich, bevor Sie sie in einer Produktionsumgebung implementieren.

Einschränkungen von Aurora

- Die Verfügbarkeit und der Support von Funktionen variieren je nach Version der einzelnen Datenbank-Engines und zwischen den einzelnen Versionen AWS-Regionen. Weitere Informationen zur Verfügbarkeit von Funktionen und Regionen für die regionsübergreifende Replikation finden Sie unter Regionsübergreifende Read Replicas.
- Für globale Aurora-Datenbanken gelten spezifische Konfigurationsanforderungen für unterstützte Aurora-DB-Instance-Klassen und die maximale Anzahl von AWS-Regionen. Weitere Informationen finden Sie unter Konfigurationsanforderungen einer globalen Amazon Aurora Aurora-Datenbank.

- Diese Lösung wurde mit einer primären Datenbank-Instance mit einer Read Replica getestet. Wenn Sie mehr als eine Read Replica verwenden möchten, testen Sie die Lösung gründlich, bevor Sie sie in einer Produktionsumgebung implementieren.

ElastiCache Einschränkungen

- Informationen zur regionalen Verfügbarkeit für Global Datastore und zu den ElastiCache Konfigurationsanforderungen finden Sie in der ElastiCache Dokumentation unter Voraussetzungen und Einschränkungen.

Amazon RDS-Produktversionen

Amazon RDS unterstützt die folgenden Engine-Versionen:

- MySQL — Amazon RDS unterstützt DB-Instances, auf denen die folgenden Versionen von MySQL ausgeführt werden: MySQL 8.0 und MySQL 5.7
- PostgreSQL — Informationen zu unterstützten Versionen von Amazon RDS for PostgreSQL finden Sie unter Verfügbare PostgreSQL-Datenbankversionen.
- MariaDB — Amazon RDS unterstützt DB-Instances, auf denen die folgenden Versionen von MariaDB ausgeführt werden:
  - MariaDB 10.11
  - MariaDB 10.6
  - MariaDB 10.5

Aurora-Produktversionen

- Für den globalen Datenbank-Switchover von Amazon Aurora ist Aurora MySQL-kompatibel mit MySQL 5.7-Kompatibilität, Version 2.09.1 und höher erforderlich

  Weitere Informationen finden Sie unter Einschränkungen der globalen Amazon Aurora Aurora-Datenbanken.

ElastiCache für Redis-Produktversionen

Amazon ElastiCache for Redis unterstützt die folgenden Redis-Versionen:

- Redis 7.1 (erweitert)

- Redis 7.0 (erweitert)
- Redis 6.2 (erweitert)
- Redis 6.0 (erweitert)
- Redis 5.0.6 (erweitert)

Weitere Informationen finden Sie unter Unterstützt ElastiCache für Redis-Versionen.

Architektur

Amazon RDS-Architektur

Die Amazon RDS-Architektur umfasst die folgenden Ressourcen:

- Die in der primären Region (`us-east-1`) erstellte primäre Amazon RDS-DB-Instance mit Lese-/Schreibzugriff für Kunden
- Eine Amazon RDS-Lesereplik, die in der sekundären Region (`us-west-2`) mit schreibgeschütztem Zugriff für Kunden erstellt wurde
- Das DR Orchestrator Framework wird sowohl in der primären als auch in der sekundären Region eingesetzt

Das Diagramm zeigt Folgendes:

1. Asynchrone Replikation zwischen der primären Instance und der sekundären Instance
2. Lese-/Schreibzugriff für Clients in der primären Region
3. Nur-Lese-Zugriff für Clients in der sekundären Region

Aurora-Architektur

Die Amazon Aurora Aurora-Architektur umfasst die folgenden Ressourcen:

- Der primäre Aurora-DB-Cluster, der in der primären Region (`us-east-1`) mit einem Active-Writer-Endpunkt erstellt wurde
- Ein Aurora-DB-Cluster, der in der sekundären Region (`us-west-2`) mit einem inaktiven Writer-Endpunkt erstellt wurde

- Das DR Orchestrator Framework wird sowohl in der primären als auch in der sekundären Region eingesetzt

Das Diagramm zeigt Folgendes:

1. Asynchrone Replikation zwischen dem primären Cluster und dem sekundären Cluster
2. Der primäre DB-Cluster mit einem Active-Writer-Endpunkt
3. Der sekundäre DB-Cluster mit einem inaktiven Writer-Endpunkt

ElastiCache für die Redis-Architektur

Die Architektur von Amazon ElastiCache for Redis umfasst die folgenden Ressourcen:

- Ein globaler Datenspeicher ElastiCache für Redis, der mit zwei Clustern erstellt wurde:
  1. Der primäre Cluster in der primären Region () `us-east-1`
  2. Der sekundäre Cluster in der sekundären Region (`us-west-2`)
- Ein regionsübergreifender Amazon-Link mit TLS 1.2-Verschlüsselung zwischen den beiden Clustern
- DR Orchestrator Framework wird sowohl in primären als auch in sekundären Regionen eingesetzt

Automatisierung und Skalierung

DR Orchestrator Framework ist skalierbar und unterstützt den Failover oder Failback von mehr als einer AWS Datenbank parallel.

Sie können den folgenden Payload-Code verwenden, um ein Failover für mehrere AWS Datenbanken in Ihrem Konto durchzuführen. In diesem Beispiel führen drei AWS Datenbanken (zwei globale Datenbanken wie Aurora MySQL-kompatibel oder Aurora PostgreSQL-kompatibel und eine Amazon RDS for MySQL MySQL-Instance) ein Failover zur DR-Region durch:

```
{
  "StatePayload": [
    {
```

```
      "layer": 1,
      "resources": [
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (MySQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-mysql-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-mysql-cluster-
identifier"
          }
        },
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (PostgreSQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-postgres-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-postgres-cluster-
identifier"
          }
        },
        {
          "resourceType": "PromoteRDSReadReplica",
          "resourceName": "Promote RDS for MySQL Read Replica",
          "parameters": {
            "RDSInstanceIdentifier": "!Import rds-mysql-instance-identifier",
            "TargetClusterIdentifier": "!Import rds-mysql-instance-global-arn"
          }
        }
      ]
    }
  ]
}
```

Tools

AWS Dienste

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.

- Amazon ElastiCache unterstützt Sie bei der Einrichtung, Verwaltung und Skalierung verteilter In-Memory-Cache-Umgebungen in der AWS Cloud. Dieses Muster verwendet Amazon ElastiCache für Redis.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster werden Lambda-Funktionen verwendet AWS Step Functions , um die Schritte auszuführen.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud Dieses Muster unterstützt Amazon RDS for MySQL, Amazon RDS for PostgreSQL und Amazon RDS for MariaDB.
- AWS SDK for Python (Boto3)hilft Ihnen bei der Integration Ihrer Python-Anwendung, -Bibliothek oder Ihres Skripts mit AWS-Services. In diesem Muster werden Boto3-APIs verwendet, um mit den Datenbankinstanzen oder globalen Datenbanken zu kommunizieren.
- AWS Step Functionsist ein serverloser Orchestrierungsdienst, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen. In diesem Muster werden Step Functions Functions-Zustandsmaschinen verwendet, um den regionsübergreifenden Failover und das Failback der Datenbankinstanzen oder globalen Datenbanken zu orchestrieren und auszuführen.

Code-Repository

Der Code für dieses Muster ist im Repository aws-cross-region-dr-databases unter GitHub verfügbar.

Epen

Installieren Sie DR Orchestrator Framework

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Führen Sie den folgenden Befehl aus, um das Repository zu klonen: `git clone https://github.com/aws-samp`	AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/aws-cross-region-dr-databases.git`	

Paketieren Sie den Code der Lambda-Funktionen in einem ZIP-Dateiarchiv.	Erstellen Sie die Archivdat eien für Lambda-Funktionen, um die DR Orchestrator Framework-Abhängigkeiten einzubeziehen:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts`
	`bash scripts/deploy-orchestrator-sh.sh`
		AWS-Administrator

S3-Buckets erstellen.	S3-Buckets werden benötigt, um DR Orchestrator Framework zusammen mit Ihrer neuesten Konfiguration zu speichern. Erstellen Sie zwei S3-Buckets, einen in der primären Region (`us-east-1`) und einen in der sekundäre n Region (): `us-west-2` • `dr-orchestrator-xxxxxx-us-east-1` • `dr-orchestrator-xxxxxx-us-west-2` `xxxxxx`Ersetzen Sie ihn durch einen zufälligen Wert, um die Bucket-Namen eindeutig zu machen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Subnetze und Sicherheitsgruppen.	Erstellen Sie sowohl in der primären Region (`us-east-1`) als auch in der sekundären Region (`us-west-2`) zwei Subnetze und eine Sicherheitsgruppe für die Bereitstellung von Lambda-Funktionen in Ihrer VPC: • `subnet-XXXXXXX` • `subnet-YYYYYYY` • `sg-XXXXXXXXXXXX`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die DR Orchestrator-Parameterdateien.	Aktualisieren Sie in dem `<YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` Ordner die folgenden DR Orchestrator-Parameterdateien: • `Orchestrator-Deployer-parameters-us-east-1.json` • `Orchestrator-Deployer-parameters-us-west-2.json` Verwenden Sie die folgenden Parameterwerte x und y ersetzen Sie diese durch die Namen Ihrer Ressourcen: `[ { "ParameterKey": "TemplateStoreS3BucketName", "ParameterValue": "dr-orchestrator-xxxxxx-us-east-1" }, { "ParameterKey": "TemplateVPCId", "ParameterValue": "vpc-xxxxxx" }, {`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"ParameterKey": "TemplateLambdaSubnetID1", "ParameterValue": "subnet-xxxxx" }, { "ParameterKey": "TemplateLambdaSubnetID2", "ParameterValue": "subnet-yyyyy" }, { "ParameterKey": "TemplateLambdaSecurityGroupID", "ParameterValue": "sg-xxxxxxxxxx" }]	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den DR Orchestrator Framework-Code in den S3-Bucket hoch.	Der Code ist in einem S3-Bucket sicherer als im lokalen Verzeichnis. Laden Sie das `DR-Orchestration-artifacts` Verzeichnis, einschließlich aller Dateien und Unterordner, in die S3-Buckets hoch. Gehen Sie wie folgt vor, um den Code hochzuladen: 1. Melden Sie sich bei der an AWS Management Console. 2. Navigieren Sie zur Amazon S3 S3-Konsole. 3. Wählen Sie das `dr-orchestrator-xxxxxx-us-east-1` `bucket` aus. 4. Wählen Sie Upload und anschließend Ordner hinzufügen. 5. Wählen Sie den `DR-Orchestration-artifacts` -Ordner aus. 6. Klicken Sie auf Hochladen. 7. Wählen Sie den `dr-orchestrator-xxxxxx-us-west-2` Bucket aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wiederholen Sie die Schritte 4—7.	

Stellen Sie das DR Orchestrator Framework in der primären Region bereit.	Führen Sie die folgenden Befehle aus, um DR Orchestrator Framework in der primären Region (`us-east-1`) bereitzustellen:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie das DR Orchestrator Framework in der sekundären Region bereit.	Führen Sie in der sekundären Region (`us-west-2`) die folgenden Befehle aus:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitstellung.	Wenn der AWS CloudFormation Befehl erfolgreich ausgeführt wird, gibt er die folgende Ausgabe zurück: `Successfully created/updated stack - dr-orchestrator` Alternativ können Sie zur AWS CloudFormation Konsole navigieren und den Status des `dr-orchestrator` Stacks überprüfen.	AWS-Administrator

Erstellen Sie die Datenbankinstanzen oder Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datenbank-Subnetze und Sicherheitsgruppen.	Erstellen Sie in Ihrer VPC zwei Subnetze und eine Sicherheitsgruppe für die DB-Instance oder globale Datenbank sowohl in der primären (`us-east-1`) als auch in der sekundären (`us-west-2`) Region: • `subnet-XXXXXX` • `subnet-XXXXXX` • `sg-XXXXXXXXXX`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameterdatei für die primäre DB-Instance oder den Cluster.	Aktualisieren `<YOUR LOCAL GIT FOLDER>/App-Stack` Sie im Ordner die Parameter datei für die primäre Region. Amazon RDS Aktualisieren Sie in der `RDS-MySQL-parameter-us-east-1.json` Datei `SubnetIds` und geben `DBSecurityGroup` Sie die Namen der Ressourcen an, die Sie erstellt haben: `{ "Parameters": { "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId" } }`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Aurora Aktualisieren Sie in der `Aurora-MySQL-parameter-us-east-1.json` Datei `SubnetIds` und `DBSecurityGroup` mit den Namen der Ressourcen, die Sie erstellt haben: `{ "Parameters": { "SubnetIds": "subnet1-xxxxxx,subnet2-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql", "DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon ElastiCache für Redis Aktualisieren Sie die `ElastiCache-parameter-us-east-1.json` Datei `DBSecurityGroup` mit `SubnetIds` den Namen der Ressourcen, die Sie erstellt haben. `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-xxxxxxxxxx", "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId", "PrimaryRegion": "us-east-1",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"SecondaryRegion": "us-west-2" } }</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie Ihre DB-Instanz oder Ihren Cluster in der primären Region bereit.	Um Ihre Instance oder Ihren Cluster in der primären Region (`us-east-1`) bereitzustellen, führen Sie die folgenden Befehle basierend auf Ihrer Datenbank-Engine aus.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-Primary.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-Primary.yaml \`
	`--parameter-overrides file://Aurora-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon ElastiCache für Redis
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 --stack-name elasticache-ds-app-stack \`
	`--template-file ElastiCache-Primary.yaml \`
	`--parameter-overrides file://ElastiCache-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass die AWS CloudFormation Ressourcen erfolgreich eingesetzt wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameterdatei für die sekundäre DB-Instance oder den Cluster.	Aktualisieren `<YOUR LOCAL GIT FOLDER>/App-Stack` Sie im Ordner die Parameter datei für die sekundäre Region. Amazon RDS Aktualisieren Sie die `RDS-MySQL-parameter-us-west-2.json` Datei `DBSecurityGroup` mit `SubnetIDs` den Namen der Ressourcen, die Sie erstellt haben. Aktualisieren Sie den `PrimaryRegionKMSKeyArn` mit dem Wert von `MySQLKmsKeyId` aus dem Abschnitt Outputs des AWS CloudFormation Stacks für die primäre DB-Instance: `{ "Parameters": { "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1",`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> "SecondaryRegion":
	 "us-west-2",
	    "KMSKeyAliasName":
	 "rds/rds-mysql-ins
	tance-KmsKeyId",
	    "PrimaryRegionKMSK
	eyArn":"arn:aws:km
	s:us-east-1:xxxxxx
	xxx:key/mrk-xxxxxx
	xxxxxxxxxxxxxx"
	  }
	}</pre>
	Amazon Aurora
	
	Aktualisieren Sie in der `Aurora-MySQL-parameter-us-west-2.json` Datei `SubnetIDs` und `DBSecurityGroup` mit den Namen der Ressourcen, die Sie erstellt haben. Aktualisieren Sie den `PrimaryRegionKMSKeyArn` mit dem Wert `AuroraKmsKeyId` aus dem Abschnitt Outputs des AWS CloudFormation Stacks für die primäre DB-Instance:
	
	<pre>{
	  "Parameters": {
	    "SubnetIds":
	 "subnet1-aaaaaaaaa
	,subnet2-bbbbbbbbb",
	    "DBSecurityGroup":
	 "sg-ccccccccc",
	    "GlobalClusterIden
	tifier":"dr-globaldb-
	cluster-mysql",</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"DBClusterName":"dbcluster-01",
	"SourceDBClusterName":"dbcluster-02",
	"DBPortNumber": "3787",
	"DBInstanceClass": "db.r5.large",
	"InitialDatabaseName": "sampledb",
	"PrimaryRegion": "us-east-1",
	"SecondaryRegion": "us-west-2",
	"KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId"
	}
	}</pre>
	Amazon ElastiCache für Redis
	
	Aktualisieren Sie in der `ElastiCache-parameter-us-west-2.json` Datei `SubnetIDs` und `DBSecurityGroup` geben Sie die Namen der Ressourcen an, die Sie erstellt haben. Aktualisieren Sie den `PrimaryRegionKMSKeyArn` mit dem Wert von `ElastiCacheKmsKeyId` aus dem Abschnitt Outputs des AWS CloudFormation Stacks für die primäre DB-Instance:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	{
	  "Parameters": {
	  "CacheNodeType": "cache.m5.large",
	  "DBSecurityGroup": "sg-ccccccccc",
	  "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb",
	  "EngineVersion": "5.0.6",
	  "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore",
	  "NumReplicas": "1",
	  "NumShards": "1",
	  "ReplicationGroupId": "demo-redis-cluster",
	  "DBPortNumber": "3788",
	  "TransitEncryption": "true",
	  "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId",
	  "PrimaryRegion": "us-east-1",
	  "SecondaryRegion": "us-west-2"
	  }
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie Ihre DB-Instanz oder Ihren Cluster in der sekundären Region bereit.	Führen Sie die folgenden Befehle basierend auf Ihrer Datenbank-Engine aus.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-DR.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-DR.yaml \`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--parameter-overrides file://Aurora-MySQL-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	
	Amazon ElastiCache für Redis	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack aws cloudformation deploy \ --region us-west-2 \ --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-DR.yaml \ --parameter-overrides file://ElastiCache-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	
	Stellen Sie sicher, dass die AWS CloudFormation Ressourcen erfolgreich eingesetzt wurden.	

Zugehörige Ressourcen

- Strategie zur Notfallwiederherstellung für Datenbanken auf AWS (AWS Prescriptive Guidance-Strategie)
- Automatisieren Sie Ihre DR-Lösung für relationale Datenbanken auf AWS (AWS Prescriptive Guidance Guide Guide)
- Verwendung globaler Amazon Aurora Aurora-Datenbanken
- Replikation AWS-Regionen über globale Datenspeicher hinweg
- Automatisieren Sie Ihre DR-Lösung für relationale Datenbanken auf AWS (AWS Prescriptive Guidance Guide)

Automatisieren der Replikation von Amazon RDS-Instances über AWS-Konten hinweg

Erstellt von Parag Nagwekar (AWS) und Arun Chpillai (AWS)

Umgebung: Produktion	Technologien: Datenbanken DevOps; Serverless; Infrastruktur	Workload: Alle anderen Workloads
AWS-Services: AWS Lambda; Amazon RDS; AWS SDK for Python (Boto3); AWS Step Functions ;Amazon SNS		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie den Prozess der Replikation, Nachverfolgung und des Rollbacks Ihrer Amazon Relational Database Service (Amazon RDS)-DB-Instances über verschiedene AWS-Konten hinweg mithilfe von AWS Step Functions und AWS Lambda automatisieren können. Sie können diese Automatisierung verwenden, um eine groß angelegte Replikation von RDS-DB-Instances ohne Leistungseinbußen oder Betriebsaufwand durchzuführen – unabhängig von der Größe Ihrer Organisation. Sie können dieses Muster auch verwenden, um Ihre Organisation bei der Einhaltung obligatorischer Data-Governance-Strategien oder Compliance-Anforderungen zu unterstützen, die erfordern, dass Ihre Daten repliziert und über verschiedene AWS-Konten und AWS-Regionen redundant werden. Die kontoübergreifende Replikation von Amazon-RDS-Daten in großem Umfang ist ein ineffizienter und fehleranfälliger manueller Prozess, der kostspielig und zeitaufwändig sein kann. Die Automatisierung in diesem Muster kann Ihnen jedoch helfen, eine kontoübergreifende Replikation sicher, effektiv und effizient zu erreichen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei AWS-Konten
- Eine RDS-DB-Instance, die im AWS-Quellkonto ausgeführt wird

- Eine Subnetzgruppe für die RDS-DB-Instance im AWS-Zielkonto
- Ein AWS Key Management Service (AWS KMS)-Schlüssel, der im AWS-Quellkonto erstellt und für das Zielkonto freigegeben wurde (weitere Informationen zu Richtliniendetails finden Sie im Abschnitt Zusätzliche Informationen dieses Musters).
- Ein AWS KMS-Schlüssel im AWS-Zielkonto zum Verschlüsseln der Datenbank im Zielkonto

Produktversionen

- Python 3.9 (mit AWS Lambda)
- PostgreSQL 11.3, 13.x und 14.x

Architektur

Technologie-Stack

- Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Verwendung von Step Functions zur Orchestrierung der geplanten On-Demand-Replikation von RDS-DB-Instances von einem Quellkonto (Konto A) zu einem Zielkonto (Konto B).

Im Quellkonto (Konto A im Diagramm) führt der Step-Functions-Zustandsautomat Folgendes aus:

1. Erstellt einen Snapshot aus der RDS-DB-Instance in Konto A.
2. Kopiert und verschlüsselt den Snapshot mit einem AWS KMS-Schlüssel aus Konto A. Um die Verschlüsselung bei der Übertragung sicherzustellen, wird der Snapshot verschlüsselt, unabhängig davon, ob die DB-Instance verschlüsselt ist oder nicht.

3. Gibt den DB-Snapshot für Konto B frei, indem Konto B Zugriff auf den Snapshot gewährt wird.
4. Überträgt eine Benachrichtigung an das SNS-Thema und ruft dann das SNS-Thema die Lambda-Funktion in Konto B auf.

Im Zielkonto (Konto B im Diagramm) führt die Lambda-Funktion den Step-Functions-Zustandsautomaten aus, um Folgendes zu orchestrieren:

1. Kopiert den freigegebenen Snapshot von Konto A in Konto B, während der AWS KMS-Schlüssel von Konto A verwendet wird, um die Daten zuerst zu entschlüsseln, und dann die Daten mithilfe des AWS KMS-Schlüssels in Konto B verschlüsselt.
2. Liest das Secret aus Secrets Manager, um den Namen der aktuellen DB-Instance zu erfassen.
3. Stellt die DB-Instance aus dem Snapshot mit einem neuen Namen und einem neuen AWS KMS-Standardschlüssel für Amazon RDS wieder her.
4. Liest den Endpunkt der neuen Datenbank, aktualisiert das Secret in Secrets Manager mit dem neuen Datenbankendpunkt und markiert dann die vorherige DB-Instance, damit sie später gelöscht werden kann.
5. Behält die neuesten N Instances der Datenbanken bei und löscht alle anderen Instances.

Tools

AWS-Tools

- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

- AWS SDK for Python (Boto3) ist ein Software Development Kit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr -Skript in AWS-Services integrieren können.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Code

Der Code für dieses Muster ist im GitHub Repository Kontoübergreifende RDS-Replikation verfügbar.

Polen

Automatisieren der Replikation von RDS-DB-Instances über AWS-Konten hinweg mit einem einzigen Klick

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack im Quellkonto bereit.	1. Melden Sie sich bei der AWS-Managementkonsole für das Quellkonto (Konto A) an und öffnen Sie die CloudFormation Konsole . 2. Klicken Sie im Navigationsbereich auf Stacks. 3. Wählen Sie Stack erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren) aus. 4. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 5. Wählen Sie auf der Seite Vorlage angeben die Option Vorlage hochladen aus.	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie Datei auswählen, wählen Sie die `Cloudformation-SourceAccountRDS.yaml` Datei aus dem GitHub Repository Kontoüber greifende RDS-Replikation aus und klicken Sie dann auf Weiter. 7. Geben Sie für Stack-Name einen Namen für Ihren Stack ein. 8. Geben Sie im Abschnitt Parameter die Parameter an, die in der Stack-Vorlage definiert sind: • DestinationAccount NumberGeben Sie für die Kontonummer für Ihre Ziel-RDS-DB-Instance ein. • KeyNameGeben Sie für Ihren AWS KMS-Schlüssel ein. • ScheduleExpression Geben Sie für einen Cron-Ausdruck ein (Standardeinstellung ist 12:00 Uhr täglich). • Geben Sie für SourceDBIdentifier den Namen der Quelldatenbank ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Geben Sie für SourceDBSnapshotName den Namen des Snapshots ein oder akzeptieren Sie den Standard. 9. Wählen Sie Weiter aus. 10. Behalten Sie auf der Seite Stack-Optionen konfigurieren die Standardwerte bei und wählen Sie dann Weiter aus. 11. Überprüfen Sie Ihre Stack-Konfiguration und wählen Sie dann Absenden aus. 12. Wählen Sie die Registerkarte Ressourcen für Ihren Stack und notieren Sie sich dann den Amazon-Ressourcennamen (ARN) des SNS-Themas.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack im Zielkonto bereit.	1. Melden Sie sich bei der AWS-Managementkonsole für das Zielkonto (Konto B) an und öffnen Sie die CloudFormation Konsole . 2. Klicken Sie im Navigationsbereich auf Stacks. 3. Wählen Sie Stack erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren) aus. 4. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 5. Wählen Sie auf der Seite Vorlage angeben die Option Vorlage hochladen aus. 6. Wählen Sie Datei , wählen Sie die `Cloudformation-DestinationAccountRDS.yaml` Datei aus dem Repository GitHub Kontoübergreifende RDS-Replikation aus und wählen Sie dann Weiter aus. 7. Geben Sie für Stack-Name einen Namen für Ihren Stack ein. 8. Geben Sie im Abschnitt Parameter die Parameter an, die in der Stack-Vorlage definiert sind:	Cloud-Architekt, DevOps Techniker, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• DatabaseNameGeben Sie für einen Namen für Ihre Datenbank ein. • Geben Sie für Engine den Datenbank-Engine-Typ ein, der der Quelldatenbank entspricht. • Geben Sie für DB den bevorzugten Datenbank InstanceClass-Instance-Typ ein oder akzeptieren Sie den Standardwert. • Geben Sie für Subnetzgruppen die vorhandene VPC-Subnetzgruppe ein. Anweisungen zum Erstellen einer Subnetzgruppe finden Sie unter Schritt 2: Erstellen einer DB-Subnetzgruppe im Amazon-RDS-Benutzerhandbuch. • Geben Sie für den Pfad und den Secret-SecretNameNamen ein oder akzeptieren Sie die Standardeinstellung. • Geben Sie für SGID die Sicherheitsgruppen-ID Ihres Ziel-Clusters ein. • Geben Sie für KMSKey den ARN des KMS-Schlü	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ssels in Ihrem Zielkonto ein. • NoOfOlderInstances Geben Sie für die Anzahl der alten Kopien der RDS-DB-Instances ein, die Sie für das Rollback behalten möchten. 9. Wählen Sie Weiter aus. 10. Behalten Sie auf der Seite Stack-Optionen konfiguri eren die Standardwerte bei und wählen Sie dann Weiter aus. 11. Überprüfen Sie Ihre Stack-Konfiguration und wählen Sie dann Absenden aus. 12. Wählen Sie die Registerk arte Ressourcen für Ihren Stack und notieren Sie sich dann die physische ID und den ARN von `InvokeSte pFunction` .	
Überprüfen Sie die Erstellun g der RDS-DB-Instance im Zielkonto.	1. Melden Sie sich bei der AWS-Managementkons ole an und öffnen Sie die Amazon RDS-Konsole . 2. Wählen Sie im Navigatio nsbereich Datenbanken und überprüfen Sie dann, ob die neue RDS-DB-Instance unter dem neuen Cluster angezeigt wird.	Cloud-Administrator, Cloud-Architekt, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Abonnieren Sie die Lambda-Funktion für das SNS-Thema.	Sie müssen die folgenden AWS Command Line Interface (AWS CLI)-Befehle ausführen , um die Lambda-Funktion im Zielkonto (Konto B) für das SNS-Thema im Quellkonto (Konto A) zu abonnieren.
	
	Führen Sie in Konto A den folgenden Befehl aus:
	
	`aws sns add-permission \ --label lambda-access --aws-account-id <DestinationAccount> \ --topic-arn <Arn of SNSTopic > \ --action-name Subscribe ListSubscriptionsB yTopic`
	
	Führen Sie in Konto B den folgenden Befehl aus:
	
	`aws lambda add-permi ssion \ --function-name <Name of InvokeStepFunction > \ --source-arn <Arn of SNSTopic > \ --statement-id function-with-sns \ --action lambda:In vokeFunction \`
		Cloud-Administrator, Cloud-Architekt, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--principal sns.amazonaws.com`
	
	Führen Sie in Konto B den folgenden Befehl aus:
	
	`aws sns subscribe \ --protocol "lambda" \ --topic-arn <Arn of SNSTopic> \ --notification-endpoint <Arn of InvokeStepFunction>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synchronisieren Sie die RDS-DB-Instance aus dem Quellkonto mit dem Zielkonto.	Starten Sie die On-Demand-Datenbankreplikation, indem Sie den Step Functions -Zustandsautomaten im Quellkonto starten. 1. Öffnen Sie die Step-Functions-Konsole . 2. Wählen Sie im Navigationsbereich Zustandsautomaten aus. 3. Wählen Sie Ihren Zustandsautomaten aus. 4. Wählen Sie auf der Registerkarte Ausführungen Ihre Funktion aus und wählen Sie dann Ausführung starten, um den Workflow zu starten. Hinweis: Es ist ein Scheduler vorhanden, der Ihnen hilft, die Replikation automatisch nach dem Zeitplan auszuführen, aber der Scheduler ist standardmäßig deaktiviert. Sie finden den Namen der Amazon- CloudWatch Regel für den Scheduler auf der Registerkarte Ressourcen des CloudFormation Stacks im Zielkonto. Anweisungen zum Ändern der CloudWatch Ereignisregel finden Sie unter	Cloud-Architekt, DevOps Techniker, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Löschen oder Deaktivieren einer CloudWatch Ereignisregel im CloudWatch -Benutzerhandbuch.	
Setzen Sie Ihre Datenbank bei Bedarf auf eine der vorherigen Kopien zurück.	1. Öffnen Sie die Secrets Manager-Konsole. 2. Wählen Sie aus der Liste der Secrets das Secret aus, das Sie zuvor mithilfe der CloudFormation Vorlage erstellt haben. Ihre Anwendung verwendet das Secret, um auf die Datenbank im Ziel-Cluster zuzugreifen. 3. Um den Secret-Wert auf der Detailseite zu aktualisieren, wählen Sie im Abschnitt Secret-Wert die Option Secret-Wert abrufen und dann Bearbeiten aus. 4. Geben Sie die Details des Datenbankendpunkts ein.	Cloud-Administrator, DBA, DevOps Engineering

Zugehörige Ressourcen

- Regionsübergreifende Lesereplikate (Amazon-RDS-Benutzerhandbuch)
- Blau/Grün-Bereitstellungen (Amazon-RDS-Benutzerhandbuch)

Zusätzliche Informationen

Sie können die folgende Beispielrichtlinie verwenden, um Ihren AWS KMS-Schlüssel für mehrere AWS-Konten freizugeben.

```
{
    "Version": "2012-10-17",
    "Id": "cross-account-rds-kms-key",
    "Statement": [
        {
            "Sid": "Enable user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<SourceAccount>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DestinationAccount>:root"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<DestinationAccount>:root",
                    "arn:aws:iam::<SourceAccount>:root"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Automatisches Sichern von SAP HANA-Datenbanken mit Systems Manager und EventBridge

Erstellt von Ambarish Satarkar (AWS) und Gaurav Rath (AWS)

Code-Repository: HDB_Backup_SSM_Document	Umgebung: Produktion	Technologien: Datenbanken; Speicher und Backup
Workload: SAP	AWS-Services: Amazon EC2; Amazon EventBridge; Amazon S3; AWS Systems Manager	

Übersicht

Dieses Muster beschreibt, wie Sie SAP HANA-Datenbank-Backups mit AWS Systems Manager , Amazon EventBridge, Amazon Simple Storage Service (Amazon S3) und AWS Backint Agent für SAP HANA automatisieren.

Dieses Muster bietet einen auf Shell-Skripten basierenden Ansatz mit dem -`BACKUP DATA`Befehl und macht es überflüssig, Skripts und Auftragskonfigurationen für jede Betriebssystem-Instance (OS) über zahlreiche Systeme hinweg zu verwalten.

> Hinweis: Seit April 2023 hat AWS Backup die Unterstützung für SAP HANA-Datenbanken in Amazon Elastic Compute Cloud (Amazon EC2) angekündigt. Weitere Informationen finden Sie unter Backup von SAP HANA-Datenbanken auf Amazon-EC2-Instances.
>
> Je nach den Anforderungen Ihrer Organisation können Sie den AWS Backup-Service verwenden , um Ihre SAP HANA-Datenbanken automatisch zu sichern, oder Sie können dieses Muster verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene SAP HANA-Instance mit einer unterstützten Version im Ausführungsstatus auf einer verwalteten Amazon Elastic Compute Cloud (Amazon EC2)-Instance, die für Systems Manager konfiguriert ist
- Systems Manager Agent (SSM Agent) 2.3.274.0 oder höher installiert
- Ein S3-Bucket, für den der öffentliche Zugriff nicht aktiviert ist
- Ein -hdbuserstoreSchlüssel mit dem NamenSYSTEM
- Eine AWS Identity and Access Management (IAM)-Rolle für das Automation-Runbook, das nach Zeitplan ausgeführt werden soll
- `AmazonSSMManagedInstanceCore` - und -`ssm:StartAutomationExecution`Richtlinien sind an die Systems Manager Automation-Servicerolle angehängt.

Einschränkungen

- AWS Backint Agent für SAP HANA unterstützt keine Deduplizierung.
- AWS Backint Agent für SAP HANA unterstützt keine Datenkomprimierung.

Produktversionen

AWS Backint Agent wird auf den folgenden Betriebssystemen unterstützt:

- SUSE-Linux-Enterprise-Server
- SUSE Linux Enterprise Server für SAP
- Red Hat Enterprise Linux für SAP

AWS Backint Agent unterstützt die folgenden Datenbanken:

- SAP HANA 1.0 SP12 (einzelner Knoten und mehrere Knoten)
- SAP HANA 2.0 und höher (einzelner Knoten und mehrere Knoten)

Architektur

Zieltechnologie-Stack

- AWS-Backint-Agent
- Amazon S3

- AWS Systems Manager
- Amazon EventBridge
- SAP HANA

Zielarchitektur

Das folgende Diagramm zeigt die Installationsskripte, die AWS Backint Agent, den S3-Bucket und Systems Manager und installieren EventBridge, die ein Befehlsdokument verwenden, um regelmäßige Backups zu planen.

Automatisierung und Skalierung

- Mehrere AWS Backint Agents können mithilfe eines Systems Manager Automation-Runbooks installiert werden.
- Jede Ausführung des Systems Manager-Runbooks kann je nach Zielauswahl auf eine Anzahl von SAP HANA-Instan cesskaliert werden.
- EventBridge kann SAP HANA-Backups automatisieren.

Tools

- AWS Backint Agent für SAP HANA ist eine eigenständige Anwendung, die in Ihre vorhandenen Workflows integriert werden kann, um Ihre SAP HANA-Datenbank in einem S3-Bucket zu sichern, den Sie in der Konfigurationsdatei angeben. AWS Backint Agent unterstützt vollständige, inkrementelle und differentielle Backups von SAP HANA-Datenbanken. Es wird auf einem SAP HANA-Datenbankserver ausgeführt, auf dem Backups und Kataloge von der SAP HANA-Datenbank an den AWS Backint Agent übertragen werden.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren Anwendungen, Software-as-a-Service (SaaS)-Anwendungen und AWS-Services für Ziele wie AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen Konten bereit.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.

- AWS Systems Manager unterstützt Sie beim Anzeigen und Steuern Ihrer Infrastruktur in AWS. Mit der Systems Manager-Konsole können Sie Betriebsdaten aus mehreren AWS-Services anzeigen und Betriebsaufgaben in Ihren AWS-Ressourcen automatisieren.

Code

Der Code für dieses Muster ist im aws-backint-automated-backup GitHub Repository verfügbar.

Sekunden

Erstellen eines hdbuserstore-Schlüssels SYSTEM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen hdbuserstore-Schlüssel.	1. Navigieren Sie zu `/usr/sap/<SID>/HDB<InstNo>/exe`.
	2. Führen Sie den folgenden Befehl mitXX als Instance-Nummer der SAP HANA-Datenbank aus.
	`hdbuserstore -i set SYSTEM <hostname>:3XX13@SYSTEMDB SYSTEM`
	Führen Sie beispielsweise für einen SAP HANA-Hostsaphanadb mit der Instance-Nummer den folgenden Befehl `00`aus.
	`hdbuserstore -i set SYSTEM saphanadb:30013@SYSTEMDB SYSTEM`
		AWS-Administrator, SAP HANA-Administrator

Installieren von AWS Backint Agent

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS Backint Agent.	Folgen Sie den Anweisungen unter Installieren und Konfigurieren des AWS Backint Agent für SAP HANA in der AWS Backint Agent-Dokumentation.	AWS-Administrator, SAP HANA-Administrator

Erstellen des Systems Manager-Befehlsdokuments

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Systems Manager-Befehlsdokument.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Systems Manager-Konsole. 2. Wählen Sie Dokumente und dann In meinem Besitz aus. 3. Vergewissern Sie sich, dass Sie sich in derselben AWS-Region wie Ihre SAP HANA-Datenbank befinden. 4. Wählen Sie Create document ,Command oder session, um Ihr Dokument zu erstellen. 5. Verwenden Sie einen eindeutigen und beschreibenden Namen ohne Leerzeichen (z. B. SAP HANA-Backup).	AWS-Administrator, SAP HANA-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Stellen Sie sicher, dass der Dokumenttyp auf Befehlsdokument festgelegt ist. 7. Unter dem Header Inhalt befindet sich ein Beispielcode. Stellen Sie sicher, dass Sie den JSON-Codetyp auswählen, und ersetzen Sie den Code durch den Code aus der `HDB_Backup_SSM_Document.json` Datei aus dem GitHub Repository . 8. Wählen Sie Create document (Dokument erstellen) aus. 9. Überprüfen Sie Ihr Dokument im Abschnitt Eigentum von mir.	

Planen von Backups in regelmäßigen Abständen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie regelmäßige Backups mit Amazon EventBridge.	1. Öffnen Sie die Amazon-EventBridgeKonsole, wählen Sie Regeln und dann Regel erstellen aus. 2. Geben Sie auf dem Bildschirm Regeldetail definieren einen eindeutigen Namen und eine eindeutige Beschreib	AWS-Administrator, SAP HANA-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ung für Ihre Regel ein und verwenden Sie den Standard-Event-Bus. 3. Wählen Sie unter Regeltyp die Option Planen und dann Weiter aus. 4. Wählen Sie auf dem Bildschirm Zeitplan definieren das entsprech ende Zeitplanmuster und den entsprechenden Cron- oder Rate-Ausdruck basierend auf der erforderl ichen Häufigkeit aus. 5. Wählen Sie auf dem Bildschirm Ziele auswählen für Zieltyp die Option AWS-Service aus. Wählen Sie unter Ziel auswählen die Option Systems Manager Run Command aus. 6. Wählen Sie das Dokument aus, das Sie zuvor erstellt haben. 7. Geben Sie unter Zielschlü ssel und Zielwert die Instance-ID an. Sie können Tag-Namen und Tag-Werte verwenden, um mehrere Instances hinzuzufügen. 8. Wählen Sie unter Konfiguri eren von Automatis ierungsparametern die Option Konstant	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für inkrementelle oder differentielle Sicherung en aus. Wenn Sie eine vollständige Sicherung wünschen, wählen Sie Keine Parameter aus. 9. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene Rolle verwenden möchten. Wenn Sie eine vorhandene Rolle verwenden, stellen Sie sicher, dass sie über die Richtlinien verfügt, die zum Aufrufen des Ziels erforderl ich sind. 10. Behalten Sie die zusätzlic hen Standardeinstellungen bei und wählen Sie Weiter aus. 11. Der Bildschirm Tags konfigurieren ist optional. Wählen Sie Next aus. 12. Überprüfen Sie auf dem Bildschirm Überprüfen und erstellen die Regeleins tellungen und wählen Sie Erstellen aus. Die Regel sollte erfolgreich erstellt werden. Sie können den Backup-Er folg über den S3-Bucket-Pfad überprüfen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`s3:/<your_bucket_name>/<target folder>/<SID>/usr/sap/<SID>/SYS/global/hdb/backint/DB_<SID>/` Sie können Backups auch aus dem SAP HANA-Backup-Katalog überprüfen.	

Zugehörige Ressourcen

- AWS Backint Agent für SAP HANA
- Installieren und Konfigurieren des AWS Backint Agent für SAP HANA

Blockieren des öffentlichen Zugriffs auf Amazon RDS mithilfe von Cloud Custodian

Erstellt von abhay kumar (AWS) und Dwarikapatra (AWS)

Umgebung: Produktion	Technologien: Datenbanken; Sicherheit, Identität, Compliance	Workload: Alle anderen Workloads; Open-Source
AWS-Services: Amazon RDS		

Übersicht

Viele Organisationen führen ihre Workloads und Services auf mehreren Cloud-Anbietern aus. In diesen Hybrid-Cloud-Umgebungen benötigt die Cloud-Infrastruktur zusätzlich zur Sicherheit der einzelnen Cloud-Anbieter eine strikte Cloud-Governance. Eine Cloud-Datenbank wie Amazon Relational Database Service (Amazon RDS) ist ein wichtiger Service, der auf Zugriffs- und Berechtigungsschwachstellen überwacht werden muss. Obwohl Sie den Zugriff auf die Amazon-RDS-Datenbank einschränken können, indem Sie eine Sicherheitsgruppe konfigurieren, können Sie eine zweite Schutzebene hinzufügen, um Aktionen wie den öffentlichen Zugriff zu verbieten. Die Sicherstellung, dass der öffentliche Zugriff blockiert ist, unterstützt Sie bei der Einhaltung der Datenschutz-Vorschriften (GDPR), des Health Insurance Portability and Accountability Act (HIPAA), des National Institute of Standards and Technology (NIST) und des Payment Card Industry Data Security Standard (PCI DSS).

Cloud Custodian ist eine Open-Source-Regel-Engine, mit der Sie Zugriffsbeschränkungen für Amazon Web Services (AWS)-Ressourcen wie Amazon RDS erzwingen können. Mit Cloud Custodian können Sie Regeln festlegen, die die Umgebung anhand definierter Sicherheits- und Compliance-Standards validieren. Sie können Cloud Custodian verwenden, um Ihre Cloud-Umgebungen zu verwalten, indem Sie dazu beitragen, die Einhaltung von Sicherheitsrichtlinien, Tag-Richtlinien und Garbage Collection ungenutzter Ressourcen und Kostenmanagement sicherzustellen. Mit Cloud Custodian können Sie eine einzige Schnittstelle für die Implementierung von Governance in einer Hybrid-Cloud-Umgebung verwenden. Sie könnten beispielsweise die Cloud-Custodiaan-Schnittstelle verwenden, um mit AWS und Microsoft Azure zu interagieren, wodurch der Aufwand

für die Arbeit mit Mechanismen wie AWS Config, AWS-Sicherheitsgruppen und Azure-Richtlinien reduziert wird.

Dieses Muster enthält Anweisungen zur Verwendung von Cloud Custodian in AWS, um die Einschränkung der öffentlichen Zugänglichkeit auf Amazon RDS-Instances durchzusetzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Schlüsselpaar
- AWS Lambda installiert

Architektur

Zieltechnologie-Stack

- Amazon RDS
- AWS CloudTrail
- AWS Lambda
- Cloud Custodian

Zielarchitektur

Das folgende Diagramm zeigt Cloud Custodian, das die Richtlinie in Lambda bereitstellt, AWS, das das `CreateDBInstance` Ereignis CloudTrail initiiert, und die Lambda-Funktionseinstellung auf Amazon RDS `PubliclyAccessible` auf „false“.

Tools

AWS-Services

- AWS CloudTrail unterstützt Sie bei der Prüfung der Governance, Compliance und des Betriebsrisikos Ihres AWS-Kontos.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.

Andere Tools

- Cloud Custodian vereinheitlicht die Tools und Skripts, die viele Organisationen zur Verwaltung ihrer öffentlichen Cloud-Konten verwenden, in einem Open-Source-Tool. Es verwendet eine zustandslose Regel-Engine für die Definition und Durchsetzung von Richtlinien mit Metriken, strukturierten Ausgaben und detaillierten Berichten für die Cloud-Infrastruktur. Es lässt sich eng in eine Serverless-Laufzeit integrieren, um Korrektur und Reaktion in Echtzeit mit geringem Betriebsaufwand zu ermöglichen.

Polen

Einrichten der AWS CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS CLI.	Um AWS CLI zu installieren, folgen Sie den Anweisungen in der AWS-Dokumentation.	AWS-Administrator
Richten Sie AWS-Anmeldeinformationen ein.	Konfigurieren Sie die Einstellungen, die die AWS CLI für die Interaktion mit AWS verwendet, einschließlich der AWS-Region und des Ausgabeformats, das Sie verwenden möchten.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$>aws configure`
	`AWS Access Key ID`
	` [None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	` [None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	` [None]:`
	`Default output format`
	` [None]:`
	
	Weitere Informationen finden Sie in der AWS-Dokumentation.	

Erstellen Sie eine IAM-Rolle.	Führen Sie den folgenden Befehl aus, um eine IAM-Rolle mit der Lambda-Ausführungsrolle zu erstellen.
	
	`aws iam create-role --`
	`role-name lambda-ex --`
	`assume-role-policy-`
	`document '{"Version":`
	` "2012-10-17","Stat`
	`ement": [{ "Effect":`
	` "Allow", "Principal":`
	` {"Service": "lambda.a`
	`mazonaws.com"},`
	` "Action": "sts:Assu`
	`meRole"}]}`
		AWS DevOps

Einrichten von Cloud Custodian

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Cloud Custodian.	Um Cloud Custodian für Ihr Betriebssystem und Ihre Umgebung zu installieren, folgen Sie den Anweisungen in der Cloud-Custom-Dokumentation.	DevOps Techniker
Überprüfen Sie das Cloud-Kustomschema.	Verwenden Sie den folgenden Befehl, um die vollständige Liste der Amazon-RDS-Ressourcen anzuzeigen, für die Sie Richtlinien ausführen können. `custodian schema aws.rds`	DevOps Techniker
Erstellen Sie die Richtlinie Cloud Custodian.	Speichern Sie den Code, der sich unter der Cloud-Custom-Richtliniendatei befindet, im Abschnitt Zusätzliche Informationen mit einer YAML-Erweiterung.	DevOps Techniker
Definieren Sie Cloud Custodian-Aktionen, um das öffentlich zugängliche Flag zu ändern.	1. Suchen Sie den -Custodian-Code (z. B. `/Users/abcd/custodian/lib/python3.9/site-packages/c7n/resources/rds.py`). 2. Suchen Sie die `RDSSetPublicAvailability` Klasse in `rds.py`und ändern Sie diese Klasse	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mithilfe des Codes, der sich in der Datei c7n resources rds.py im Abschnitt Zusätzliche Informationen befindet.	
Führen Sie einen Testlauf durch.	(Optional) Verwenden Sie den folgenden Befehl, um zu überprüfen, welche Ressourcen von der Richtlinie identifiziert werden, ohne Aktionen für die Ressourcen auszuführen. `custodian run -dryrun <policy_name>.yaml -s <output_directory>`	DevOps Techniker

Bereitstellen der Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Richtlinie mithilfe von Lambda bereit.	Verwenden Sie den folgenden Befehl, um die Lambda-Funktion zu erstellen, die die Richtlinie ausführt. `custodian run -s policy.yaml` Diese Richtlinie wird dann durch das AWS CloudTrail `CreateDBInstance` -Ereignis initiiert.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Daher setzt AWS Lambda das öffentlich zugängliche Flag für Instances, die den Kriterien entsprechen, auf „false“.	

Zugehörige Ressourcen

- AWS Lambda
- Amazon RDS
- Cloud Custodian

Zusätzliche Informationen

YAML-Datei für Cloud-Custom-Richtlinien

```
policies:
  - name: "block-public-access"
    resource: rds
    description: |
      This Enforcement blocks public access for RDS instances.
    mode:
      type: cloudtrail
      events:
        - event: CreateDBInstance # Create RDS instance cloudtrail event
          source: rds.amazonaws.com
          ids: requestParameters.dBInstanceIdentifier
      role: arn:aws:iam::1234567890:role/Custodian-compliance-role
    filters:
      - type: event
        key: 'detail.requestParameters.publiclyAccessible'
        value: true
    actions:
      - type: set-public-access
        state: false
```

c7n-Ressourcen rds.py-Datei

```
@actions.register('set-public-access')
 class RDSSetPublicAvailability(BaseAction):

     schema = type_schema(
         "set-public-access",
         state={'type': 'boolean'})
     permissions = ('rds:ModifyDBInstance',)

     def set_accessibility(self, r):
         client = local_session(self.manager.session_factory).client('rds')
         waiter = client.get_waiter('db_instance_available')
         waiter.wait(DBInstanceIdentifier=r['DBInstanceIdentifier'])
         client.modify_db_instance(
             DBInstanceIdentifier=r['DBInstanceIdentifier'],
             PubliclyAccessible=self.data.get('state', False))


     def process(self, rds):
         with self.executor_factory(max_workers=2) as w:
             futures = {w.submit(self.set_accessibility, r): r for r in rds}
             for f in as_completed(futures):
                 if f.exception():
                     self.log.error(
                         "Exception setting public access on %s  \n %s",
                         futures[f]['DBInstanceIdentifier'], f.exception())
         return rds
```

Integration von Security Hub

Cloud Custodian kann in AWS Security Hub integriert werden, um Sicherheitserkenntnisse zu senden und Korrekturmaßnahmen zu versuchen. Weitere Informationen finden Sie unter Ankündigung der Integration von Cloud-Kustomen in AWS Security Hub.

Konfigurieren von schreibgeschütztem Routing in einer AlwaysOn-Verfügbarkeitsgruppe in SQL Server auf AWS

Erstellt von Subhani Shaik (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Infrastruktur	Workload: Microsoft
AWS-Services: AWS Managed Microsoft AD; Amazon EC2		

Übersicht

Dieses Muster behandelt die Verwendung des sekundären Standby-Replikats in SQL Server Always On durch Auslagern der schreibgeschützten Workloads vom primären Replikat auf das sekundäre Replikat.

Die Datenbankspiegelung weist eine one-to-one Zuordnung auf. Sie können die sekundäre Datenbank nicht direkt lesen, daher müssen Sie Snapshots erstellen. Die AlwaysOn-Verfügbarkeitsgruppenfunktion wurde in Microsoft SQL Server 2012 eingeführt. In späteren Versionen wurden Hauptfunktionen eingeführt, einschließlich schreibgeschütztem Routing. In AlwaysOn-Verfügbarkeitsgruppen können Sie die Daten direkt aus dem sekundären Replikat lesen, indem Sie den Replikatmodus auf schreibgeschützt ändern.

Die AlwaysOn-Verfügbarkeitsgruppenlösung unterstützt Hochverfügbarkeit (HA), Notfallwiederherstellung (DR) und eine Alternative zur Datenbankspiegelung. AlwaysOn-Verfügbarkeitsgruppen funktionieren auf Datenbankebene und maximieren die Verfügbarkeit einer Reihe von Benutzerdatenbanken.

SQL Server verwendet den schreibgeschützten Routing-Mechanismus, um die eingehenden schreibgeschützten Verbindungen an das sekundäre Lesereplikat umzuleiten. Um dies zu erreichen, sollten Sie der Verbindungszeichenfolge die folgenden Parameter und Werte hinzufügen:

- `ApplicationIntent=ReadOnly`
- `Initial Catalog=<database name>`

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einer Virtual Private Cloud (VPC), zwei Availability Zones, privaten Subnetzen und einer Sicherheitsgruppe
- Zwei Amazon Elastic Compute Cloud (Amazon EC2)-Maschinen mit SQL Server 2019 Enterprise Edition Amazon Machine Image mit Windows Server Failover Clustering (WSFC) ,die auf Instance-Ebene konfiguriert sind, und einer AlwaysOn-Verfügbarkeitsgruppe, die auf SQL Server-Ebene zwischen dem Primärknoten (`WSFCNODE1`) und dem Sekundärknoten (`WSFCNODE2`) konfiguriert ist, die Teil des AWS Directory Service for Microsoft Active Directory-Verzeichnisses namens sind `tagechtalk.com`
- Ein oder mehrere Knoten, die für die Annahme `read-only` im sekundären Replikat konfiguriert sind
- Ein Listener mit dem Namen `SQLAG1` für die AlwaysOn-Verfügbarkeitsgruppe
- SQL Server Database Engine, die mit demselben Servicekonto auf zwei Knoten ausgeführt wird
- SQL Server Management Studio (SSMS)
- Eine Testdatenbank mit dem Namen `test`

Produktversionen

- SQL Server 2014 und höher

Architektur

Zieltechnologie-Stack

- Amazon EC2
- AWS Managed Microsoft AD
- Amazon FSx

Zielarchitektur

Das folgende Diagramm zeigt, wie der Always On Availability Group (AG)-Listener Abfragen umleitet, die den `ApplicationIntent` Parameter in der Verbindung zum entsprechenden sekundären Knoten enthalten.

1. Eine Anforderung wird an den Verfügbarkeitsgruppen-Listener AlwaysOn gesendet.
2. Wenn die Verbindungszeichenfolge nicht über den -`ApplicationIntent`Parameter verfügt, wird die Anforderung an die primäre Instance gesendet.
3. Wenn die Verbindungszeichenfolge enthält`ApplicationIntent=ReadOnly`, wird die Anforderung an die sekundäre Instance mit schreibgeschützter Routing-Konfiguration gesendet, die WSFC mit einer Always On-Verfügbarkeitsgruppe ist.

Tools

AWS-Services

- AWS Directory Service for Microsoft Active Directory ermöglicht es Ihren verzeichnisfähigen Workloads und AWS-Ressourcen, Microsoft Active Directory in der AWS Cloud zu verwenden.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon FSx bietet Dateisysteme, die branchenübliche Konnektivitätsprotokolle unterstützen und eine hohe Verfügbarkeit und Replikation über AWS-Regionen hinweg bieten.

Andere -Services

- SQL Server Management Studio (SSMS) ist ein Tool zum Verbinden, Verwalten und Verwalten der SQL Server-Instances.
- sqlcmd ist ein Befehlszeilendienstprogramm.

Bewährte Methoden

Weitere Informationen zu AlwaysOn-Verfügbarkeitsgruppen finden Sie in der SQL Server-Dokumentation.

Polen

Einrichten von schreibgeschütztem Routing

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Replikate auf schreibgeschützt.	Um sowohl das primäre als auch das sekundäre Replikat auf schreibgeschützt zu aktualisieren, stellen Sie von SSMS aus eine Verbindun g zum primären Replikat her und führen Sie den Code aus Schritt 1 im Abschnitt Zusätzlic he Informationen aus.	DBA
Erstellen Sie die Routing-URL.	Um eine Routing-URL für beide Replikate zu erstellen , führen Sie den Code aus Schritt 2 im Abschnitt Zusätzlic he Informationen aus. In diesem Code `tagechtal k.com` ist der Name des AWS Managed Microsoft AD-Verzeichnisses.	DBA
Erstellen Sie die Routing-Liste.	Um die Routing-Liste für beide Replikate zu erstellen, führen Sie den Code von Schritt 3 im Abschnitt Zusätzliche Informati onen aus.	DBA
Validieren Sie die Routing-L iste.	Stellen Sie von SQL Server Management Studio aus eine Verbindung zur primären Instance her und führen Sie den Code Schritt 4 aus dem Abschnitt Zusätzliche Informati	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen aus, um die Routing-L iste zu validieren.	

Testen des schreibgeschützten Routings

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe des ApplicationIntent Parameters eine Verbindung her.	1. Stellen Sie von SSMS aus eine Verbindun g mit dem Listener-Namen der AlwaysOn-Verfügbarkeitsgrup pe mit her`ApplicationIntent=ReadOnly; Initial Catalog=test` . 2. Die Verbindung wird mit dem sekundären Replikat hergestellt. Führen Sie zum Testen den folgenden Befehl aus, um den Namen des verbundenen Servers anzuzeigen. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')` Die Ausgabe zeigt den aktuellen sekundäre n Replikatnamen (`WSFCN0DE2`).	DBA
Führen Sie ein Failover durch.	1. Stellen Sie von SSMS aus eine Verbindung mit	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Listener-Namen der AlwaysOn-Verfügbar keitsgruppe her. 2. Stellen Sie sicher, dass die primäre und sekundäre Datenbank synchron sind, ohne Datenverlust. 3. Führen Sie ein Failover durch, damit das aktuelle primäre Replikat zum sekundären Replikat und das sekundäre Replikat zum primären Replikat wird. 4. Stellen Sie von SSMS aus eine Verbindun g mit dem Listener-Namen der AlwaysOn-Verfügbarkeitsgrup pe mit her`ApplicationIntent=ReadOnly; Initial Catalog=test` . 5. Die Verbindung wird mit dem sekundären Replikat hergestellt. Um dies zu testen, zeigen Sie den Namen des verbundenen Servers an, indem Sie den folgenden Befehl ausführen. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Es wird der aktuelle sekundäre Replikatname () angezeigt`WSFCNODE1` .	

Herstellen einer Verbindung mithilfe des Befehlszeilen-Hilfsprogramms sqlcmd

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung mithilfe von sqlcmd her.	Um eine Verbindung von sqlcmd herzustellen, führen Sie den Code von Schritt 5 im Abschnitt Zusätzliche Informationen an der Eingabeaufforderung aus. Nachdem Sie verbunden sind, führen Sie den folgenden Befehl aus, um den Namen des verbundenen Servers anzuzeigen. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios') .` Die Ausgabe zeigt den aktuellen sekundären Replikatnamen (`WSFCNODE1`) an.	DBA

Fehlerbehebung

Problem	Lösung
Das Erstellen des Listeners schlägt mit der Meldung „Der WSFC-Cluster konnte die Netzwerknamen-Ressource nicht online schalten“ fehl.	Weitere Informationen finden Sie im Microsoft-Blogbeitrag Listener-Fails mit der Meldung „Der WSFC-Cluster konnte die Netzwerknamen-Ressource nicht online schalten“ erstellen.
Mögliche Probleme, einschließlich anderer Listener-Probleme oder Netzwerkzugriffsprobleme.	Weitere Informationen finden Sie unter Fehlerbehebung bei der Konfiguration von Always On Availability Groups (SQL Server) in der Microsoft-Dokumentation.

Zugehörige Ressourcen

- Konfigurieren von schreibgeschütztem Routing für eine AlwaysOn-Verfügbarkeitsgruppe
- Fehlerbehebung bei der Konfiguration von Always On Availability Groups (SQL Server)

Zusätzliche Informationen

Schritt 1. Aktualisieren Sie die Replikate auf schreibgeschützt

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
```

Schritt 2. Erstellen der Routing-URL

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode1.tagechtalk.com:1433'))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode2.tagechtalk.com:1433'))
```

```
GO
```

Schritt 3. Erstellen der Routing-Liste

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH
 (PRIMARY_ROLE(READ_ONLY_ROUTING_LIST=('WSFCNODE2','WSFCNODE1')));
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (PRIMARY_ROLE
 (READ_ONLY_ROUTING_LIST=('WSFCNODE1','WSFCNODE2')));
GO
```

Schritt 4. Validieren der Routing-Liste

```
SELECT AGSrc.replica_server_name AS PrimaryReplica, AGRepl.replica_server_name AS
 ReadOnlyReplica, AGRepl.read_only_routing_url AS RoutingURL , AGRL.routing_priority
 AS RoutingPriority FROM sys.availability_read_only_routing_lists AGRL INNER JOIN
 sys.availability_replicas AGSrc ON AGRL.replica_id = AGSrc.replica_id INNER JOIN
 sys.availability_replicas AGRepl ON AGRL.read_only_replica_id = AGRepl.replica_id
 INNER JOIN sys.availability_groups AV ON AV.group_id = AGSrc.group_id ORDER BY
 PrimaryReplica
```

Schritt 5. SQL Command Utility

```
sqlcmd -S SQLAG1,1433 -E -d test -K ReadOnly
```

Stellen Sie eine Connect über einen SSH-Tunnel in pgAdmin her

Erstellt von Jeevan Shetty (AWS) und Bhanu Ganesh Gudivada (AWS)

Umgebung: Produktion	Technologien: Datenbanken; Sicherheit, Identität, Compliance	Arbeitslast: Open Source
AWS-Dienste: Amazon RDS; Amazon Aurora		

Übersicht

Aus Sicherheitsgründen ist es immer gut, Datenbanken in einem privaten Subnetz zu platzieren. Abfragen an der Datenbank können ausgeführt werden, indem eine Verbindung über einen Amazon Elastic Compute Cloud (Amazon EC2) -Bastion-Host in einem öffentlichen Subnetz in der Amazon Web Services (AWS) Cloud hergestellt wird. Dies erfordert die Installation von Software wie pgAdmin oder DBeaver, die häufig von Entwicklern oder Datenbankadministratoren verwendet werden, auf dem Amazon EC2 EC2-Host.

Um pgAdmin auf einem Linux-Server auszuführen und über einen Webbrowser darauf zuzugreifen, müssen zusätzliche Abhängigkeiten installiert, Berechtigungen eingerichtet und konfiguriert werden.

Als alternative Lösung können Entwickler oder Datenbankadministratoren eine Verbindung zu einer PostgreSQL-Datenbank herstellen, indem sie pgAdmin verwenden, um einen SSH-Tunnel von ihrem lokalen System aus zu aktivieren. Bei diesem Ansatz verwendet pgAdmin den Amazon EC2 EC2-Host im öffentlichen Subnetz als Zwischenhost, bevor eine Verbindung zur Datenbank hergestellt wird. Das Diagramm im Abschnitt Architektur zeigt das Setup.

Hinweis: Stellen Sie sicher, dass die an die PostgreSQL-Datenbank angehängte Sicherheitsgruppe eine Verbindung über Port 5432 vom Amazon EC2 EC2-Host aus zulässt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein bestehendes AWS-Konto
- Eine virtuelle private Cloud (VPC) mit einem öffentlichen Subnetz und einem privaten Subnetz

- Eine EC2-Instanz mit einer angehängten Sicherheitsgruppe
- Eine Amazon Aurora PostgreSQL-kompatible Edition-Datenbank mit einer angehängten Sicherheitsgruppe
- Ein Secure Shell (SSH) -Schlüsselpaar für die Einrichtung des Tunnels

Produktversionen

- pgAdmin versie 6.2+
- Amazon Aurora PostgreSQL-kompatible Edition Version 12.7+

Architektur

Zieltechnologie-Stack

- Amazon EC2
- Amazon Aurora PostgreSQL-kompatibel

Zielarchitektur

Das folgende Diagramm zeigt die Verwendung von pgAdmin mit einem SSH-Tunnel, um über ein Internet-Gateway eine Verbindung zur EC2-Instance herzustellen, die eine Verbindung zur Datenbank herstellt.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

Andere Dienste

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Epen

Stellen Sie die Verbindung her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Server.	Wählen Sie in pgAdmin Create und dann Server aus. Zusätzliche Hilfe zur Einrichtung von pgAdmin für die Registrierung eines Servers, die Konfiguration einer Verbindung und die Verbindung über SSH-Tunneling mithilfe des Server-Dialogs finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	DBA
Geben Sie einen Namen für den Server ein.	Geben Sie auf der Registerkarte Allgemein einen Namen ein.	DBA
Geben Sie die Datenbankdetails ein.	Geben Sie auf der Registerkarte Verbindung Werte für Folgendes ein: • Hostname/Adresse • Port • Wartungsdatenbank • Username • Passwort	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Amazon EC2-Serverdetails ein.	Geben Sie auf der Registerkarte SSH-Tunnel die Details der Amazon EC2 EC2-Instance ein, die sich im öffentlichen Subnetz befindet. • Setzen Sie SSH-Tunnelling verwenden auf Ja, um anzugeben, dass pgAdmin bei der Verbindung mit dem angegebenen Server einen SSH-Tunnel verwenden soll. • Geben Sie im Feld Tunnelhost den Namen oder die IP-Adresse des SSH-Hosts an (z. B. 10.x.x.x). • Geben Sie im Feld Tunnel-Port den Port des SSH-Hosts an (z. B. 22). • Geben Sie im Feld Benutzername den Namen eines Benutzers mit Anmeldeberechtigungen für den SSH-Host an (z. B. ec2-user). • Geben Sie den Authentifizierungstyp als Identitätsdatei an, damit pgAdmin bei der Verbindung eine private Schlüsseldatei verwendet. • Geben Sie den Speicherort der Privacy Enhanced Mail (PEM) -Datei in das	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Feld Identitätsdatei ein. Die.pem-Datei ist das Amazon EC2 EC2-Schlüsselpaar.	
Speichern und verbinden.	Wählen Sie Speichern, um die Einrichtung abzuschließen und mithilfe des SSH-Tunnels eine Verbindung zur Aurora PostgreSQL-kompatiblen Datenbank herzustellen.	DBA

Zugehörige Ressourcen

- Dialogfeld „Server“
- Connect zum Server herstellen

Konvertieren von JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL

Erstellt von Pinesh Singal (AWS) und Lokesh Gurram (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Datenbanken; Migration
AWS-Services: Amazon Aurora; Amazon RDS		

Übersicht

Dieser Migrationsprozess für den Wechsel von einer lokalen zur Amazon Web Services (AWS) Cloud verwendet das AWS Schema Conversion Tool (AWS SCT), um den Code aus einer Oracle-Datenbank in eine PostgreSQL-Datenbank zu konvertieren. Der Großteil des Codes wird automatisch von AWS SCT konvertiert. JSON-bezogene Oracle-Abfragen werden jedoch nicht automatisch konvertiert.

Ab Oracle 12.2 unterstützt Oracle Database verschiedene JSON-Funktionen, die bei der Konvertierung von JSON-basierten Daten in ROW-basierte Daten helfen. AWS SCT konvertiert JSON-basierte Daten jedoch nicht automatisch in eine Sprache, die von PostgreSQL unterstützt wird.

Dieses Migrationsmuster konzentriert sich hauptsächlich auf die manuelle Konvertierung der JSON-bezogenen Oracle-Abfragen mit Funktionen wie `JSON_OBJECT`, `JSON_ARRAYAGG`und `JSON_TABLE` von einer Oracle-Datenbank in eine PostgreSQL-Datenbank.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine lokale Oracle-Datenbank-Instance (in Betrieb)

- Eine Datenbank-Instance von Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL – kompatible Edition (in Betrieb)

Einschränkungen

- JSON-bezogene Abfragen erfordern ein festes - KEY und -VALUEFormat. Wenn Sie dieses Format nicht verwenden, wird das falsche Ergebnis zurückgegeben.
- Wenn eine Änderung der JSON-Struktur neue - KEY und -VALUEPaare im Ergebnisabschnitt hinzufügt, muss die entsprechende Prozedur oder Funktion in der SQL-Abfrage geändert werden.
- Einige JSON-bezogene Funktionen werden in früheren Versionen von Oracle und PostgreSQL unterstützt, verfügen jedoch über weniger Funktionen.

Produktversionen

- Oracle Database Version 12.2 und höher
- Amazon RDS für PostgreSQL oder Aurora PostgreSQL – kompatible Version 9.5 und höher
- AWS SCT neueste Version (getestet mit Version 1.0.664)

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank-Instance mit Version 19c

Zieltechnologie-Stack

- Eine mit Amazon RDS for PostgreSQL oder Aurora PostgreSQL kompatible Datenbank-Instance mit Version 13

Zielarchitektur

1. Verwenden Sie AWS SCT mit dem JSON-Funktionscode, um den Quellcode von Oracle in PostgreSQL zu konvertieren.
2. Die Konvertierung erzeugt von PostgreSQL unterstützte migrierte .sql-Dateien.

3. Konvertieren Sie die nicht konvertierten Oracle-JSON-Funktionscodes manuell in PostgreSQL-JSON-Funktionscodes.
4. Führen Sie die SQL-Dateien auf der Aurora PostgreSQL-kompatiblen DB-Ziel-Instance aus.

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Andere -Services

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht.
- pgAdmin oder DBeaver . pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können. DBeaver ist ein universelles Datenbank-Tool.

Bewährte Methoden

Die Oracle-Abfrage hat den Typ `CAST` als Standard bei Verwendung der `JSON_TABLE` Funktion . Eine bewährte Methode besteht darin, auch `CAST` in PostgreSQL zu verwenden, wobei doppelte größere Zeichen verwendet werden (>>).

Weitere Informationen finden Sie unter Postgres_SQL_Read_JSON im Abschnitt Zusätzliche Informationen.

Polen

Generieren der JSON-Daten in den Oracle- und PostgreSQL-Datenbanken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die JSON-Daten in der Oracle-Datenbank.	Erstellen Sie eine Tabelle in der Oracle-Datenbank und speichern Sie die JSON-Daten in der `CLOB` Spalte . Verwenden Sie das Oracle_Table_Creation_Insert_Script, das sich im Abschnitt Zusätzliche Informationen befindet.	Migrationsingenieur
Speichern Sie die JSON-Daten in der PostgreSQL-Datenbank.	Erstellen Sie eine Tabelle in der PostgreSQL-Datenbank und speichern Sie die JSON-Daten in der `TEXT` Spalte . Verwenden Sie das Postgres_Table_Creation_Insert_Script, das sich im Abschnitt Zusätzliche Informationen befindet.	Migrationsingenieur

Konvertieren des JSON in das ROW-Format

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie die JSON-Daten in der Oracle-Datenbank.	Schreiben Sie eine Oracle SQL-Abfrage, um die JSON-Daten im ROW-Format zu lesen. Weitere Informationen und Beispielsyntax finden Sie unter Oracle_SQL_Read_JS	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ON im Abschnitt Zusätzliche Informationen.	
Konvertieren Sie die JSON-Daten in der PostgreSQL-Datenbank.	Schreiben Sie eine PostgreSQL-Abfrage, um die JSON-Daten im ROW-Format zu lesen. Weitere Informationen und Beispielsyntax finden Sie unter Postgres_SQL_Read_JSON im Abschnitt Zusätzliche Informationen.	Migrationsingenieur

Manuelles Konvertieren der JSON-Daten mithilfe der SQL-Abfrage und Melden der Ausgabe im JSON-Format

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Aggregationen und Validierungen für die Oracle SQL-Abfrage durch.	Um die JSON-Daten manuell zu konvertieren, führen Sie einen Join, eine Aggregation und eine Validierung für die Oracle SQL-Abfrage durch und melden Sie die Ausgabe im JSON-Format. Verwenden Sie den Code unter Oracle_SQL_JSON_Aggregation_Join im Abschnitt Zusätzliche Informationen. 1. JOIN – Die JSON-formatierten Daten werden als Eingabeparameter an die Abfrage übergeben. Zwischen diesen statischen Daten und den JSON-	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Daten in der Oracle-DB-Tabelle wird eine innere JOIN erstelltaws_test_table . 2. Aggregation mit Validierung – Die JSON-Daten haben -KEY und -VALUEParameter mit Werten wie accountNumber , parentAccountNumber businessUnitId und positionId , die für COUNT - SUM und -Aggregationen verwendet werden. 3. JSON-Format – Nach dem Join und der Aggregation werden die Daten im JSON-Format unter Verwendung von JSON_OBJECT und gemeldetJSON_ARRAYAGG .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Aggregationen und Validierungen für die Postgres-SQL-Abfrage durch.	Um die JSON-Daten manuell zu konvertieren, führen Sie einen Join, eine Aggregation und eine Validierung für die PostgreSQL-Abfrage durch und melden Sie die Ausgabe im JSON-Format. Verwenden Sie den Code unter Postgres_SQL_JSON_Aggregation_Join im Abschnitt Zusätzliche Informationen. 1. JOIN – Die JSON-formatierten Daten (`tab1`) werden als Eingabeparameter an die -`WITH`Klauselabfrage übergeben. Zwischen diesen statischen Daten und den JSON-Daten, die sich in der `tab` Tabelle befinden, wird eine JOIN erstellt. Eine JOIN wird auch mit der -`WITH`Klausel erstellt, die JSON-Daten in der `aws_test_pg_table` Tabelle enthält. 2. Aggregation – Die JSON-Daten haben - `KEY` und `parentAccountNumber` -`VALUE`Parameter mit Werten wie `accountNumber` , `businessU`	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`nitId` , und `positionI d` , die für die `COUNT` Aggregationen `SUM` und verwendet werden. 3. JSON-Format – Nach dem Join und der Aggregation werden die Daten im JSON-Format unter Verwendung von `JSON_BUILD_OBJECT` und gemeldet`JSON_AGG`.	

Konvertieren Sie die Oracle-Prozedur in eine PostgreSQL-Funktion, die JSON-Abfragen enthält

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie die JSON-Abfragen in der Oracle-Pr ozedur in Zeilen.	Verwenden Sie für das Oracle-Beispielverfahren die vorherige Oracle-Abfrage und den Code unterOracle_pr ocedure_with_JSON_Query im Abschnitt Zusätzliche Informati onen.	Migrationsingenieur
Konvertieren Sie die PostgreSQL-Funktionen mit JSON-Abfragen in zeilenbas ierte Daten.	Verwenden Sie für die Beispielfunktionen von PostgreSQL die vorherige PostgreSQL-Abfrage und den Code unter Postgres_ function_with_JSON_Query im Abschnitt Zusätzliche Informati onen.	Migrationsingenieur

Zugehörige Ressourcen

- Oracle-JSON-Funktionen
- PostgreSQL-JSON-Funktionen
- Beispiele für Oracle JSON Functions
- Beispiele für PostgreSQL-JSON-Funktionen
- AWS Schema Conversion Tool

Zusätzliche Informationen

Um JSON-Code von der Oracle-Datenbank in die PostgreSQL-Datenbank zu konvertieren, verwenden Sie der Reihe nach die folgenden Skripts.

1. Oracle_Table_Creation_Insert_Script

```
create table aws_test_table(id number,created_on date default sysdate,modified_on
 date,json_doc clob);

REM INSERTING into EXPORT_TABLE
SET DEFINE OFF;
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc)
values (1,to_date('02-AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022
 12:30:14','DD-MON-YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -'",
    "a]')
|| TO_CLOB(q'[ccount" : {
      "companyId" : "SMGE",
```

```
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
]')
|| TO_CLOB(q'[        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc) values (2,to_date('02-
AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022 12:30:14','DD-MON-
YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "pqr@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -'",
    "account" : {
      "companyId" : "CARS",
      "busin]')
|| TO_CLOB(q'[essUnitId" : 6,
```

```
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
      ]')
|| TO_CLOB(q'[  "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));

commit;
```

2. Postgres_Table_Creation_Insert_Script

```
create table aws_test_pg_table(id int,created_on date ,modified_on date,json_doc text);
insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(1,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
```

```
    "positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');


insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(2,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "a*b**@h**.k**",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -",
```

```
    "account" : {
      "companyId" : "CARS",
      "businessUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');
```

3. Oracle_SQL_Read_JSON

Die folgenden Codeblöcke zeigen, wie Oracle-JSON-Daten in das Zeilenformat konvertiert werden.

Beispielabfrage und Syntax

```
SELECT   JSON_OBJECT(
 'accountCounts' VALUE JSON_ARRAYAGG(
           JSON_OBJECT(
               'businessUnitId' VALUE business_unit_id,
                       'parentAccountNumber' VALUE parent_account_number,
                       'accountNumber' VALUE account_number,
                       'totalOnlineContactsCount' VALUE online_contacts_count,
                       'countByPosition' VALUE
                   JSON_OBJECT(
                       'taxProfessionalCount' VALUE tax_count,
                       'attorneyCount' VALUE attorney_count,
                       'nonAttorneyCount' VALUE non_attorney_count,
```

```
                        'clerkCount' VALUE clerk_count
                               ) ) ) ) FROM
   (SELECT   tab_data.business_unit_id,
           tab_data.parent_account_number,
           tab_data.account_number,
           SUM(1) online_contacts_count,
           SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
           SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
non_attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
 COLUMNS (
         parent_account_number NUMBER PATH
          '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data
     ON ( static_data.parent_account_number = tab_data.parent_account_number
          AND static_data.account_number = tab_data.account_number
          AND static_data.business_unit_id = tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
           tab_data.parent_account_number,
```

```
            tab_data.account_number );
```

Das JSON-Dokument speichert die Daten als Sammlungen. Jede Sammlung kann - KEY und -VALUEPaare haben. Jedes VALUE kann verschachtelte - KEY und -VALUEPaare haben. Die folgende Tabelle enthält Informationen zum Lesen des spezifischen VALUE aus dem JSON-Dokument.

SCHLÜSSEL	HIERARCHY oder PATH, die zum Abrufen des WERTS verwendet werden sollen	WERT
`profileType`	`metadata` -> `profileType`	„P“
`positionId`	`data` -> `positionId`	„0100“
`accountNumber`	`data` -> Konto -> `accountNumber`	42000

In der vorherigen Tabelle KEY `profileType` ist eine VALUE der `metadata` KEY. Die KEY `positionId` ist eine VALUE der `data` KEY. Der KEY `accountNumber` ist ein VALUE von `account` KEYund der `account` KEY ist ein VALUE von `data` KEY.

Beispiel für ein JSON-Dokument

```
{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
"profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
"positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
```

```
      "businessUnitId" : 7,
"accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}
```

SQL-Abfrage, die verwendet wird, um die ausgewählten Felder aus dem JSON-Dokument abzurufen

```
select parent_account_number,account_number,business_unit_id,position_id from
 aws_test_table aws,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
account_number NUMBER PATH '$.data.account.accountNumber',
business_unit_id NUMBER PATH '$.data.account.businessUnitId',
position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'
)) as sc
```

In der vorherigen Abfrage `JSON_TABLE` ist eine integrierte Funktion in Oracle, die die JSON-Daten in das Zeilenformat konvertiert. Die Funktion JSON_TABLE erwartet Parameter im JSON-Format.

Jedes Element in `COLUMNS` hat eine vordefinierte `PATH`, und es `KEY` wird eine `VALUE` für eine bestimmte geeignete im Zeilenformat zurückgegeben.

Ergebnis der vorherigen Abfrage

PARENT_AC COUNT_NUMBER	ACCOUNT_NUMBER	Bol_UNIT_ID	POSITION_ID
32000	42000	7	0 100
32001	42001	6	0090

4. Postgres_SQL_Read_JSON

Beispielabfrage und Syntax

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::VARCHAR as positionId
from aws_test_pg_table) d ;
```

In Oracle PATH wird verwendet, um die spezifischen KEY und zu identifizierenVALUE. PostgreSQL verwendet jedoch ein HIERARCHY Modell zum Lesen KEY und VALUE aus JSON. Die gleichen JSON-Daten, die unter erwähnt werden, `Oracle_SQL_Read_JSON` werden in den folgenden Beispielen verwendet.

SQL-Abfrage mit Typ CAST nicht zulässig

(Wenn Sie den Typ erzwingenCAST, schlägt die Abfrage mit einem Syntaxfehler fehl.)

```
select *
from (
select (json_doc::json->'data'->'account'->'parentAccountNumber') as
 parentAccountNumber,
(json_doc::json->'data'->'account'->'accountNumber')as accountNumber,
(json_doc::json->'data'->'account'->'businessUnitId') as businessUnitId,
(json_doc::json->'data'->'positionId')as positionId
from aws_test_pg_table) d ;
```

Die Verwendung eines einzigen Größer-als-Operators (>) gibt die für diese VALUE definierte zurückKEY. Zum Beispiel KEY: und `positionId`VALUE: `"0100"`.

Der Typ CAST ist nicht zulässig, wenn Sie den Einzeloperator „größer als“ (>) verwenden.

SQL-Abfrage mit erlaubtem Typ CAST

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) d ;
```

Um den Typ zu verwendenCAST, müssen Sie den Doppelter-größer-als-Operator verwenden. Wenn Sie den Einzeloperator größer als verwenden, gibt die Abfrage den VALUE definierten zurück (z. B. KEY: positionIdund VALUE: "0100"). Die Verwendung des Doppel-größer-als-Operators (>>) gibt den dafür definierten tatsächlichen Wert zurück KEY (z. B. KEY: positionIdund VALUE: 0100, ohne doppelte Anführungszeichen).

Im vorherigen Fall parentAccountNumber ist Typ CAST zu INT, accountNumber ist Typ CAST zu INT, businessUnitId ist Typ zu INT, ist Typ CAST zu und positionId ist Typ CAST zu VARCHAR.

Die folgenden Tabellen zeigen Abfrageergebnisse, die die Rolle des Einzeloperators größer als (>) und des Doppeloperators größer als () erläutern>>.

In der ersten Tabellentabelle verwendet die Abfrage den Einzeloperator „größer als“ (>). Jede Spalte hat den JSON-Typ und kann nicht in einen anderen Datentyp konvertiert werden.

parentAccountNumber	accountNumber	businessUnitId	positionId
2003565430	2003564830	7	„0100“
2005284042	2005284042	6	„0090“
2000272719	2000272719	1	„0100“

In der zweiten Tabelle verwendet die Abfrage den doppelten größer als-Operator (>>). Jede Spalte unterstützt den Typ CAST basierend auf dem Spaltenwert. Zum Beispiel INTEGER in diesem Kontext.

parentAccountNumber	accountNumber	businessUnitId	positionId
2003565430	2003564830	7	0 100
2005284042	2005284042	6	0090
2000272719	2000272719	1	0 100

5. Oracle_SQL_JSON_Aggregation_Join

Beispielabfrage

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
```

```
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
  COLUMNS (
          parent_account_number NUMBER PATH
           '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Um die Daten auf Zeilenebene in das JSON-Format zu konvertieren, verfügt Oracle über integrierte Funktionen wie `JSON_OBJECT`, `JSON_ARRAYJSON_OBJECTAGG`, und `JSON_ARRAYAGG`.

- `JSON_OBJECT` akzeptiert zwei Parameter: `KEY` und `VALUE`. Der`KEY` Parameter sollte hartkodiert oder statisch sein. Der `VALUE` Parameter wird aus der Tabellenausgabe abgeleitet.
- `JSON_ARRAYAGG` akzeptiert `JSON_OBJECT` als Parameter. Dies hilft bei der Gruppierung der Elemente `JSON_OBJECT` als Liste. Wenn Sie beispielsweise ein -`JSON_OBJECT`Element haben, das mehrere Datensätze enthält (mehrere - `KEY` und -`VALUE`Paare im Datensatz), hängt den Datensatz `JSON_ARRAYAGG` an und erstellt eine Liste. Gemäß der Sprache Data Structure `LIST` ist

eine Gruppe von Elementen. In diesem Zusammenhang `LIST` ist eine Gruppe von `JSON_OBJECT` Elementen.

Das folgende Beispiel zeigt ein -`JSON_OBJECT`Element.

```
{
   "taxProfessionalCount": 0,
   "attorneyCount": 0,
   "nonAttorneyCount": 1,
   "clerkCount": 0
}
```

Das nächste Beispiel zeigt zwei `JSON_OBJECT` Elemente, wobei durch eckige Klammern () `LIST` dargestellt wird`[ ]`.

```
[
    {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
,
    {
        "taxProfessionalCount": 2,
        "attorneyCount": 1,
        "nonAttorneyCount": 3,
        "clerkCount":4
      }
]
```

Beispiel für eine SQL-Abfrage

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
```

```
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               )
                        )
                                        )
              )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE   0 END
            )      tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN        1    ELSE
  0 END
            )      attorney_count,

            SUM(CASE    WHEN tab_data.position_id = '0090' THEN        1    ELSE
  0 END
            )      non_attorney_count,

            SUM(CASE    WHEN tab_data.position_id = '0050' THEN        1    ELSE
  0 END
            )      clerk_count

        FROM
            aws_test_table scco,  JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
```

```
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data ON ( static_data.parent_account_number =
 tab_data.parent_account_number
                         AND static_data.account_number = tab_data.account_number

                         AND static_data.business_unit_id =
 tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Beispielausgabe der vorherigen SQL-Abfrage

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
```

```
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

6. Postgres_SQL_JSON_Aggregation_Join

Die integrierten PostgreSQL-Funktionen `JSON_BUILD_OBJECT` und `JSON_AGG` konvertieren die Daten auf ROW-Ebene in das JSON-Format. PostgreSQL `JSON_BUILD_OBJECT` und `JSON_AGG` entsprechen Oracle `JSON_OBJECT` und `JSON_ARRAYAGG`.

Beispielabfrage

```
select
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            )
        )
    )
)
from (
with tab as (select * from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) a ) ,
tab1 as ( select
```

```
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer
 businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
from (
select '{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }'::json as jc) b)
select
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
from tab1,tab
where tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
and tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
and tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
```

Beispielausgabe der vorherigen Abfrage

Die Ausgabe von Oracle und PostgreSQL ist genau gleich.

```
{
  "accountCounts": [
    {
```

```
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

7.Oracle_procedure_with_JSON_Query

Dieser Code konvertiert die Oracle-Prozedur in eine PostgreSQL-Funktion mit JSON-SQL-Abfragen. Es zeigt, wie die Abfrage JSON in Zeilen und umgekehrt transponiert.

```
CREATE OR REPLACE PROCEDURE p_json_test(p_in_accounts_json IN varchar2,
 p_out_accunts_json  OUT varchar2)
IS
BEGIN
/*
p_in_accounts_json paramter should have following format:
       {
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
```

```
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }
*/
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
into p_out_accunts_json
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
        FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( p_in_accounts_json, '$.accounts[*]' ERROR ON ERROR
```

```
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
EXCEPTION
WHEN OTHERS THEN
   raise_application_error(-20001,'Error while running the JSON query');
END;
/
```

Ausführen der Prozedur

Der folgende Codeblock erklärt, wie Sie die zuvor erstellte Oracle-Prozedur mit einer JSON-Beispieleingabe für die Prozedur ausführen können. Außerdem erhalten Sie das Ergebnis oder die Ausgabe dieses Verfahrens.

```
set serveroutput on;
declare
v_out varchar2(30000);
v_in varchar2(30000):= '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }';
begin
  p_json_test(v_in,v_out);
  dbms_output.put_line(v_out);
end;
```

```
/
```

Ausgabe der Prozedur

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

8.Postgres_function_with_JSON_Query

Beispielfunktion

```
CREATE OR REPLACE  FUNCTION f_pg_json_test(p_in_accounts_json  text)
RETURNS text
LANGUAGE plpgsql
AS
$$
DECLARE
```

```
 v_out_accunts_json   text;
BEGIN
SELECT
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            ))))
INTO v_out_accunts_json
FROM (
WITH tab AS (SELECT * FROM (
SELECT (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER AS
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER AS accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER AS businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar AS positionId
FROM aws_test_pg_table) a ) ,
tab1 AS ( SELECT
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
FROM (
SELECT p_in_accounts_json::json AS jc) b)
SELECT
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
```

```
FROM tab1,tab
WHERE tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
AND tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
AND tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
RETURN v_out_accunts_json;
END;
$$;
```

Ausführen der Funktion

```
select    f_pg_json_test('{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }')   ;
```

Funktionsausgabe

Die folgende Ausgabe ähnelt der Oracle-Prozedurausgabe. Der Unterschied besteht darin, dass diese Ausgabe im Textformat vorliegt.

```
{
  "accountCounts": [
    {
      "businessUnitId": "6",
      "parentAccountNumber": "32001",
      "accountNumber": "42001",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
```

```
    },
    {
      "businessUnitId": "7",
      "parentAccountNumber": "32000",
      "accountNumber": "42000",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

Kopieren von Amazon-DynamoDB-Tabellen über -Konten hinweg mithilfe einer benutzerdefinierten Implementierung

Erstellt von Ramkumar Ramanujam (AWS)

Umgebung: Produktion	Quelle: Amazon DynamoDB	Ziel: Amazon DynamoDB
R-Typ: N/A	Workload: Alle anderen Workloads	Technologien: Datenbanken
AWS-Services: Amazon DynamoDB		

Übersicht

Bei der Arbeit mit Amazon DynamoDB in Amazon Web Services (AWS) besteht ein häufiger Anwendungsfall darin, DynamoDB-Tabellen in Entwicklungs-, Test- oder Staging-Umgebungen mit den Tabellendaten zu kopieren oder zu synchronisieren, die sich in der Produktionsumgebung befinden. Standardmäßig verwendet jede Umgebung ein anderes AWS-Konto.

DynamoDB unterstützt jetzt kontoübergreifende Backups mit AWS Backup . Informationen zu den zugehörigen Speicherkosten bei Verwendung von AWS Backup finden Sie unter AWS Backup – Preise. Wenn Sie AWS Backup verwenden, um zwischen Konten zu kopieren, müssen die Quell- und Zielkonten Teil einer AWS Organizations-Organisation sein. Es gibt andere Lösungen für die kontoübergreifende Sicherung und Wiederherstellung mithilfe von AWS-Services wie AWS Data Pipeline oder AWS Glue . Die Verwendung dieser Lösungen erhöht jedoch den Anwendungsaufwand, da mehr AWS-Services bereitgestellt und gewartet werden müssen.

Sie können Amazon DynamoDB Streams auch verwenden, um Tabellenänderungen im Quellkonto zu erfassen. Anschließend können Sie eine AWS Lambda-Funktion initiieren und die entsprechenden Änderungen in der Zieltabelle im Zielkonto vornehmen. Diese Lösung gilt jedoch für Anwendungsfälle, in denen Quell- und Zieltabellen immer synchron gehalten werden müssen. Dies gilt möglicherweise nicht für Entwicklungs-, Test- und Staging-Umgebungen, in denen Daten häufig aktualisiert werden.

Dieses Muster enthält Schritte zur Implementierung einer benutzerdefinierten Lösung zum Kopieren einer Amazon-DynamoDB-Tabelle von einem Konto in ein anderes. Dieses Muster kann mithilfe

gängiger Programmiersprachen wie C#, Java und Python implementiert werden. Wir empfehlen die Verwendung einer Sprache, die von einem AWS SDK unterstützt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten
- DynamoDB-Tabellen in beiden Konten
- Kenntnisse von AWS Identity and Access Management (IAM)-Rollen und -Richtlinien
- Kenntnisse über den Zugriff auf Amazon-DynamoDB-Tabellen mit jeder gängigen Programmiersprache wie C#, Java oder Python

Einschränkungen

Dieses Muster gilt für DynamoDB-Tabellen, die etwa 2 GB oder kleiner sind. Mit zusätzlicher Logik zur Behandlung von Verbindungs- oder Sitzungsunterbrechungen, Drosselung sowie Fehlern und Wiederholungen kann sie für größere Tabellen verwendet werden.

Der DynamoDB-Scanvorgang, der Elemente aus der Quelltabelle liest, kann nur bis zu 1 MB an Daten in einem einzigen Aufruf abrufen. Bei größeren Tabellen, die größer als 2 GB sind, kann diese Einschränkung die Gesamtzeit für die Durchführung einer vollständigen Tabellenkopie erhöhen.

Architektur

Automatisierung und Skalierung

Dieses Muster gilt für DynamoDB-Tabellen, die kleiner sind und etwa 2 GB groß sind.

Um dieses Muster für größere Tabellen anzuwenden, beheben Sie die folgenden Probleme:

- Während des Tabellenkopiervorgangs werden zwei aktive Sitzungen mit unterschiedlichen Sicherheitstoken verwaltet. Wenn der Tabellenkopiervorgang länger dauert als die Token-Ablaufzeiten, müssen Sie Logik einrichten, um die Sicherheitstoken zu aktualisieren.
- Wenn nicht genügend Lesekapazitätseinheiten (RCUs) und Schreibkapazitätseinheiten (WCUs) bereitgestellt werden, werden Lese- oder Schreibvorgänge in der Quell- oder Zieltabelle möglicherweise gedrosselt. Stellen Sie sicher, dass Sie diese Ausnahmen abfangen und behandeln.

- Behandeln Sie alle anderen Fehler oder Ausnahmen und setzen Sie einen Wiederholungsmechanismus ein, um es erneut zu versuchen oder von dort aus fortzufahren, wo der Kopiervorgang fehlgeschlagen ist.

Tools

Tools

- Amazon DynamoDB – Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Die zusätzlichen erforderlichen Tools unterscheiden sich je nach Programmiersprache, die Sie für die Implementierung auswählen. Wenn Sie beispielsweise C# verwenden, benötigen Sie Microsoft Visual Studio und die folgenden NuGet Pakete:
  - `AWSSDK`
  - `AWSSDK.DynamoDBv2`

Code

Der folgende Python-Codeausschnitt löscht und erstellt eine DynamoDB-Tabelle mithilfe der Boto3-Bibliothek neu.

Verwenden Sie nicht die `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` eines IAM-Benutzers, da es sich um langfristige Anmeldeinformationen handelt, die für den programmatischen Zugriff auf AWS-Services vermieden werden sollten. Weitere Informationen zu temporären Anmeldeinformationen finden Sie im Abschnitt Bewährte Methoden.

Die im folgenden Codeausschnitt `TEMPORARY_SESSION_TOKEN` verwendeten `AWS_ACCESS_KEY_ID`, und sind temporäre Anmeldeinformationen`AWS_SECRET_ACCESS_KEY`, die vom AWS Security Token Service (AWS STS) abgerufen werden.

```
import boto3
import sys
import json

#args = input-parameters = GLOBAL_SEC_INDEXES_JSON_COLLECTION,
 ATTRIBUTES_JSON_COLLECTION, TARGET_DYNAMODB_NAME, TARGET_REGION, ...
```

```
#Input param: GLOBAL_SEC_INDEXES_JSON_COLLECTION
#[{"IndexName":"Test-index","KeySchema":[{"AttributeName":"AppId","KeyType":"HASH"},
{"AttributeName":"AppType","KeyType":"RANGE"}],"Projection":
{"ProjectionType":"INCLUDE","NonKeyAttributes":["PK","SK","OwnerName","AppVersion"]}}]

#Input param: ATTRIBUTES_JSON_COLLECTION
#[{"AttributeName":"PK","AttributeType":"S"},
{"AttributeName":"SK","AttributeType":"S"},
{"AttributeName":"AppId","AttributeType":"S"},
{"AttributeName":"AppType","AttributeType":"N"}]

region = args['TARGET_REGION']
target_ddb_name = args['TARGET_DYNAMODB_NAME']

global_secondary_indexes = json.loads(args['GLOBAL_SEC_INDEXES_JSON_COLLECTION'])
attribute_definitions = json.loads(args['ATTRIBUTES_JSON_COLLECTION'])

# Drop and create target DynamoDB table
dynamodb_client = boto3.Session(
        aws_access_key_id=args['AWS_ACCESS_KEY_ID'],
        aws_secret_access_key=args['AWS_SECRET_ACCESS_KEY'],
        aws_session_token=args['TEMPORARY_SESSION_TOKEN'],
    ).client('dynamodb')

# Delete table
print('Deleting table: ' + target_ddb_name + ' ...')

try:
    dynamodb_client.delete_table(TableName=target_ddb_name)

    #Wait for table deletion to complete
    waiter = dynamodb_client.get_waiter('table_not_exists')
    waiter.wait(TableName=target_ddb_name)
    print('Table deleted.')
except dynamodb_client.exceptions.ResourceNotFoundException:
    print('Table already deleted / does not exist.')
    pass

print('Creating table: ' + target_ddb_name + ' ...')

table = dynamodb_client.create_table(
    TableName=target_ddb_name,
    KeySchema=[
        {
```

```
            'AttributeName': 'PK',
            'KeyType': 'HASH'  # Partition key
        },
        {
            'AttributeName': 'SK',
            'KeyType': 'RANGE'  # Sort key
        }
    ],
    AttributeDefinitions=attribute_definitions,
    GlobalSecondaryIndexes=global_secondary_indexes,
    BillingMode='PAY_PER_REQUEST'
)

waiter = dynamodb_client.get_waiter('table_exists')
waiter.wait(TableName=target_ddb_name)

print('Table created.')
```

Bewährte Methoden

Temporäre Anmeldeinformationen

Vermeiden Sie als bewährte Sicherheitsmethode beim programmgesteuerten Zugriff auf AWS-Services die Verwendung von `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` eines IAM-Benutzers, da es sich um langfristige Anmeldeinformationen handelt. Versuchen Sie immer, temporäre Anmeldeinformationen zu verwenden, um programmgesteuert auf AWS-Services zuzugreifen.

Beispielsweise codiert ein Entwickler während der Entwicklung die `AWS_ACCESS_KEY_ID` und eines IAM-`AWS_SECRET_ACCESS_KEY`Benutzers in der Anwendung fest, entfernt aber die fest codierten Werte nicht, bevor Änderungen an das Code-Repository übertragen werden. Diese offengelegten Anmeldeinformationen können von unbeabsichtigten oder böswilligen Benutzern verwendet werden, was schwerwiegende Auswirkungen haben kann (insbesondere wenn die offengelegten Anmeldeinformationen über Administratorrechte verfügen). Diese offengelegten Anmeldeinformationen sollten sofort mithilfe der IAM-Konsole oder der AWS Command Line Interface (AWS CLI) deaktiviert oder gelöscht werden.

Verwenden Sie AWS STS, um temporäre Anmeldeinformationen für den programmgesteuerten Zugriff auf AWS-Services abzurufen. Temporäre Anmeldeinformationen sind nur für die angegebene Zeit gültig (von 15 Minuten bis zu 36 Stunden). Die maximal zulässige Dauer temporärer

Anmeldeinformationen hängt von Faktoren wie Rolleneinstellungen und Rollenverkettung ab. Weitere Informationen zu AWS STS finden Sie in der Dokumentation .

Polen

Einrichten von DynamoDB-Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie DynamoDB-Tabellen.	Erstellen Sie DynamoDB-Tabellen mit Indizes sowohl in Quell- als auch in Ziel-AWS-Konten. Legen Sie die Kapazität sbereitstellung als On-Demand-Modus fest, sodass DynamoDB Lese-/Sch reibkapazitäten je nach Workload dynamisch skalieren kann. Alternativ können Sie bereitgestellte Kapazität mit 4 000 RCUs und 4 000 WCUs verwenden.	App-Entwickler, DBA, Migrationsingenieur
Füllen Sie die Quelltabelle aus.	Füllen Sie die DynamoDB-Tabelle im Quellkonto mit Testdaten aus. Mindestens 50 MB oder mehr Testdaten helfen Ihnen dabei, die Spitzen- und durchschn ittlichen RCUs zu sehen, die während der Tabellenkopie verbraucht werden. Anschließ end können Sie die Kapazität	App-Entwickler, DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sbereitstellung nach Bedarf ändern.	

Einrichten von Anmeldeinformationen für den Zugriff auf die DynamoDB-Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie IAM-Rollen für den Zugriff auf die Quell- und Ziel-DynamoDB-Tabellen.	Erstellen Sie eine IAM-Rolle im Quellkonto mit Berechtig ungen für den Zugriff (Lesen) auf die DynamoDB-Tabelle im Quellkonto. Fügen Sie das Quellkonto als vertrauenswürdige Entität für diese Rolle hinzu. Erstellen Sie eine IAM-Rolle im Zielkonto mit Berechtig ungen zum Zugriff (Erstellen, Lesen, Aktualisieren, Löschen) auf die DynamoDB-Tabelle im Zielkonto. Fügen Sie das Zielkonto als vertrauenswürdige Entität für diese Rolle hinzu.	App-Entwickler, AWS DevOps

Kopieren von Tabellendaten von einem Konto in ein anderes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie temporäre Anmeldeinformationen für die IAM-Rollen ab.	Rufen Sie temporäre Anmeldeinformationen für die	App-Entwickler, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Quellkonto erstellte IAM-Rolle ab. Rufen Sie temporäre Anmeldeinformationen für die im Zielkonto erstellte IAM-Rolle ab. Eine Möglichkeit, die temporären Anmeldein formationen für die IAM-Rolle abzurufen, ist die Verwendun g von AWS STS über die AWS CLI. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/<role-name> --role-session-name <session-name> --profile <profile-name>` Verwenden Sie das entsprech ende AWS-Profil (entsprec hend dem Quell- oder Zielkonto). Weitere Informationen zu verschiedenen Möglichke iten zum Abrufen temporärer Anmeldeinformationen finden Sie im Folgenden: • AWS Security Token Service – API-Referenz	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Abrufen von IAM-Rolle nanmeldeinformationen für den CLI-Zugriff	
Initialisieren Sie die DynamoDB-Clients für den Quell- und Ziel-DynamoDB-Zugriff.	Initialisieren Sie die DynamoDB-Clients, die vom AWS SDK bereitgestellt werden, für die Quell- und Ziel-DynamoDB-Tabellen. • Verwenden Sie für den DynamoDB-Quellclient die temporären Anmeldein formationen, die vom Quellkonto abgerufen wurden. • Verwenden Sie für den DynamoDB-Zielclient die temporären Anmeldein formationen, die vom Zielkonto abgerufen wurden. Weitere Informationen zum Senden von Anforderungen mithilfe temporärer IAM-Anmel deinformationen finden Sie in der AWS-Dokumentation.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Zieltabelle und erstellen Sie sie neu.	Löschen Sie die DynamoDB-Zieltabelle (zusammen mit Indizes) im Zielkonto und erstellen Sie sie neu, indem Sie den DynamoDB-Zielkonto-Client verwenden. Das Löschen aller Datensätze aus einer DynamoDB-Tabelle ist eine kostspielige Operation, da sie bereitgestellte WCUs verbraucht. Durch das Löschen und Neuerstellen der Tabelle werden diese zusätzlichen Kosten vermieden. Sie können einer Tabelle nach der Erstellung Indizes hinzufügen, dies dauert jedoch 2–5 Minuten länger. Das Erstellen von Indizes während der Tabellenerstellung, indem die Indizessammlung an den `createTable` Aufruf übergeben wird, ist effizienter.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Tabellenkopie durch.	Wiederholen Sie die folgenden Schritte, bis alle Daten kopiert wurden: • Führen Sie mithilfe des DynamoDB-Quellclients einen Scan der Tabelle im Quellkonto durch. Jeder DynamoDB-Scan ruft nur 1 MB an Daten aus der Tabelle ab. Daher müssen Sie diesen Vorgang wiederholen, bis alle Elemente oder Datensätze gelesen wurden. • Schreiben Sie die Elemente für jeden Satz gescannte r Elemente in die Tabelle im Zielkonto mit dem DynamoDB-Zielclient unter Verwendung des `BatchWriteItem` Aufrufs in AWS SDK for DynamoDB . Dadurch wird die Anzahl der `PutItem` Anforderungen an DynamoDB reduziert. • `BatchWriteItem` hat eine Begrenzung von 25 Schreibvorgängen oder Puts oder bis zu 16 MB. Sie müssen Logik hinzufügen, um gescannte Elemente in Anzahlen von	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	25 zu sammeln, bevor Sie aufrufen`BatchWrit eItem` . gibt eine Liste von Elementen `BatchWrit eItem` zurück, die nicht erfolgreich kopiert werden konnten. Fügen Sie mithilfe dieser Liste Wiederhol ungslogik hinzu, um einen weiteren `BatchWrit eItem` Aufruf nur mit den Elementen durchzuführen, die nicht erfolgreich waren. Weitere Informationen finden Sie in der Referenzi mplementierung in C# (zum Löschen, Erstellen und Auffüllen von Tabellen) im Abschnitt Anhänge. Eine Beispieldatei für die Tabellenk onfiguration JavaScript Object Notation (JSON) ist ebenfalls angehängt.	

Zugehörige Ressourcen

- Amazon-DynamoDB-Dokumentation
- Erstellen eines IAM-Benutzers in Ihrem AWS-Konto
- AWS-SDKs
- Verwenden temporärer Anmeldeinformationen mit AWS-Ressourcen

Zusätzliche Informationen

Dieses Muster wurde mit C# implementiert, um eine DynamoDB-Tabelle mit 200.000 Elementen zu kopieren (durchschnittliche Elementgröße von 5 KB und Tabellengröße von 250 MB). Die DynamoDB-Zieltabelle wurde mit einer bereitgestellten Kapazität von 4000 RCUs und 4000 WCUs eingerichtet.

Die vollständige Tabellenkopieroperation (vom Quellkonto zum Zielkonto), einschließlich des Löschens und Neuerstellens der Tabelle, dauerte 5 Minuten. Gesamt verbrauchte Kapazitätseinheiten: 30 000 RCUs und ungefähr 400 000 WCUs.

Weitere Informationen zu DynamoDB-Kapazitätsmodi finden Sie unter Lese-/Schreibkapazitätsmodus in der AWS-Dokumentation.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Kopieren von Amazon DynamoDB-Tabellen über Konten hinweg mit AWS Backup

Erstellt von Ramkumar Ramanujam (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Migration	AWS-Services: Amazon DynamoDB ;AWS Backup

Übersicht

Bei der Arbeit mit Amazon DynamoDB in Amazon Web Services (AWS) besteht ein häufiger Anwendungsfall darin, DynamoDB-Tabellen in Entwicklungs-, Test- oder Staging-Umgebungen mit den Tabellendaten in der Produktionsumgebung zu kopieren oder zu synchronisieren. Standardmäßig verwendet jede Umgebung ein anderes AWS-Konto.

AWS Backup unterstützt die regions- und kontoübergreifende Sicherung und Wiederherstellung von Daten für DynamoDB , Amazon Simple Storage Service (Amazon S3) und andere AWS-Services. Dieses Muster enthält die Schritte zur Verwendung der kontoübergreifenden Sicherung und Wiederherstellung von AWS Backup zum Kopieren von DynamoDB-Tabellen zwischen AWS-Konten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten, die zur selben AWS Organizations-Organisation gehören
- DynamoDB-Tabellen in beiden Konten.
- AWS Identity and Access Management (IAM)-Berechtigungen zum Erstellen und Verwenden von AWS-Backup-Tresoren

Einschränkungen

- Quell- und Ziel-AWS-Konten sollten Teil derselben AWS Organizations-Organisation sein.

Architektur

Zieltechnologie-Stack

- AWS Backup
- Amazon DynamoDB

Zielarchitektur

1. Erstellen Sie das DynamoDB-Tabellen-Backup im AWS Backup-Backup-Tresor im Quellkonto.
2. Kopieren Sie das Backup in den Backup-Tresor im Zielkonto.
3. Stellen Sie die DynamoDb Tabelle im Zielkonto mithilfe der Sicherung aus dem Zielkonto-Sicherungstresor wieder her.

Automatisierung und Skalierung

Sie können AWS Backup verwenden, um Backups so zu planen, dass sie in bestimmten Intervallen ausgeführt werden.

Tools

- AWS Backup – AWS Backup ist ein vollständig verwalteter Service zur Zentralisierung und Automatisierung des Datenschutzes über AWS-Services, in der Cloud und On-Premises. Mit diesem Service können Sie Backup-Richtlinien konfigurieren und Aktivitäten für Ihre AWS-Ressourcen an einem Ort überwachen. Damit können Sie Backup-Aufgaben automatisieren und konsolidieren, die zuvor ausgeführt wurden service-by-service, und Sie müssen keine benutzerdefinierten Skripts und manuellen Prozesse erstellen.
- Amazon DynamoDB – Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.

Polen

Aktivieren der AWS Backup-Funktionen in den Quell- und Zielkonten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie erweiterte Funktionen für DynamoDB und kontoübergreifende Backups.	Gehen Sie sowohl in den Quell- als auch in den Ziel-AWS-Konten wie folgt vor: 1. Öffnen Sie in der AWS-Managementkonsole die AWS Backup-Konsole. 2. Wählen Sie Settings (Einstellungen) aus. 3. Vergewissern Sie sich unter Erweiterte Funktionen für Amazon-DynamoDB-Backups, dass Erweiterte Funktionen aktiviert sind, oder wählen Sie Aktivieren aus. 4. Wählen Sie unter Kontoübergreifende Verwaltung für Kontoüber greifende Sicherung die Option Aktivieren aus.	AWS DevOps, Migration singenieur

Erstellen von Backup-Tresoren in den Quell- und Zielkonten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Backup-Tresore.	Gehen Sie sowohl in den Quell- als auch in den Ziel-AWS-Konten wie folgt vor:	AWS DevOps, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Wählen Sie in der AWS Backup-Konsole Backup-Tresore aus. 2. Wählen Sie Create backup vault (Sicherungstresor erstellen) aus. 3. Kopieren Sie den Amazon-Ressourcennamen (ARN) des Backup-Tresors und speichern Sie ihn. Die ARNs sowohl des Quell- als auch des Ziel-Backup-Tresors sind erforderlich, wenn Sie das DynamoDB-Tabellen-Backup zwischen dem Quellkonto und dem Zielkonto kopieren.	

Backup und Wiederherstellung mit Backup-Tresoren durchführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie im Quellkonto eine DynamoDB-Tabellensicherung.	Gehen Sie wie folgt vor, um ein Backup für die DynamoDB-Tabelle im Quellkonto zu erstellen: 1. Wählen Sie auf der Seite AWS Backup Dashboard die Option On-Demand-Backup erstellen aus. 2. Wählen Sie im Abschnitt Einstellungen für Ressource	AWS DevOps, DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ntyp die Option DynamoDB und dann den Tabellenn amen aus. 3. Wählen Sie in der Dropdownliste Backup-Tr esor den Backup-Tresor aus, den Sie im Quellkonto erstellt haben. 4. Wählen Sie den gewünscht en Aufbewahrungszeitraum aus. 5. Wählen Sie On-Demand-Backup erstellen. Ein neuer Backup-Auftrag wird erstellt. Um den Status des Backup-Auftrags zu überwachen, wählen Sie auf der Seite AWS Backup-Aufträge die Registerk arte Backup-Aufträge aus. Alle aktiven, laufenden und abgeschlossenen Backup-Aufträge sind auf dieser Registerkarte aufgeführt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie das Backup aus dem Quellkonto in das Zielkonto.	Nachdem der Sicherungsauftrag abgeschlossen ist, kopieren Sie das DynamoDB-Tabellen-Backup aus dem Sicherungstresor im Quellkonto in den Sicherungstresor im Zielkonto. Gehen Sie wie folgt vor, um den Backup-Tresor im Quellkonto zu kopieren: 1. Wählen Sie in der AWS Backup-Konsole Backup-Tresore aus. 2. Wählen Sie unter Backups die DynamoDB-Tabellensicherung aus. 3. Wählen Sie Aktionen, Kopieren. 4. Geben Sie die AWS-Region des Zielkontos ein. 5. Geben Sie für ARN des externen Tresors den ARN des Backup-Tresors ein, den Sie im Zielkonto erstellt haben. 6. Um Backups vom Quellkonto in das Zielkonto zu kopieren, aktivieren Sie im Zielkonto-Backup-Tresor den Zugriff von einem anderen Konto aus.	AWS DevOps, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Backup im Zielkonto wieder her.	Gehen Sie im AWS-Zielkonto wie folgt vor: 1. Wählen Sie in der AWS Backup-Konsole Backup-Tresore aus. 2. Wählen Sie unter Backups das Backup aus, das Sie aus dem Quellkonto kopiert haben. 3. Wählen Sie Aktionen, Wiederherstellen aus. 4. Geben Sie den Namen der DynamoDB-Zieltabelle ein, die Sie wiederherstellen möchten.	AWS DevOps, DBA, Migration singenieur

Zugehörige Ressourcen

- Verwenden von AWS Backup mit DynamoDB
- Erstellen von Sicherungskopien über AWS-Konten hinweg
- AWS Backup – Preise

Erstellen detaillierter Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora

Erstellt von Lakshmanan Lakshmanan (AWS) und Sudarshan Narasimhan

Umgebung: Produktion	Technologien: Datenbanken; Kostenmanagement; Analysen	AWS-Services: Amazon Athena; Amazon Aurora; Amazon RDS; AWS-Fakturierung und Kostenmanagement

Übersicht

Dieses Muster zeigt, wie Sie die Nutzungskosten für Amazon Relational Database Service (Amazon RDS)- oder Amazon Aurora-Cluster verfolgen, indem Sie benutzerdefinierte Kostenzuordnungs-Tags konfigurieren. Sie können diese Tags verwenden, um detaillierte Kosten- und Nutzungsberichte in AWS Cost Explorer für Cluster über mehrere Dimensionen hinweg zu erstellen. Sie können beispielsweise die Nutzungskosten auf Team-, Projekt- oder Kostenstellenebene verfolgen und dann die Daten in Amazon Athena analysieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine oder mehrere Amazon RDS- oder Amazon Aurora-Instances

Einschränkungen

Informationen zu Tagging-Einschränkungen finden Sie im AWS Billing-Benutzerhandbuch.

Architektur

Zieltechnologie-Stack

- Amazon RDS oder Amazon Aurora

- AWSKosten- und Nutzungsbericht
- AWS Cost Explorer
- Amazon Athena

Workflow und Architektur

Der Tagging- und Analyse-Workflow besteht aus folgenden Schritten:

1. Ein Dateningenieur, Datenbankadministrator oder AWS-Administrator erstellt benutzerdefinierte Kostenzuordnungs-Tags für die Amazon RDS- oder Aurora-Cluster.
2. Ein AWS-Administrator aktiviert die Tags.
3. Die Tags melden Metadaten an AWS Cost Explorer .
4. Ein Dateningenieur, Datenbankadministrator oder AWS-Administrator erstellt einen monatlichen Kostenzuordnungsbericht.
5. Ein Dateningenieur, Datenbankadministrator oder AWS-Administrator analysiert den monatlichen Kostenzuordnungsbericht mithilfe von Amazon Athena .

Das folgende Diagramm zeigt, wie Sie Tags anwenden, um die Nutzungskosten für Amazon-RDS- oder Aurora-Instances zu verfolgen.

Das folgende Architekturdiagramm zeigt, wie der Kostenzuordnungsbericht zur Analyse in Amazon Athena integriert ist.

Der monatliche Kostenzuordnungsbericht wird in einem von Ihnen angegebenen Amazon S3-Bucket gespeichert. Wenn Sie Athena mit der AWS- CloudFormation Vorlage einrichten, wie im Abschnitt „PiCs“ beschrieben, stellt die Vorlage mehrere zusätzliche Ressourcen bereit, darunter einen AWS Glue-Crawler, eine AWS Glue-Datenbank, ein Amazon Simple Notification System (Amazon SNS)-Ereignis, AWS Lambda-Funktionen und AWS Identity and Access Management (IAM)-Rollen für die Lambda-Funktionen. Wenn neue Kostendatendateien im S3-Bucket eingehen, werden Ereignisbenachrichtigungen verwendet, um diese Dateien zur Verarbeitung an eine Lambda-Funktion weiterzuleiten. Die Lambda-Funktion initiiert einen AWS Glue-Crawler-Auftrag zum Erstellen

oder Aktualisieren der Tabelle im AWS Glue Data Catalog. Diese Tabelle wird dann verwendet, um Daten in Athena abzufragen.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mit Standard-SQL vereinfacht.
- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- AWS CloudFormation ist ein Infrastructure as Code (IaC)-Service, mit dem Sie AWS und Ressourcen von Drittanbietern einfach modellieren, bereitstellen und verwalten können.
- AWS Cost Explorer hilft Ihnen, Ihre AWS-Kosten und -Nutzung anzuzeigen und zu analysieren.

Polen

Erstellen und Aktivieren von Tags für Ihren Amazon-RDS- oder Aurora-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerdefinierte Kostenzuordnungs-Tags für Ihren Amazon-RDS- oder Aurora-Cluster.	Um Tags zu einem neuen oder vorhandenen Amazon-RDS- oder Aurora-Cluster hinzuzufügen, folgen Sie den Anweisungen unter Hinzufügen, Auflisten und Entfernen von Tags im Amazon-Aurora-Benutzerhandbuch. Hinweis: Informationen zum Einrichten eines Amazon-Aurora-Clusters finden Sie in den Anweisungen für MySQL und	AWS-Administrator, Dateningenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PostgreSQL im Amazon-Aurora-Benutzerhandbuch.	
Aktivieren Sie die benutzerdefinierten Kostenzuordnungs-Tags.	Folgen Sie den Anweisungen unter Aktivieren benutzerdefinierter Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.	AWS-Administrator

Erstellen von Kosten- und Nutzungsberichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie Kosten- und Nutzungsberichte für Ihre Cluster.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-Fakturierungskonsole. 2. Wählen Sie im linken Navigationsbereich Kosten- und Nutzungsberichte aus. 3. Wählen Sie Create report (Bericht erstellen) aus. 4. Geben Sie einen Berichtsnamen an, behalten Sie die Standardeinstellungen für andere Optionen bei und wählen Sie dann Weiter aus. 5. Wählen Sie Konfigurieren und geben Sie die Details eines vorhandenen S3-Buckets an. Auf diesem Bildschirm können Sie auch einen neuen S3-	App-Besitzer, AWS-Administrator, DBA, Allgemeines AWS, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket erstellen. Wählen Sie Weiter aus. 6. Überprüfen Sie die Standardrichtlinie, die auf Ihren Bucket angewende t wird, aktivieren Sie das Bestätigungs-Kontrollkästch en und wählen Sie dann Speichern aus. 7. Geben Sie für Berichtsp fadpräfix das Präfix an, dem Sie den Berichtsnamen voranstellen möchten. 8. Wählen Sie für Zeitgranu larität die Option Stündlich, Täglich oder Monatlich aus, je nachdem, wie oft Daten für den Bericht erfasst werden sollen. 9. Wählen Sie unter Berichts-Versioning aus, ob Sie möchten, dass neue Versionen des Berichts separat erstellt werden, oder ob Sie den vorhanden en Bericht mit jeder Version überschreiben möchten. 10. Wählen Sie für Berichtsd atenintegration für aktiviere n die Option Amazon Athena aus. Stellen Sie sicher, dass der Komprimie rungstyp auf Parquet festgelegt ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie Weiter aus. 12. Überprüfen Sie die Berichtseinstellungen und wählen Sie dann Überprüfen und Abschließen aus. Die Daten sind in 24 Stunden verfügbar.	

Analysieren von Kosten- und Nutzungsberichtsdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die Daten des Kosten- und Nutzungsberichts.	1. Richten Sie Athena ein und verwenden Sie es, um die Berichtsdaten zu analysieren. Anweisungen finden Sie unter Abfragen von Kosten- und Nutzungsberichten mit Amazon Athena im AWS-Benutzerhandbuch für Kosten- und Nutzungsberichte. Wir empfehlen Ihnen, die von Athena bereitgestellte AWS- CloudFormation Vorlage zu verwenden. 2. Führen Sie Athena-Abfragen aus. Sie können beispielsweise die folgende SQL-Abfrage verwenden, um den Status der Datenaktualisierung zu überprüfen.	App-Besitzer, AWS-Administrator, DBA, Allgemeines AWS, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`select status from cost_and_usage_data_status` Weitere Informationen finden Sie unter Ausführen von Amazon Athena-Abfragen im AWS-Benutzerhandbuch für Kosten- und Nutzungsberichte. Hinweis: Stellen Sie beim Ausführen Ihrer SQL-Abfrage sicher, dass die richtige Datenbank aus der Dropdown-Liste ausgewählt ist.	

Zugehörige Ressourcen

Referenzen

- Einrichten von Athena mithilfe von AWS- CloudFormation Vorlagen (empfohlen)
- Manuelles Einrichten von Athena
- Ausführen von Amazon Athena-Abfragen
- Laden von Berichtsdaten in andere Ressourcen

Tutorials und Videos

- Analysieren von Kosten- und Nutzungsberichten mit Amazon Athena (YouTube Video)

Emulieren von Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL

Erstellt von HariKrishna Boorgadda (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Aurora PostgreSQL
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Datenbanken; Migration
AWS-Services: Amazon Aurora; Amazon CloudWatch		

Übersicht

Dieses Muster beschreibt, wie Services in einer Oracle Real Application Clusters (Oracle RAC)-Workload emuliert werden, indem die Amazon Aurora PostgreSQL -kompatible Edition mit benutzerdefinierten Endpunkten verwendet wird, die Workloads auf Instances innerhalb eines einzigen Clusters verteilen. Das Muster zeigt Ihnen, wie Sie benutzerdefinierte Endpunkte für Amazon-Aurora-Datenbanken erstellen. Mit benutzerdefinierten Endpunkten können Sie Workloads auf verschiedene Sätze von DB-Instances in Ihrem Aurora-Cluster verteilen und ausgleichen.

In einer Oracle RAC-Umgebung können sich -Services über eine oder mehrere Instances erstrecken und einen Workload-Balancing basierend auf der Transaktionsleistung ermöglichen. Zu den Servicefunktionen gehören end-to-end eine unbeaufsichtigte Wiederherstellung, fortlaufende Änderungen nach Workload und vollständige Standorttransparenz. Sie können dieses Muster verwenden, um einige dieser Funktionen zu emulieren. Sie können beispielsweise die Möglichkeit emulieren, Verbindungen für meldende Anwendungen weiterzuleiten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein PostgreSQL-JDBC-Treiber

- Eine mit Aurora PostgreSQL kompatible Datenbank
- Eine Oracle RAC-Datenbank, die zu einer Aurora PostgreSQL-kompatiblen Datenbank migriert wurde

Einschränkungen

- Einschränkungen für benutzerdefinierte Endpunkte finden Sie unter Angeben von Eigenschaften für benutzerdefinierte Endpunkte in der Amazon-RDS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine Oracle RAC-Datenbank mit drei Knoten

Zieltechnologie-Stack

- Eine mit Aurora PostgreSQL kompatible Datenbank mit zwei Lesereplikaten

Quellarchitektur

Das folgende Diagramm zeigt die Architektur einer Oracle RAC-Datenbank mit drei Knoten.

Zielarchitektur

Das folgende Diagramm zeigt die Architektur einer Aurora-PostgreSQL-kompatiblen Datenbank mit zwei Lesereplikaten. Drei verschiedene Anwendungen/Services verwenden benutzerdefinierte Endpunkte, die verschiedenen Anwendungsbenutzern dienen und den Datenverkehr und die Last zwischen Primär- und Lesereplikaten umleiten.

Tools

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Polen

Erstellen des Aurora PostgreSQL -kompatiblen Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Cluster.	Informationen zum Erstellen des Clusters finden Sie unter Erstellen eines DB-Clusters und Herstellen einer Verbindung mit einer Datenbank in einem Aurora-PostgreSQL-DB-Cluster in der Amazon-RDS-Dokumentation.	AWS-Administrator
Erstellen Sie eine benutzerdefinierte Parametergruppe für den Workload.	Informationen zum Erstellen einer Parametergruppe finden Sie unter Erstellen einer DB-Cluster-Parametergruppe in der Amazon-RDS-Dokumentation.	AWS-Administrator
Erstellen Sie Ereignisbenachrichtigungen und Alarme.	Sie können Ereignisbenachrichtigungen und Amazon- CloudWatch Alarme verwenden, um Sie zu benachrichtigen, wenn der Cluster den Status ändert, und um Metriken zu erfassen,	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wenn ein vordefinierter Schwellenwert erreicht wird. Informationen zum Erstellen eines CloudWatch Alarms finden Sie unter Erstellen eines CloudWatch Alarms basierend auf einem statischen Schwellenwert in der - CloudWatch Dokumentation. Informationen zum Erstellen einer Ereignisbenachrichtigung finden Sie unter Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird in der - CloudWatch Dokumentation.	

Hinzufügen von Replikaten zum mit Aurora PostgreSQL kompatiblen DB-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Lesereplikate zum Cluster hinzu.	1. Erstellen Sie ein Lesereplikat . 2. Fügen Sie das Lesereplikat derselben Availability Zone hinzu, in der sich Ihr DB-Cluster befindet. Hinweis: Sie können eine andere Availability Zone verwenden , wenn Sie Anforderungen für Ihren Failover-Knoten erfüllen müssen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich den Lesereplikat-Endpunkt.	Dokumentieren Sie Ihren Lesereplikat-Endpunkt zur späteren Verwendung beim Erstellen der benutzerdefinierten Endpunkte.	AWS-Administrator

Erstellen benutzerdefinierter Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie einen Namen für den benutzerdefinierten Endpunkt ein.	Erstellen Sie für jeden Endpunkt, den Sie benötigen, einen eindeutigen Endpunktnamen, der sich auf Ihren Workload oder Ihre Anwendung bezieht.	AWS-Administrator
Fügen Sie die Endpunktmitglieder hinzu.	Fügen Sie Ihre Lesereplikat-Endpunkte einer benutzerdefinierten Gruppe hinzu. Weitere Informationen finden Sie unter Bearbeiten eines benutzerdefinierten Endpunkts in der Amazon-RDS-Dokumentation.	AWS-Administrator
(Optional) Fügen Sie dem Cluster zukünftige Instances hinzu.	Wenn Sie der benutzerdefinierten Gruppe weitere Replikate oder Endpunkte hinzufügen möchten, finden Sie weitere Informationen unter Hinzufügen von Aurora-Replikaten zu einem DB-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cluster in der Amazon-RDS-Dokumentation.	
Erstellen Sie den Endpunkt.	Informationen zum Erstellen des Endpunkts finden Sie unter Erstellen eines benutzerdefinierten Endpunkts in der Amazon-RDS-Dokumentation.	AWS-Administrator

Testen von Anwendungsverbindungen mithilfe benutzerdefinierter Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Teilen Sie die benutzerdefinierten Endpunktdetails mit der Anwendung, die auf Ihren Workload verweist.	Fügen Sie Ihre benutzerdefinierten Endpunktdetails zu den Datenbankverbindungsdetails in der Berichtsanwendung hinzu, die Sie testen möchten.	AWS-Administrator
Verbinden Sie den Workload mithilfe des benutzerdefinierten Endpunkts.	Validieren Sie die benutzerdefinierten Endpunktdetails in der Berichtsanwendung.	AWS-Administrator
Überprüfen Sie die Verbindungsdetails aus der Datenbank.	1. Testen Sie den Benutzernamen und die Verbindungsanzahl für Ihre Anwendung. 2. Überprüfen Sie den Lastausgleich auf Ihre Workloads, um sicherzustellen, dass die Verbindungen auf verschiedene benutzerdefinierte	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Endpunkte (primäre und Lesereplikate) verteilt sind.	

Zugehörige Ressourcen

- Arten von Aurora-Endpunkten
- Mitgliedschaftsregeln für benutzerdefinierte Endpunkte
- E nd-to-end AWS CLI-Beispiel für benutzerdefinierte Endpunkte
- Amazon Aurora als Alternative zu Oracle RAC
- Herausforderungen bei der Migration von Oracle zu PostgreSQL – und wie man sie überwindet

Aktivieren verschlüsselter Verbindungen für PostgreSQL-DB-Instances in Amazon RDS

Erstellt von Rohit Kapoor (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Netzwerk; Sicherheit, Identität, Compliance	Workload: Open-Source
AWS-Services: Amazon RDS; Amazon Aurora		

Übersicht

Amazon Relational Database Service (Amazon RDS) unterstützt SSL-Verschlüsselung für PostgreSQL-DB-Instances. Mit SSL können Sie eine PostgreSQL-Verbindung zwischen Ihren Anwendungen und Ihren Amazon RDS for PostgreSQL-DB-Instances verschlüsseln. Standardmäßig verwendet Amazon RDS for PostgreSQL SSL/TLS und erwartet, dass alle Clients eine Verbindung mithilfe der SSL/TLS-Verschlüsselung herstellen. Amazon RDS for PostgreSQL unterstützt die TLS-Versionen 1.1 und 1.2.

Dieses Muster beschreibt, wie Sie verschlüsselte Verbindungen für eine DB-Instance von Amazon RDS für PostgreSQL aktivieren können. Sie können denselben Prozess verwenden, um verschlüsselte Verbindungen für Amazon Aurora PostgreSQL – kompatible Edition zu aktivieren.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto
- Eine DB-Instance von Amazon RDS für PostgreSQL
- Ein SSL-Paket

Architektur

Tools

- pgAdmin ist eine Open-Source-Verwaltungs- und Entwicklungsplattform für PostgreSQL . Sie können pgAdmin unter Linux, Unix, macOS und Windows verwenden, um Ihre Datenbankobjekte in PostgreSQL 10 und höher zu verwalten.
- PostgreSQL-Editoren bieten eine benutzerfreundlichere Oberfläche, die Sie beim Erstellen, Entwickeln und Ausführen von Abfragen unterstützt und Code an Ihre Anforderungen anpasst.

Bewährte Methoden

- Überwachen Sie unsichere Datenbankverbindungen.
- Prüfen Sie die Zugriffsrechte für Datenbanken.
- Stellen Sie sicher, dass Backups und Snapshots im Ruhezustand verschlüsselt sind.
- Überwachen Sie den Datenbankzugriff.
- Vermeiden Sie uneingeschränkte Zugriffsgruppen.
- Verbessern Sie Ihre Benachrichtigungen mit Amazon GuardDuty.
- Überwachen Sie die Einhaltung von Richtlinien regelmäßig.

Polen

Herunterladen eines vertrauenswürdigen Zertifikats und Importieren in Ihren Trust Store

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie ein vertrauen swürdiges Zertifikat auf Ihren Computer.	Gehen Sie folgendermaßen vor, um Zertifikate zum Speicher der vertrauen swürdigen Stammzertifizierun gsstellen für Ihren Computer hinzuzufügen. (Diese Anweisungen verwenden als Beispiel Window Server.)	DevOps Ingenieur, Migration singenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Wählen Sie unter Windows ServerStart ,Ausführen und geben Sie dannmmc ein. 2. Wählen Sie in der Konsole Datei , Snap-in hinzufügen/ entfernen aus. 3. Wählen Sie unter Verfügbar e Snap-Ins die OptionZer tifikate und dann Hinzufüge n aus. 4. Wählen Sie unter Dieses Snap-In verwaltet immer Zertifikate für , Computerk onto , Weiter aus. 5. Wählen Sie Lokaler Computer, Fertigstellen aus. 6. Wenn Sie der Konsole keine Snap-Ins mehr hinzufügen möchten, wählen Sie OK aus. 7. Doppelklicken Sie in der Konsolenstruktur aufCertificates. 8. Klicken Sie mit der rechten Maustaste auf Vertrauen swürdige Stammzert ifizierungsstellen. 9. Wählen Sie Alle Aufgaben, Importieren, um die heruntergeladenen Zertifika te zu importieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Führen Sie die Schritte im Assistenten zum Importieren von Zertifikaten aus.	

SSL-Verbindungen erzwingen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Parametergruppe und legen Sie den Parameter rds.force_ssl fest.	Wenn die PostgreSQL-DB-Instance über eine benutzerdefinierte Parametergruppe verfügt, bearbeiten Sie die Parametergruppe und ändern Sie `rds.force_ssl` in 1. Wenn die DB-Instance die Standardparametergruppe verwendet, die nicht `rds.force_ssl` aktiviert ist, erstellen Sie eine neue Parametergruppe. Sie können die neue Parametergruppe mithilfe der Amazon RDS-API oder manuell ändern, wie in den folgenden Anweisungen gezeigt. So erstellen Sie eine neue Parametergruppe: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole für	DevOps Ingenieur, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die AWS-Region, die die DB-Instance hostet. 2. Wählen Sie im Navigationsbereich Parametergruppen aus. 3. Wählen Sie Parametergruppe erstellen und legen Sie die folgenden Werte fest: • Wählen Sie für Parametergruppenfamilie postgres14 aus. • Geben Sie für Gruppenname pgsql-<database_instance>-ssl ein. • Geben Sie unter Beschreibung eine Freiformbeschreibung für die Parametergruppe ein, die Sie hinzufügen. • Wählen Sie Erstellen. 4. Wählen Sie die Parametergruppe aus, die Sie erstellt haben. 5. Wählen Sie für Parametergruppenaktionen die Option Bearbeiten. 6. Suchen Sie rds.force_ssl und ändern Sie seine Einstellung auf 1.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Führen Sie clientseitige Tests durch, bevor Sie diesen Parameter ändern. 7. Wählen Sie Änderungen speichern aus. So verknüpfen Sie die Parametergruppe mit Ihrer PostgreSQL-DB-Instance: 1. Wählen Sie in der Amazon-RDS-Konsole im Navigationsbereich Datenbanken und dann die PostgreSQL-DB-Instance aus. 2. Wählen Sie Ändern aus. 3. Wählen Sie unter Zusätzliche Konfiguration die neue Parametergruppe und dann Weiter aus. 4. Wählen Sie unter Änderungen planen die Option Sofort anwenden aus. 5. Wählen Sie Modify DB Instance (DB-Instance ändern) aus. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
SSL-Verbindungen erzwingen.	Stellen Sie eine Verbindung mit der DB-Instance von Amazon RDS für PostgreSQL her. Verbindungsversuche, die SSL nicht verwenden, werden mit einer Fehlermeldung abgelehnt. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	DevOps Ingenieur, Migrationsingenieur, DBA

Installieren der SSL-Erweiterung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die SSL-Erweiterung.	1. Starten Sie eine psql- oder pgAdmin-Verbindung als DBA.
	2. Rufen Sie die Funktion ssl_is_used() auf, um festzustellen, ob SSL verwendet wird.
	`select ssl_is_used();`
	Die Funktion gibt zurück`t`, wenn die Verbindung SSL verwendet. Andernfalls gibt sie zurück`f`.
	3. Installieren Sie die SSL-Erweiterung.
	`create extension sslinfo;`
		DevOps Ingenieur, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`show ssl;`
	`select ssl_cipher();`
	
	Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	

Konfigurieren Ihres PostgreSQL-Clients für SSL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie einen Client für SSL.	Durch die Verwendung von SSL können Sie den PostgreSQL-Server mit Unterstützung für verschlüsselte Verbindungen starten, die TLS-Protokolle verwenden. Der Server lauscht sowohl auf Standard- als auch auf SSL-Verbindungen auf demselben TCP-Port und verhandelt mit jedem verbindenden Client, ob SSL verwendet werden soll. Standardmäßig ist dies eine Client-Option. Wenn Sie den psql-Client verwenden: 1. Stellen Sie sicher, dass das Amazon-RDS-Zertifikat auf Ihren lokalen Computer geladen wurde.	DevOps Ingenieur, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Starten Sie eine SSL-Client-Verbindung, indem Sie Folgendes hinzufügen:
	
	`psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser sslmode=verify-full sslrootcert=rds-ssl-ca-cert.pem`
	`select ssl_cipher();`
	
	Für andere PostgreSQL-Clients:
	
	• Ändern Sie den jeweiligen öffentlichen Schlüsselparameter der Anwendung. Dies kann als Option, als Teil Ihrer Verbindungszeichenfolge oder als Eigenschaft auf der Verbindungsseite in GUI-Tools verfügbar sein.
	
	Sehen Sie sich die folgenden Seiten für diese Clients an:
	
	• pgAdmin-Dokumentation
	• JDBC-Dokumentation	

Fehlerbehebung

Problem	Lösung
Das SSL-Zertifikat kann nicht heruntergeladen werden.	Überprüfen Sie Ihre Verbindung zur Website und versuchen Sie erneut, das Zertifikat auf Ihren lokalen Computer herunterzuladen.

Zugehörige Ressourcen

- Dokumentation zu Amazon RDS für PostgreSQL
- Verwenden von SSL mit einer PostgreSQL-DB-Instance (Amazon-RDS-Dokumentation)
- Sichere TCP/IP-Verbindungen mit SSL (PostgreSQL-Dokumentation)
- Verwenden von SSL (JDBC-Dokumentation)

Verschlüsseln einer vorhandenen DB-Instance von Amazon RDS für PostgreSQL

Erstellt von Piyush Goyal (AWS), Shobana Raghu (AWS) und Yaser R Bol (AWS)

Umgebung: Produktion	Technologien: Datenbanken; Sicherheit, Identität, Compliance	AWS-Services: Amazon RDS; AWS KMS; AWS DMS

Übersicht

In diesem Muster wird erläutert, wie Sie eine vorhandene Amazon Relational Database Service (Amazon RDS) for PostgreSQL-DB-Instance in der Amazon Web Services (AWS) Cloud mit minimalen Ausfallzeiten verschlüsseln. Dieser Prozess funktioniert auch für DB-Instances von Amazon RDS für MySQL.

Sie können die Verschlüsselung für eine Amazon RDS-DB-Instance aktivieren, wenn Sie sie erstellen, aber nicht nachdem sie erstellt wurde. Sie können jedoch einer unverschlüsselten DB-Instance Verschlüsselung hinzufügen, indem Sie einen Snapshot Ihrer DB-Instance erstellen und dann eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie eine DB-Instance aus dem verschlüsselten Snapshot wiederherstellen, um eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance zu erhalten. Wenn Ihr Projekt während dieser Aktivität Ausfallzeiten (mindestens für Schreibtransaktionen) zulässt, müssen Sie nur dies tun. Wenn die neue, verschlüsselte Kopie der DB-Instance verfügbar ist, können Sie Ihre Anwendungen auf die neue Datenbank verweisen. Wenn Ihr Projekt jedoch keine erheblichen Ausfallzeiten für diese Aktivität zulässt, benötigen Sie einen alternativen Ansatz, der dazu beiträgt, die Ausfallzeiten zu minimieren. Dieses Muster verwendet den AWS Database Migration Service (AWS DMS), um die Daten zu migrieren und kontinuierlich zu replizieren, sodass der Cutover auf die neue, verschlüsselte Datenbank mit minimalen Ausfallzeiten durchgeführt werden kann.

Amazon RDS-verschlüsselte DB-Instances verwenden den branchenüblichen AES-256-Verschlüsselungsalgorithmus, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre Amazon RDS-DB-Instances hostet. Nachdem Ihre Daten verschlüsselt wurden, übernimmt Amazon RDS die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten transparent, mit minimalen Auswirkungen auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um Verschlüsselung anzuwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine unverschlüsselte DB-Instance von Amazon RDS für PostgreSQL
- Erfahrung mit der Arbeit mit AWS DMS-Aufgaben (Erstellen, Ändern oder Stoppen) (siehe Arbeiten mit AWS DMS-Aufgaben in der AWS DMS-Dokumentation)
- Vertrautheit mit AWS Key Management Service (AWS KMS) zur Verschlüsselung von Datenbanken (siehe AWS KMS-Dokumentation)

Einschränkungen

- Sie können die Verschlüsselung für eine Amazon RDS-DB-Instance nur aktivieren, wenn Sie sie erstellen, nicht nachdem die DB-Instance erstellt wurde.
- Daten in nicht protokollierten Tabellen werden nicht mithilfe von Snapshots wiederhergestellt. Weitere Informationen finden Sie unter Bewährte Methoden für die Arbeit mit PostgreSQL.
- Es ist nicht möglich, ein verschlüsseltes Lesereplikat einer unverschlüsselten DB-Instance oder ein unverschlüsseltes Lesereplikat einer verschlüsselten DB-Instance zu erstellen.
- Sie können ein unverschlüsseltes Backup oder einen solchen Snapshot nicht als verschlüsselte DB-Instance wiederherstellen.
- AWS DMS überträgt die Sequenzen nicht automatisch, daher sind zusätzliche Schritte erforderlich, um dies zu bewältigen.

Weitere Informationen finden Sie unter Einschränkungen von mit Amazon RDS verschlüsselten DB-Instances in der Amazon-RDS-Dokumentation.

Architektur

Quellarchitektur

- Unverschlüsselte RDS-DB-Instance

Zielarchitektur

- Verschlüsselte RDS-DB-Instance

- Die Ziel-RDS-DB-Instance wird erstellt, indem die DB-Snapshot-Kopie der Quell-RDS-DB-Instance wiederhergestellt wird.
- Ein AWS KMS-Schlüssel wird für die Verschlüsselung bei der Wiederherstellung des Snapshots verwendet.
- Eine AWS DMS-Replikationsaufgabe wird verwendet, um die Daten zu migrieren.

Tools

Tools, die zur Aktivierung der Verschlüsselung verwendet werden:

- AWS KMS-Schlüssel für die Verschlüsselung – Wenn Sie eine verschlüsselte DB-Instance erstellen, können Sie einen vom Kunden verwalteten Schlüssel oder den von AWS verwalteten Schlüssel für Amazon RDS zum Verschlüsseln Ihrer DB-Instance auswählen. Wenn Sie die Schlüsselkennung für einen vom Kunden verwalteten Schlüssel nicht angeben, verwendet Amazon RDS den von AWS verwalteten Schlüssel für Ihre neue DB-Instance. Amazon RDS erstellt einen von AWS verwalteten Schlüssel für Amazon RDS für Ihr AWS-Konto. Ihr AWS-Konto verfügt für jede AWS-Region über einen anderen von AWS verwalteten Schlüssel für Amazon RDS. Weitere Informationen zur Verwendung von KMS-Schlüsseln für die Amazon-RDS-Verschlüsselung finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

Tools, die für die fortlaufende Replikation verwendet werden:

- AWS DMS – Sie können AWS Database Migration Service (AWS DMS) verwenden, um Änderungen aus der Quell-DB in die Ziel-DB zu replizieren. Es ist wichtig, die Quell- und Ziel-DB synchron zu halten, um Ausfallzeiten auf ein Minimum zu beschränken. Informationen zum Einrichten von AWS DMS und Erstellen von Aufgaben finden Sie in der AWS DMS-Dokumentation.

Polen

Erstellen eines Snapshots der Quell-DB-Instance und Verschlüsseln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Details für die PostgreSQL-DB-Quell-Instance.	Wählen Sie in der Amazon-RDS-Konsole die PostgreSQL-DB-Quell-Instance aus. Stellen Sie auf der Registerkarte Konfiguration sicher, dass die Verschlüsselung für die Instance nicht aktiviert ist. Eine Bildschirmdarstellung finden Sie im Abschnitt Zusätzliche Informationen.	DBA
Erstellen Sie den DB-Snapshot.	Erstellen Sie einen DB-Snapshot der Instance, die Sie verschlüsseln möchten. Wie lange die Erstellung eines Snapshots dauert, hängt von der Größe Ihrer Datenbank ab. Anweisungen finden Sie unter Erstellen eines DB-Snapshots in der Amazon-RDS-Dokumentation.	DBA
Verschlüsseln Sie den Snapshot.	Wählen Sie im Navigationsbereich der Amazon-RDS-Konsole Snapshots und dann den von Ihnen erstellten DB-Snapshot aus. Wählen Sie für Actions (Aktionen) die Option Copy Snapshot (Snapshot kopieren). Geben Sie die AWS-Zielregion und	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Namen der DB-Snapshot-Kopie in den entsprechenden Feldern an. Aktivieren Sie das Kontrollkästchen Verschlüsselung aktivieren. Geben Sie für Master Key (Masterschlüssel) den Bezeichner des zum Verschlüsseln der DB-Snapshot-Kopie zu verwenden den KMS-Schlüssel an. Wählen Sie Copy Snapshot (Snapshot kopieren) aus. Weitere Informationen finden Sie unter Kopieren eines Snapshots in der Amazon-RDS-Dokumentation.	

Vorbereiten der Ziel-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den DB-Snapshot wieder her.	Wählen Sie in der Amazon-RDS-Konsole Snapshots aus. Wählen Sie den verschlüsselten Snapshot aus, den Sie erstellt haben. Wählen Sie unter Actions (Aktionen) die Option Restore Snapshot (Snapshot wiederherstellen). Geben Sie für DB-Instance-Kennung einen eindeutigen Namen für die neue DB-Instance an. Überprüfen Sie die Instance-Details und	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann DB-Instan ce wiederherstellen aus. Aus Ihrem Snapshot wird eine neue, verschlüsselte DB-Instance erstellt. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Snapshot in der Amazon-RDS-Dokumentation.	
Migrieren Sie Daten mithilfe von AWS DMS.	Erstellen Sie in der AWS DMS-Konsole eine AWS DMS-Aufgabe. Wählen Sie für Migrationstyp die Option Vorhandene Daten migrieren und laufende Änderungen replizieren aus. Wählen Sie unter Aufgabeneinstellun gen für Zieltabellenvorber eitungsmodus die Option Verkürzen aus. Weitere Informationen finden Sie unter Erstellen einer Aufgabe in der AWS DMS-Dokumentation.	DBA
Aktivieren Sie die Datenvali dierung.	Wählen Sie unter Aufgabene instellungen die Option Validierung aktivieren aus. Auf diese Weise können Sie die Quelldaten mit den Zieldaten vergleichen, um sicherzus tellen, dass die Daten korrekt migriert wurden.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie Einschränkungen für die Ziel-DB-Instance.	Deaktivieren Sie alle Auslöser und Fremdschlüsseleinschränkungen auf der Ziel-DB-Instance und starten Sie dann die AWS DMS-Aufgabe. Weitere Informationen zum Deaktivieren von Auslösern und Fremdschlüsseleinschränkungen finden Sie in der AWS DMS-Dokumentation.	DBA
Überprüfen Sie die Daten.	Überprüfen Sie nach Abschluss des vollständigen Ladevorgangs die Daten auf der Ziel-DB-Instance, um festzustellen, ob sie mit den Quelldaten übereinstimmen. Weitere Informationen finden Sie unter AWS DMS-Datenvalidierung in der AWS DMS-Dokumentation.	DBA

Umstellung auf die Ziel-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie Schreibvorgänge auf der Quell-DB-Instance.	Halten Sie die Schreibvorgänge auf der Quell-DB-Instance an, damit die Anwendungsausfallzeit beginnen kann. Stellen Sie sicher, dass AWS DMS die Replikation für die Daten in der Pipeline abgeschlossen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hat. Aktivieren Sie Auslöser und Fremdschlüssel auf der Ziel-DB-Instance.	
Aktualisieren von Datenbank sequenzen	Wenn die Quelldatenbank Sequenznummern enthält, überprüfen und aktualisieren Sie die Sequenzen in der Zieldatenbank.	DBA
Konfigurieren Sie den Anwendungsendpunkt.	Konfigurieren Sie Ihre Anwendungsverbindungen für die Verwendung der neuen Endpunkte der Amazon-RDS-DB-Instance. Die DB-Instance ist jetzt verschlüsselt.	DBA, Anwendungsbesitzer

Zugehörige Ressourcen

- Erstellen einer AWS DMS-Aufgabe
- Überwachen von Replikationsaufgaben mit Amazon CloudWatch
- Überwachen von AWS DMS-Aufgaben
- Aktualisieren des Amazon-RDS-Verschlüsselungsschlüssels

Zusätzliche Informationen

Überprüfen der Verschlüsselung für die PostgreSQL-DB-Quell-Instance:

Zusätzliche Hinweise für dieses Muster:

- Aktivieren Sie die Replikation in PostgreSQL, indem Sie den `rds.logical_replication` Parameter auf 1 setzen.

Wichtiger Hinweis: Replikations-Slots behalten die Write-Ahead-Log-Dateien (WAL), bis die Dateien extern verbraucht werden, z. B. von `pg_recvlogical`, ETL-Aufträgen (Extract, Transform, Load) oder von AWS DMS. Wenn Sie den `rds.logical_replication` Parameterwert auf 1 setzen, legt AWS DMS die `max_connections` Parameter `wal_level`, `max_wal_sendersmax_replication_slots`, und fest. Wenn logische Replikations-Slots vorhanden sind, aber kein Konsument für die vom Replikations-Slot beibehaltenen WAL-Dateien vorhanden ist, können Sie eine Zunahme der Transaktionsprotokoll-Festplattennutzung und eine konstante Abnahme des freien Speicherplatzes feststellen. Weitere Informationen und Schritte zur Behebung dieses Problems finden Sie im Artikel Wie kann ich feststellen, was den Fehler „Kein Speicherplatz mehr auf dem Gerät“ oder „DiskFull“ auf Amazon RDS für PostgreSQL verursacht? im AWS Support Knowledge Center.

- Alle Schemaänderungen, die Sie nach dem Erstellen des DB-Snapshots an der Quell-DB-Instance vornehmen, sind auf der Ziel-DB-Instance nicht vorhanden.
- Nachdem Sie eine verschlüsselte DB-Instance erstellt haben, können Sie den von dieser DB-Instance verwendeten KMS-Schlüssel nicht mehr ändern. Stellen Sie sicher, dass Sie Ihre KMS-Schlüsselanforderungen ermitteln, bevor Sie Ihre verschlüsselte DB-Instance erstellen.
- Sie müssen Auslöser und Fremdschlüssel auf der Ziel-DB-Instance deaktivieren, bevor Sie die AWS DMS-Aufgabe ausführen. Sie können diese wieder aktivieren, wenn die Aufgabe abgeschlossen ist.

Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen

Umgebung: Produktion	Technologien: Datenbanken; Cloud-nativ; Sicherheit, Identität, Compliance	AWS-Dienste: Amazon RDS; Amazon SNS; AWS CloudTrail; Amazon CloudWatch

Übersicht

Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der Amazon Web Services (AWS) Cloud erleichtert. Dieser Service bietet kostengünstige und anpassbare Kapazität für eine Branchenstandards entsprechende relationale Datenbank sowie die Verwaltung gängiger Datenbankaufgaben.

Sie können Tagging verwenden, um Ihre AWS-Ressourcen auf unterschiedliche Weise zu kategorisieren. Relationales Datenbank-Tagging ist nützlich, wenn Sie viele Ressourcen in Ihrem Konto haben und Sie anhand der Tags schnell eine bestimmte Ressource identifizieren möchten. Sie können Amazon RDS-Tags verwenden, um Ihren RDS-DB-Instances benutzerdefinierte Metadaten hinzuzufügen. Ein Tag besteht aus einem benutzerdefinierten Schlüssel und Wert. Wir empfehlen Ihnen, einen konsistenten Satz von Stichwörtern zu erstellen, um die Anforderungen Ihrer Organisation zu erfüllen.

Dieses Muster bietet eine CloudFormation AWS-Vorlage, mit der Sie RDS-DB-Instances überwachen und kennzeichnen können. Die Vorlage erstellt ein Amazon CloudWatch Events-Ereignis, das auf das AWS-Ereignis CloudTrail CreateDBInstance achtet. (CloudTrail erfasst API-Aufrufe für Amazon RDS als Ereignisse.) Wenn es dieses Ereignis erkennt, ruft es eine AWS-Lambda-Funktion auf, die automatisch von Ihnen definierte Tag-Schlüssel und -Werte anwendet. Die Vorlage sendet auch eine Benachrichtigung, dass die Instance mithilfe von Amazon Simple Notification Service (Amazon SNS) markiert wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hochladen des Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Tagging-Benachrichtigungen erhalten möchten.

Einschränkungen

- Die Lösung unterstützt CloudTrail CreateDBInstance-Ereignisse. Es erstellt keine Benachrichtigungen für andere Ereignisse.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage in jeder Region oder jedem Konto nur einmal ausführen.

Tools

AWS-Services

- AWS CloudTrail — AWS CloudTrail ist ein AWS-Service, der Sie bei der Steuerung, Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos unterstützt. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events wird sofort auf betriebliche Änderungen aufmerksam und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne dass Server bereitgestellt oder verwaltet werden müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro

Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `index.zip`ist eine komprimierte Datei, die den Lambda-Code für dieses Muster enthält.
- `rds.yaml`ist eine CloudFormation Vorlage, die den Lambda-Code bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie den Lambda-Code bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `index.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen (RDS-DB-Instances), die Sie überwachen möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `rds.yaml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die RDS-DB-Instances, die Sie überwachen möchten.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B. `index.zip` oder). `controls/index.zip`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokollierungsebene an.	Geben Sie die Protokollierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt
Geben Sie die Tag-Schlüssel und Werte für Ihre RDS-DB-Instances ein.	Geben Sie die erforderlichen Tag-Schlüssel und -Werte ein, die Sie automatisch auf die RDS-Instance anwenden möchten. Weitere Informationen finden Sie unter Tagging Amazon RDS-Ressourcen in der AWS-Dokumentation.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, wenn Ihre Instances markiert wurden, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Markieren von Amazon RDS-Ressourcen (Amazon Aurora Aurora-Dokumentation)
- Objekte hochladen (Amazon S3 S3-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudWatch Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität

Umgebung: Produktion	Technologien: Datenbanken; Cloud-nativ; Serverlos; Kostenmanagement	AWS-Dienste: Amazon DynamoDB

Übersicht

Amazon DynamoDB ist eine NoSQL-Transaktionsdatenbank, die selbst im Petabyte-Bereich Latenz im einstelligen Millisekundenbereich bietet. Dieses serverlose Angebot von Amazon Web Services (AWS) erfreut sich aufgrund seiner gleichbleibenden Leistung und Skalierbarkeit immer größerer Beliebtheit. Sie müssen die zugrunde liegende Infrastruktur nicht bereitstellen. Ihre einzelne Tabelle kann bis zu Petabyte groß werden.

Im On-Demand-Kapazitätsmodus zahlen Sie pro Anfrage für die Lese- und Schreibvorgänge, die Ihre Anwendung an den Tabellen durchführt. Die AWS-Gebühren basieren auf den kumulierten Read Request Units (RRUs) und WRITE Request Units (WRUs) in einem Monat. DynamoDB überwacht den ganzen Monat über kontinuierlich die Größe Ihrer Tabelle, um Ihre Speichergebühren zu ermitteln. Es unterstützt kontinuierliches Backup mit point-in-time-recovery (PITR). DynamoDB überwacht den ganzen Monat über kontinuierlich die Größe Ihrer PITR-fähigen Tabellen, um Ihre Backup-Gebühren zu ermitteln.

Um die DynamoDB-Kosten für ein Projekt abzuschätzen, ist es wichtig zu berechnen, wie viel RRU, WRU und Speicherplatz in den verschiedenen Phasen Ihres Produktlebenszyklus verbraucht werden. Für eine grobe Kostenschätzung können Sie den AWS-Preisrechner verwenden. Sie müssen jedoch eine ungefähre Anzahl von RRUs, WRUs und Speicheranforderungen für Ihre Tabelle angeben. Zu Beginn des Projekts kann es schwierig sein, diese abzuschätzen. Der AWS-Preisrechner berücksichtigt weder die Datenwachstumsrate noch die Artikelgröße und berücksichtigt auch nicht die Anzahl der Lese- und Schreibvorgänge für die Basistabelle und die globalen Sekundärindizes (GSIs) getrennt. Um den AWS-Preisrechner verwenden zu können, müssen Sie all diese Aspekte abschätzen, um von ungefähren Zahlen für WRU, RRU und Speichergröße auszugehen, um Ihre Kostenschätzung zu erhalten.

Dieses Muster bietet einen Mechanismus und eine wiederverwendbare Microsoft Excel-Vorlage zur Schätzung grundlegender DynamoDB-Kostenfaktoren wie Schreib-, Lese-, Speicher-,

Sicherungs- und Wiederherstellungskosten für den On-Demand-Kapazitätsmodus. Er ist detaillierter als der AWS-Preisrechner und berücksichtigt die Anforderungen der Basistabelle und der GSI unabhängig voneinander. Es berücksichtigt auch die monatliche Wachstumsrate der Artikeldaten und prognostiziert die Kosten für drei Jahre.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse in DynamoDB und DynamoDB-Datenmodelldesign
- Grundkenntnisse zu DynamoDB-Preisen, WRU, RRU, Speicher sowie Backup und Recovery (weitere Informationen finden Sie unter Preise für On-Demand-Kapazität)
- Kenntnis Ihrer Daten, Ihres Datenmodells und Ihrer Elementgröße in DynamoDB
- Kenntnisse der DynamoDB-GSIs

Einschränkungen

- Die Vorlage bietet Ihnen eine ungefähre Berechnung, ist jedoch nicht für alle Konfigurationen geeignet. Um eine genauere Schätzung zu erhalten, müssen Sie die individuelle Artikelgröße für jedes Element in der Basistabelle und den GSIs messen.
- Für eine genauere Schätzung müssen Sie die erwartete Anzahl von Schreibvorgängen (Einfügen, Aktualisieren und Löschen) und Lesevorgängen für jedes Element in einem durchschnittlichen Monat berücksichtigen.
- Dieses Muster ermöglicht es, nur die Schreib-, Lese-, Speicher-, Sicherungs- und Wiederherstellungskosten für die nächsten Jahre auf der Grundlage fester Annahmen zum Datenwachstum zu schätzen.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Andere Tools

- Der AWS-Preisrechner ist ein webbasiertes Planungstool, mit dem Sie Schätzungen für Ihre AWS-Anwendungsfälle erstellen können.

Bewährte Methoden

Um die Kosten niedrig zu halten, sollten Sie die folgenden Best Practices für den DynamoDB-Entwurf berücksichtigen.

- Entwerfen von Partitionsschlüsseln – Verwenden Sie einen Partitionsschlüssel mit hoher Kardinalität, um die Last gleichmäßig zu verteilen.
- Entwurfsmuster für Adjazenzlisten — Verwenden Sie dieses Entwurfsmuster für Verwaltung one-to-many und Beziehungen. many-to-many
- Sparser Index – Verwenden Sie den Sparse-Index für Ihre GSIs. Wenn Sie einen GSI erstellen, geben Sie einen Partitionsschlüssel und optional einen Sortierschlüssel an. Nur Elemente in der Basistabelle, die einen entsprechenden GSI-Partitionsschlüssel enthalten, werden im Sparse-Index angezeigt. Dies trägt dazu bei, die GSIs kleiner zu halten.
- Überladen von Indizes – Verwenden Sie dieselbe GSI für die Indizierung verschiedener Arten von Elementen.
- GSI Write-Sharding— Sharden Sie mit Bedacht, um Daten auf die Partitionen zu verteilen und so effiziente und schnellere Abfragen zu ermöglichen.
- Große Gegenstände – Speichern Sie nur Metadaten in der Tabelle, speichern Sie den Blob in Amazon S3 und behalten Sie die Referenz in DynamoDB bei. Teilen Sie große Elemente in mehrere Elemente auf und indizieren Sie sie effizient mithilfe von Sortierschlüsseln.

Weitere bewährte Methoden finden Sie im Leitfaden für Entwickler von Amazon DynamoDB.

Epen

Extrahieren Sie Artikelinformationen aus Ihrem DynamoDB-Datenmodell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Artikelgröße ermitteln.	1. Prüfen Sie, wie viele verschiedene Artikelty pen Sie in Ihrer Tabelle speichern werden.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Um die Größe jedes Elements in Kilobyte zu berechnen, fügen Sie die Schlüssel- und Wertgröße jedes Attributs hinzu. 3. Berechnet die Elementgröße für eine Basistabelle und für jeden globalen Index.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Schätzen Sie die Schreibkosten ab.	Um die Schreibkosten im On-Demand-Kapazitätsmodus zu schätzen, müssen Sie zunächst messen, wie viele WRUs in einem Monat verbraucht werden. Dazu müssen Sie die folgenden Faktoren berücksichtigen:
	• Anzahl der Erstellungs-, Aktualisierungs- und Löschvorgänge für jedes Element in einem Monat.
	• Anzahl der verfügbaren GSIs. Betrachten Sie jeden Index unabhängig voneinander.
	  • Durchschnittliche Größe eines Indexelements
	  • Anzahl der Synchronisationszeiten für einen Index
	• Wie viele neue Dinge (z. B. Komponenten oder Produkte) werden der Tabelle jeden Monat hinzugefügt? Die Anzahl der hinzugefügten Dinge kann von Monat zu Monat unterschiedlich sein, aber Sie können auf der Grundlage Ihrer Geschäftsszenarien von
		Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einer durchschnittlichen Wachstumsrate ausgehen. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.	
Schätzen Sie die Lesekosten ab.	Um die Lesekosten im On-Demand-Modus zu schätzen, müssen Sie zunächst messen, wie viele RRUs in einem Monat verbraucht werden. Dazu müssen Sie die folgenden Faktoren berücksichtigen: • Anzahl der verfügbaren GSIs. Betrachten Sie jeden Index unabhängig voneinander. • Durchschnittliche Größe eines Indexelements • Durchschnittliche Anzahl von Lesevorgängen pro Produkt und Monat. • Anzahl der insgesamt verfügbaren Dinge (Komponenten oder Produkte) in der DynamoDB-Tabelle.	Dateningenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie die Speicherg röße und die Kosten ab.	Schätzen Sie zunächst den durchschnittlichen monatlich en Lagerbedarf auf der Grundlage Ihrer Artikelgröße in der Tabelle. Berechnen Sie dann die Speicherkosten, indem Sie die Speichergröße mit dem Speicherpreis pro GB für Ihre AWS-Region multipliz ieren. Wenn Sie bereits Daten zur Schätzung der Schreibkosten eingegeben haben, müssen Sie diese zur Berechnung der Speichergröße nicht erneut eingeben. Andernfalls müssen Sie bei der Schätzung der Speichergröße die folgenden Faktoren berücksichtigen: • Anzahl der Datenelemente in einem Modul (Produkt) , basierend auf Ihrem Tabellenentwurf. • Durchschnittliche Elementgr öße in Kilobyte. • Anzahl der verfügbaren GSIs. Betrachten Sie jeden Index unabhängig voneinander. • Durchschnittliche Größe eines Indexelements	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wie viele neue Produkte werden jeden Monat in die Tabelle aufgenomm en? Die Anzahl der neuen Produkte kann von Monat zu Monat unterschiedlich sein, aber Sie können auf der Grundlage Ihrer Geschäftsszenarien von einer durchschnittlichen Wachstumsrate ausgehen. In diesem Beispiel werden durchschnittlich 10 Millionen neue Produkte pro Monat verwendet.	

Geben Sie die Artikel- und Objektinformationen in die Excel-Vorlage ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Excel-Vorlage aus dem Bereich Anlagen herunter und passen Sie sie an Ihre Anwendungsfalltabelle an.	1. Laden Sie die Excel-Vor lage herunter. 2. Passen Sie das Geschäfts modul und die GSIs an Ihr Tabellendesign an.	Dateningenieur
Geben Sie Informationen in die Excel-Vorlage ein.	1. Aktualisieren Sie die Artikelinformationen im Blatt. Daten nur in orangefarbenen Zellen aktualisieren. 2. Passen Sie die Objektnum mern an: Wie viel könnte	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Tabelle jeden Monat hinzugefügt werden? 3. Aktualisieren Sie die WRU- und RRU-Preise pro Million für Ihre AWS-Region. 4. Aktualisieren Sie die Speicher- und Backup-Pr eise pro GB-Monat für Ihre AWS-Region. 5. Aktualisieren Sie den Wiederherstellungspreis pro GB für Ihre AWS-Region. In der Vorlage gibt es drei Elemente oder Entitäten: Informationen, Metadaten und Beziehung. Es gibt zwei GSIs. Wenn Sie für Ihren Anwendungsfall mehr Elemente benötigen, erstellen Sie neue Zeilen. Wenn Sie mehr GSIs benötigen, kopieren Sie einen vorhanden en GSI-Block und fügen Sie ihn ein, um so viele GSI-Blöcke zu erstellen, wie Sie benötigen. Passen Sie dann die Berechnungen der Spalten SUM und TOTAL an.	

Zugehörige Ressourcen

Referenzen

- Amazon DynamoDB DynamoDB-Preise für On-Demand-Kapazität
- AWS-Preisrechner für DynamoDB
- Bewährte Methoden für Design und Architektur mit DynamoDB
- Erste Schritte mit DynamoDB

Anleitungen und Muster

- Modellieren von Daten mit Amazon DynamoDB
- Schätzen Sie die Speicherkosten für eine Amazon DynamoDB-Tabelle

Zusätzliche Informationen

Schreiben Sie ein Beispiel für eine Kostenberechnung

Das DynamoDB-Datenmodelldesign zeigt drei Elemente für ein Produkt und eine durchschnittliche Artikelgröße von 4 KB. Wenn Sie der DynamoDB-Basistabelle ein neues Produkt hinzufügen, verbraucht es die Anzahl der Elemente * (Artikelgröße/1 KB Schreibeinheit) = 3 * (4/1) = 12 WRU. In diesem Beispiel verbraucht das Produkt beim Schreiben von 1 KB 1 WRU.

Lesen Sie das Beispiel für die Kostenberechnung

Um die RRU-Schätzung zu erhalten, berücksichtigen Sie den Durchschnitt, wie oft jeder Artikel in einem Monat gelesen wird. Beispielsweise wird das Informationselement im Durchschnitt zehnmal pro Monat gelesen, und das Metadatenelement wird zweimal gelesen und das Beziehungselement wird fünfmal gelesen. In der Beispielvorlage gilt: Gesamt-RRU für alle Komponenten = Anzahl der jeden Monat neu erstellten Komponenten * RRU pro Komponente pro Monat = 10 Millionen * 17 RRU = 170 Millionen RRU pro Monat.

Jeden Monat werden neue Dinge (Komponenten oder Produkte) hinzugefügt, und die Gesamtzahl der Produkte wird im Laufe der Zeit zunehmen. Daher werden auch die RRU-Anforderungen im Laufe der Zeit steigen.

- Im ersten Monat RRU wird der Verbrauch 170 Millionen betragen.
- Im zweiten Monat wird der RRU-Verbrauch 2 * 170 Millionen = 340 Millionen betragen.
- Im dritten Monat wird der RRU-Verbrauch 3 × 170 Millionen = 510 Millionen betragen.

Die folgende Grafik zeigt die monatlichen RRU-Verbrauchs- und Kostenprognosen.

Beachten Sie, dass die Preise in der Grafik nur zur Veranschaulichung dienen. Um genaue Prognosen für Ihren Anwendungsfall zu erstellen, besuchen Sie die AWS-Preisseite und verwenden Sie diese Preise in der Excel-Tabelle.

Beispiele für die Berechnung der Kosten für Speicherung, Sicherung und Wiederherstellung

DynamoDB-Speicher, Backup und Wiederherstellung sind alle miteinander verbunden. Das Backup ist direkt mit dem Speicher verbunden, und die Wiederherstellung ist direkt mit der Größe des Backups verbunden. Mit zunehmender Tabellengröße steigen die entsprechenden Speicher-, Sicherungs- und Wiederherstellungskosten proportional.

Speichergröße und Kosten

Die Speicherkosten werden im Laufe der Zeit entsprechend Ihrer Datenwachstumsrate steigen. Nehmen wir beispielsweise an, dass die durchschnittliche Größe einer Komponente oder eines Produkts in der Basistabelle und den GSIs 11 KB beträgt und dass Ihrer Datenbanktabelle jeden Monat 10 Millionen neue Produkte hinzugefügt werden. In diesem Fall wächst die Größe Ihrer DynamoDB-Tabelle (11 KB x 10 Millionen) /1024/1024 = 105 GB pro Monat. Im ersten Monat beträgt Ihre Tabellenspeichergröße 105 GB, im zweiten Monat 105 + 105 = 210 GB usw.

- Im ersten Monat betragen die Speicherkosten 105 GB* Speicherpreis pro GB für Ihre AWS-Region.
- Für den zweiten Monat belaufen sich die Speicherkosten auf 210 GB* Speicherpreis pro GB für Ihre Region.
- Für den dritten Monat belaufen sich die Speicherkosten auf 315 GB* Speicherpreis pro GB für Ihre Region.

Informationen zur Speichergröße und zu den Kosten für die nächsten drei Jahre finden Sie im Abschnitt Speichergröße und Prognose.

Kosten für Backup

Die Backup-Kosten werden im Laufe der Zeit entsprechend Ihrer Datenwachstumsrate steigen. Wenn Sie Continuous Backup mit point-in-time-recovery (PITR) aktivieren, basieren die Gebühren für kontinuierliches Backup auf dem durchschnittlichen Speichervolumen pro Monat. In einem Kalendermonat entspricht die durchschnittliche Backup-Größe der Größe Ihres Tabellenspeichers, obwohl die tatsächliche Größe etwas anders sein kann. Da jeden Monat neue Produkte hinzugefügt

werden, werden die Gesamtspeichergröße und die Backup-Größe im Laufe der Zeit zunehmen. Beispielsweise könnte die durchschnittliche Backup-Größe von 105 GB für den ersten Monat auf 210 GB für den zweiten Monat ansteigen.

- Im ersten Monat belaufen sich die Backup-Kosten auf 105 GB-Monat* Preis für kontinuierliches Backup pro GB für Ihre AWS-Region.
- Im zweiten Monat belaufen sich die Backup-Kosten auf 210 GB-Monat* Preis für kontinuierliches Backup pro GB für Ihre Region.
- Im dritten Monat belaufen sich die Backup-Kosten auf 315 GB pro Monat * Preis für kontinuierliches Backup pro GB für Ihre Region.
- und so weiter

Die Backup-Kosten sind in der Grafik im Abschnitt Speichergröße und Kostenprognose enthalten.

Kosten für die Wiederherstellung

Wenn Sie ein kontinuierliches Backup mit aktiviertem PITR erstellen, richten sich die Gebühren für den Wiederherstellungsvorgang nach dem Umfang der Wiederherstellung. Bei jeder Wiederherstellung zahlen Sie auf der Grundlage von Gigabyte wiederhergestellter Daten. Wenn Ihre Tabelle groß ist und Sie die Wiederherstellung mehrmals im Monat durchführen, ist dies kostspielig.

Um die Wiederherstellungskosten abzuschätzen, wird in diesem Beispiel davon ausgegangen, dass Sie einmal pro Monat am Monatsende eine PITR-Wiederherstellung durchführen. In dem Beispiel wird die durchschnittliche monatliche Backup-Größe als Größe der Wiederherstellungsdaten für diesen Monat verwendet. Für den ersten Monat beträgt die durchschnittliche Backup-Größe 105 GB, und für die Wiederherstellung am Monatsende würde die Größe der Wiederherstellungsdaten 105 GB betragen. Für den zweiten Monat wären es 210 GB und so weiter.

Die Wiederherstellungskosten werden im Laufe der Zeit entsprechend Ihrer Datenwachstumsrate steigen.

- Im ersten Monat betragen die Wiederherstellungskosten 105 GB* Wiederherstellungspreis pro GB für Ihre AWS-Region.
- Im zweiten Monat belaufen sich die Wiederherstellungskosten auf 210 GB* Wiederherstellungspreis pro GB für Ihre Region.
- Im dritten Monat belaufen sich die Wiederherstellungskosten auf 315 GB* Wiederherstellungspreis pro GB für Ihre Region.

Weitere Informationen finden Sie auf der Registerkarte Speicher, Sicherung und Wiederherstellung in der Excel-Vorlage und in der Grafik im folgenden Abschnitt.

Prognose der Speichergröße und der Kosten

In der Vorlage wird die tatsächliche fakturierbare Speichergröße berechnet, indem das kostenlose Kontingent 25 GB pro Monat für die Standard-Tabellenklasse subtrahiert wird. In dem Blatt erhalten Sie ein Prognosediagramm, das in monatliche Werte unterteilt ist.

Das folgende Beispieldiagramm prognostiziert die monatliche Speichergröße in GB, die fakturierbaren Speicherkosten, die Kosten für On-Demand-Backups und die Wiederherstellungskosten für die nächsten 36 Kalendermonate. Alle Kosten sind in USD angegeben. Aus der Grafik wird deutlich, dass die Speicher-, Backup- und Wiederherstellungskosten proportional zur Speichergröße steigen.

Beachten Sie, dass die in der Grafik verwendeten Preise nur zur Veranschaulichung dienen. Um genaue Preise für Ihren Anwendungsfall zu erstellen, besuchen Sie die AWS-Preisseite und verwenden Sie diese Preise in der Excel-Vorlage.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Schätzen der Speicherkosten für eine Amazon-DynamoDB-Tabelle

Erstellt von Moinul Al-Mamun

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Big Data; Kostenmanagement; Speicher und Backup	AWS-Services: Amazon DynamoDB

Übersicht

Amazon DynamoDB ist eine NoSQL-Transaktionsdatenbank, die Latenz im einstelligen Millisekundenbereich auch bei Petabyte bietet. Dieses Serverless-Angebot von Amazon Web Services (AWS) wird aufgrund seiner konsistenten Leistung und Skalierbarkeit immer beliebter. Sie müssen keinen Speicher bereitstellen. Ihre einzelne Tabelle kann bis zu Petabyte groß werden.

DynamoDB überwacht die Größe Ihrer Tabelle im Laufe des Monats kontinuierlich, um Ihre Speichergebühren zu ermitteln. AWS berechnet Ihnen dann die durchschnittliche Speichergröße in Gigabyte. Je mehr Ihre Tabelle im Laufe der Zeit wächst, desto höher werden Ihre Speicherkosten. Um die Speicherkosten zu berechnen, können Sie AWS Pricing Calculator verwenden. Sie müssen jedoch die ungefähre Größe Ihrer Tabelle angeben, einschließlich globaler sekundärer Indizes (GSIs), was zu Beginn des Projekts wirklich schwer abzuschätzen ist. Außerdem berücksichtigt AWS Pricing Calculator die Datenwachstumsrate nicht.

Dieses Muster bietet einen Mechanismus und eine wiederverwendbare Microsoft Excel-Vorlage zur Berechnung von DynamoDB-Speichergröße und -kosten. Es berücksichtigt die Speicheranforderungen für die Basistabelle und die GSIs unabhängig. Es berechnet die Speichergröße unter Berücksichtigung der Größe Ihrer einzelnen Elemente und der Datenwachstumsrate im Laufe der Zeit.

Um eine Schätzung zu erhalten, fügen Sie zwei Informationen in die Vorlage ein:

- Die Größe des einzelnen Elements in Kilobyte für die Basistabelle und GSIs
- Wie viele neue Objekte oder Produkte der Tabelle im Durchschnitt in einem Monat hinzugefügt werden könnten (z. B. 10 Millionen)

Die Vorlage generiert ein Speicher- und Kostenprognosediagramm für die nächsten drei Jahre, wie im folgenden Beispiel gezeigt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundlegendes Wissen über DynamoDB sowie DynamoDB-Speicher und -Preise
- Kenntnisse Ihrer Daten, Ihres Datenmodells und Ihrer Elementgröße in DynamoDB
- Kenntnisse der globalen sekundären Indizes (GSIs) von DynamoDB

Einschränkungen

- Die Vorlage liefert Ihnen eine ungefähre Berechnung, ist aber nicht für alle Konfigurationen geeignet. Um eine genauere Schätzung zu erhalten, müssen Sie die individuelle Elementgröße für jedes Element in der Basistabelle und den GSIs messen.
- Dieses Muster unterstützt die Schätzung nur der Speichergröße und der Kosten für die nächsten Jahre auf der Grundlage fester Annahmen zum Datenwachstum.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Andere Tools

- AWS Pricing Calculator ist ein webbasiertes Planungstool, mit dem Sie Schätzungen für Ihre AWS-Anwendungsfälle erstellen können.

Polen

Extrahieren von Elementinformationen aus Ihrem DynamoDB-Datenmodell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Elementgröße ab.	1. Überprüfen Sie, wie viele verschiedene Elementtypen Sie in Ihrer Tabelle speichern werden. 2. Um die Größe jedes Elements in Kilobyte zu berechnen, addieren Sie die Schlüssel- und Wertgröße jedes Attributs. 3. Berechnen Sie die Elementgröße für eine Basistabelle und für jeden GSI.	Dateningenieur
Rufen Sie die Anzahl der Objekte ab, die in einem Monat hinzugefügt wurden.	Schätzen Sie, wie viele Komponenten oder Objekte durchschnittlich in einem Monat zur DynamoDB-Tabelle hinzugefügt werden.	Dateningenieur

Geben Sie die Element- und Objektinformationen in die Excel-Vorlage ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Excel-Datenblatt aus dem angehängten Dokument herunter und passen Sie es an Ihre Anwendungsfalltabelle an.	1. Laden Sie die Excel-Vorlage herunter. 2. Passen Sie das Geschäftsmodul und die GSIs an Ihr Tabellendesign an.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie Informationen in die Excel-Vorlage ein.	1. Aktualisieren Sie Elementinformationen im Blatt. 2. Passen Sie die Objektnummern an: Wie viel könnte jeden Monat zur Tabelle hinzugefügt werden? 3. Aktualisieren Sie den Speicherpreis pro GB-Monat für Ihre AWS-Region.	Dateningenieur

Zugehörige Ressourcen

- On-Demand-Preise für Amazon DynamoDB
- AWS-Preisrechner für DynamoDB

Zusätzliche Informationen

Beachten Sie, dass die angehängte Vorlage nur Speichergröße und -kosten für die Speichertabellenklasse Standard prognostiziert. Basierend auf der Prognose für die Speicherkosten und unter Berücksichtigung der Größe einzelner Elemente und der Produkt- oder Objektwachstumsrate können Sie Folgendes schätzen:

- Kosten für den Datenexport
- Backup- und Wiederherstellungskosten
- Anforderungen an die Datenspeicherung.

Amazon-DynamoDB-Datenspeicherkosten

DynamoDB überwacht die Größe Ihrer Tabellen kontinuierlich, um Ihre Speichergebühren zu ermitteln. DynamoDB misst die Größe Ihrer abrechenbaren Daten, indem es die Rohbytegröße Ihrer Daten plus einen Speicheraufwand pro Element hinzufügt, der von den Features abhängt, die Sie aktiviert haben. Weitere Informationen finden Sie im DynamoDB-Entwicklerhandbuch.

Der Preis für die Datenspeicherung hängt von Ihrer Tabellenklasse ab. Die ersten 25 GB, die jeden Monat gespeichert werden, sind kostenlos, wenn Sie die DynamoDB-Standard-Tabellenklasse verwenden. Weitere Informationen zu den Speicherkosten für die Tabellenklasse Standard und Standard-Infrequent Access in verschiedenen AWS-Regionen finden Sie unter Preise für On-Demand-Kapazität.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Schätzen der Amazon RDS-Engine-Größe für eine Oracle-Datenbank mithilfe von AWR-Berichten

Erstellt von Abhishek Verma (AWS) und Eduardoentim (AWS)

Umgebung: Produktion	Quelle: Oracle Database	Ziel: Amazon RDS oder Amazon Aurora
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Datenbanken; Migration
AWS-Services: Amazon RDS; Amazon Aurora		

Übersicht

Wenn Sie eine Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) oder Amazon Aurora migrieren, ist die Berechnung der CPU, des Arbeitsspeichers und der Festplatten-I/O für die Zieldatenbank eine wichtige Anforderung. Sie können die erforderliche Kapazität der Zieldatenbank schätzen, indem Sie die Oracle Automatic Workload Repository (AWR)-Berichte analysieren. In diesem Muster wird erläutert, wie Sie AWR-Berichte verwenden, um diese Werte zu schätzen.

Die Oracle-Quelldatenbank kann sich On-Premises befinden oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance gehostet werden, oder es könnte sich um eine DB-Instance von Amazon RDS für Oracle handeln. Die Zieldatenbank könnte eine beliebige Amazon RDS- oder Aurora-Datenbank sein.

Hinweis: Kapazitätsschätzungen werden genauer sein, wenn Ihre Zieldatenbank-Engine Oracle ist. Bei anderen Amazon-RDS-Datenbanken kann die Engine-Größe aufgrund von Unterschieden in der Datenbankarchitektur variieren.

Wir empfehlen Ihnen, den Leistungstest durchzuführen, bevor Sie Ihre Oracle-Datenbank migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Lizenz für Oracle Database Enterprise Edition und eine Lizenz für Oracle Diagnostics Pack zum Herunterladen von AWR-Berichten.

Produktversionen

- Alle Oracle Database Editionen für die Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c,19c.
- Dieses Muster deckt weder Oracle Engineered Systems noch Oracle Cloud Infrastructure (OCI) ab.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Oracle-Datenbank
- Eine Oracle-Datenbank auf einer EC2-Instance
- Eine DB-Instance von Amazon RDS für Oracle

Zieltechnologie-Stack

- Jede Amazon RDS- oder Amazon Aurora-Datenbank

Zielarchitektur

Informationen zum vollständigen Migrationsprozess finden Sie im Muster Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mithilfe von AWS DMS und AWS SCT .

Automatisierung und Skalierung

Wenn Sie mehrere Oracle-Datenbanken migrieren müssen und zusätzliche Leistungsmetriken verwenden möchten, können Sie den Prozess automatisieren, indem Sie die im Blogbeitrag Größengerechte Amazon RDS-Instances in großem Umfang basierend auf Oracle-Leistungsmetriken beschriebenen Schritte ausführen.

Tools

- Oracle Automatic Workload Repository (AWR) ist ein Repository, das in Oracle-Datenbanken integriert ist. Es sammelt und speichert regelmäßig Systemaktivitäts- und Workload-Daten, die dann von Automatic Database Diagnostic Monitor (ADDM) analysiert werden. AWR erstellt regelmäßig Snapshots von Systemleistungsdaten (standardmäßig alle 60 Minuten) und speichert die Informationen (standardmäßig bis zu 8 Tage). Sie können AWR-Ansichten und -Berichte verwenden, um diese Daten zu analysieren.

Bewährte Methoden

- Um den Ressourcenbedarf für Ihre Zieldatenbank zu berechnen, können Sie einen einzelnen AWR-Bericht, mehrere AWR-Berichte oder dynamische AWR-Ansichten verwenden. Wir empfehlen Ihnen, während der Spitzenlastphase mehrere AWR-Berichte zu verwenden, um die Ressourcen zu schätzen, die für die Bewältigung dieser Spitzenlasten erforderlich sind. Darüber hinaus bieten dynamische Ansichten mehr Datenpunkte, mit denen Sie den Ressourcenbedarf genauer berechnen können.
- Sie sollten IOPS nur für die Datenbank schätzen, die Sie migrieren möchten, nicht für andere Datenbanken und Prozesse, die den Datenträger verwenden.
- Um zu berechnen, wie viel E/A von der Datenbank verwendet wird, verwenden Sie nicht die Informationen im Abschnitt Ladeprofil des AWR-Berichts. Verwenden Sie stattdessen den Abschnitt I/O-Profil, falls dieser verfügbar ist, oder fahren Sie mit dem Abschnitt Instance-Aktivitätsstatistiken fort und sehen Sie sich die Gesamtwerte für physische Lese- und Schreibvorgänge an.
- Wenn Sie die CPU-Auslastung schätzen, empfehlen wir, anstelle von Betriebssystemstatistiken (OS) die Datenbankmetrikmethode zu verwenden, da sie auf der nur von Datenbanken verwendeten CPU basiert. (OS-Statistiken beinhalten auch die CPU-Auslastung durch andere Prozesse.) Sie sollten auch CPU-bezogene Empfehlungen im ADDM-Bericht überprüfen, um die Leistung nach der Migration zu verbessern.
- Berücksichtigen Sie I/O-Durchsatzlimits – Amazon Elastic Block Store (Amazon EBS)-Durchsatz und Netzwerkdurchsatz – für die spezifische Instance-Größe, wenn Sie den richtigen Instance-Typ ermitteln.
- Führen Sie den Leistungstest vor der Migration durch, um die Engine-Größe zu überprüfen.

Polen

Erstellen eines AWR-Berichts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den AWR-Bericht.	Um den Bericht zu aktivieren, folgen Sie den Anweisungen in der Oracle-Dokumentation.	DBA
Überprüfen Sie den Aufbewahrungszeitraum.	Verwenden Sie die folgende Abfrage, um den Aufbewahrungszeitraum des AWR-Berichts zu überprüfen. `SQL> SELECT snap_interval,retention FROM dba_hist_wr_control;`	DBA
Generieren Sie den Snapshot.	Wenn das AWR-Snapshot-Intervall nicht detailliert genug ist, um die Spitze der Spitzenlast zu erfassen, können Sie den AWR-Bericht manuell generieren. Verwenden Sie die folgende Abfrage, um den manuellen AWR-Snapshot zu generieren. `SQL> EXEC dbms_workload_repository.create_snapshot;`	DBA
Überprüfen Sie die letzten Snapshots.	Verwenden Sie die folgende Abfrage, um die letzten AWR-Snapshots zu überprüfen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQL> SELECT snap_id, to_char(begin_interval_time,'dd/MON/yy hh24:mi') Begin_Interval, to_char(end_interval_time,'dd/MON/yy hh24:mi') End_Interval FROM dba_hist_snapshot ORDER BY 1;`	

Schätzung der Festplatten-I/O-Anforderungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Methode aus.	IOPS ist das Standardmaß für Eingabe- und Ausgabevorgänge pro Sekunde auf einem Speichergerät und umfasst sowohl Lese- als auch Schreibvorgänge. Wenn Sie eine On-Premises-Datenbank zu AWS migrieren, müssen Sie die maximale Festplatten-I/O ermitteln, die von der Datenbank verwendet wird. Sie können die folgenden Methoden verwenden, um die Festplatten-I/O für Ihre Zieldatenbank zu schätzen: • Abschnitt „Load Profile“ des AWR-Berichts	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Abschnitt Instance-Aktivitätsstatistiken des AWR-Berichts (verwenden Sie diesen Abschnitt für Oracle Database 12c oder höher) • Abschnitt „E/A-Profil“ des AWR-Berichts (verwenden Sie diesen Abschnitt für Oracle-Database-Versionen vor 12c) • AWR-Ansichten In den folgenden Schritten werden diese vier Methoden beschrieben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1: Verwenden Sie das Ladeprofil.	Die folgende Tabelle zeigt ein Beispiel für den Abschnitt Lastprofil des AWR-Berichts. Wichtig: Für genauere Informationen empfehlen wir, anstelle des Ladeprofils Option 2 (E/A-Profile) oder Option 3 (Statistiken zur Instance-Aktivität) zu verwenden. Pro Seku / Pro Trans on / Pro Exec / Pro Aufruf DB-Zeit(n): 26.6 / 0.2 / 0,00 / 0,02 DB-CPU: 18.0 / 0.1 / 0,00 / 0.01 Hinte nd-CPU: 0.2 / 0.0 / 0,00 / 0,00 Redo Größe (Byte 2 458 539,9 / 17.09 Logis Lese 3.37 ,5 / 23 449,(	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Blöc Blocl 21.6 150, rung Phys 13.5 94,4 s Lese (Blöc Phys 3.46 24.1 s Schr (Blöc Lese 3 24,9 von 586, I/ O- Anfo deru Schr 574. 4,0 von I/ O- Anfo deru Lese 106. 0.7 IO (MB) Schr 27.1 0.2 IO (MB)	

Aufgabe	Beschreibung		Erforderliche Fähigkeiten
	IM-Scarilen:	0.0	0.0
	Sitzu ogisc Lese IM:		
	Benu ufruf	1 245,7	8.7
	Pars (SQL	4.62(	32.2
	Hard Pars es (SQL	8.9	0.1
	SQL- Arbe tsber (MB)	824,9	5,7
	Anm en:	1,7	0.0
	Exec (SQL	136 656,5	950,4
	Rollb :	22,9	0.2
	Tran onen	143,8	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Basierend auf diesen Informationen können Sie IOPs und den Durchsatz wie folgt berechnen: IOPS = Lese-I/O-Anforderungen: + Schreib-I/O-Anforderungen = 3 586,8 + 574,7 = 4 134,5 Durchsatz = Physischer Lesevorgang (Blöcke) + Physischer Schreibvorgang (Blöcke) = 13 575,1 + 3 467,3 = 17 042,4 Da die Blockgröße in Oracle 8 KB beträgt, können Sie den Gesamtdurchsatz wie folgt berechnen: Der Gesamtdurchsatz in MB beträgt 17042,4 * 8 * 1024/1024/1024 = 133,2 MB Warnung: Verwenden Sie das Ladeprofil nicht, um die Instance-Größe zu schätzen. Sie ist nicht so genau wie Statistiken zur Instance-Aktivität oder I/O-Profile.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Verwenden Sie Instance-Aktivitätsstatistiken.	Wenn Sie eine Oracle-Datenbankversion vor 12c verwenden, können Sie den Abschnitt Instance-Aktivitätsstatistiken des AWR-Berichts verwenden, um IOPS und den Durchsatz zu schätzen. Die folgende Tabelle zeigt ein Beispiel für diesen Abschnitt. Statist / Gesan / pro Sekun / pro Trans Physis Lese-Gesamt-IO-Anforderun / 2 547 333 217 / 3.610, / 25.11 Physis Lesevenge in Bytes / 80.776.124. / 114.48 26,26 / 796.149 8 Gesan physis Schreirgänge für IO- / 534.19 08 / 757.1 / 5.27	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anforderungen Gesamt der physischen Schreibvorgänge in Byte 25.517.849.[illegible] 36.165[illegible],84 251.508,18 Basierend auf diesen Informationen können Sie die Gesamt-IOPS und den Durchsatz wie folgt berechnen: Gesamt-IOPS = 3 610,28 + 757,11 = 4 367 Gesamt-Mbit/s = 114 482 426,26 + 36 165 631,84 = 1506 48 058,1 / 1024 / 1024 = 143 Mbit/s	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 3: Verwenden Sie E/A-Profile.	In Oracle Database 12c enthält der AWR-Bericht einen Abschnitt I/O-Profile, der alle Informationen in einer einzigen Tabelle enthält und genauere Daten zur Datenbankleistung liefert. Die folgende Tabelle zeigt ein Beispiel für diesen Abschnitt. Lesen und Schrei pro Sekun / Gelese pro Sekun / Schreib pro Sekund Gesar l der Anforc ngen: 4.367, 3.610, 757.1 Datenl anford ngen: 4.161, 3 586,8 574.7 Optimi e Anforc ngen: 0.0 0.0 0.0 Erneut Anforc ngen: 179.3 2.8 176.6	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Gesar 143.7 109.2 34,5 (MB): Datenl 133.1 106.1 27.1 (MB): Optimi 0.0 0.0 0.0 e Gesar ße (MB): Wiede 7.6 2.7 4,9 en bis (MB): 4,9 Datenl 17 13.575 3.467,3 (Blöck 042,4 Über 5 5.360, 537.6 Puffer· 898,5 Ca che (Blöck Direkt 11.143 8.214, 2.929,7 (Blöck Diese Tabelle enthält die folgenden Werte für Durchsatz und Gesamt-IOPS: Durchsatz = 143 MBPS (ab der fünften Zeile mit der Bezeichnung Summe, zweite Spalte)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IOPS = 4.367,4 (ab der ersten Zeile mit der Bezeichnung Total Requests, zweite Spalte)	
Option 4: Verwenden Sie AWR-Ansichten.	Sie können dieselben IOPS- und Durchsatzinformationen mithilfe von AWR-Ansichten anzeigen. Verwenden Sie die folgende Abfrage, um diese Informationen abzurufen: `break on report compute sum of Value on report select METRIC_NAME,avg(AVERAGE) as "Value" from dba_hist_sysmetric_summary where METRIC_NAME in ('Physical Read Total IO Requests Per Sec','Physical Write Total IO Requests Per Sec') group by metric_name;`	DBA

Schätzung des CPU-Bedarfs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Methode aus.	Sie können die für die Zieldatenbank erforderliche CPU auf drei Arten schätzen:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Durch die Verwendung der tatsächlich verfügbaren Kerne des Prozessors • Durch die Verwendung der genutzten Kerne basierend auf Betriebssystemstat istiken • Durch die Verwendung der genutzten Kerne basierend auf Datenbankstatistiken Wenn Sie sich ausgelastete Kerne ansehen, empfehlen wir Ihnen, die Datenbank metrikmethode anstelle von Betriebssystemstatistiken zu verwenden, da sie auf der CPU basiert, die nur von den Datenbanken verwendet wird, die Sie migrieren möchten. (OS-Statistiken beinhalten auch die CPU-Auslastung durch andere Prozesse.) Sie sollten auch CPU-bezogene Empfehlungen im ADDM-Bericht überprüfen, um die Leistung nach der Migration zu verbessern. Sie können die Anforderungen auch auf der Grundlage der CPU-Generierung schätzen. Wenn Sie verschiedene CPU-Generationen verwenden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, können Sie die erforderl iche CPU der Zieldatenbank schätzen, indem Sie den Anweisungen im Whitepaper Demystifizierung der Anzahl der vCPUs für optimale Workload-Leistung folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Option 1: Schätzen Sie die Anforderungen basierend auf verfügbaren Kernen.	In AWR-Berichten:
	• CPUs beziehen sich auf logische und virtuelle CPUs.
	• Kerne sind die Anzahl der Prozessoren in einem physischen CPU-Chipsatz.
	• Ein Socket ist ein physische s Gerät, das einen Chip mit einer Karte verbindet. Multi-Core-Prozessoren verfügen über Sockets mit mehreren CPU-Kernen.
	
	Sie können verfügbare Kerne auf zwei Arten schätzen:
	• Verwenden von Betriebss ystembefehlen
	• Verwenden des AWR-Beric hts
	
	So schätzen Sie die verfügbar en Kerne mithilfe von Betriebssystembefehlen
	
	Verwenden Sie den folgenden Befehl, um die Kerne im Prozessor zu zählen.
	`$ cat /proc/cpuinfo | grep "cpu cores"|uniq`
	`cpu cores : 4`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cat /proc/cpuinfo | egrep "core id|physical id" | tr -d "\n" | sed s/physical/\\nphysical/g | grep -v ^$ | sort | uniq | wc -l`
	
	Verwenden Sie den folgenden Befehl, um die Sockets im Prozessor zu zählen.
	
	`grep "physical id" /proc/cpuinfo | sort -u`
	`physical id : 0`
	`physical id : 1`
	
	Hinweis: Es wird nicht empfohlen, Betriebssystembefehle wie nmon und sar zu verwenden, um die CPU-Auslastung zu extrahieren. Dies liegt daran, dass diese Berechnungen die CPU-Auslastung durch andere Prozesse beinhalten und möglicherweise nicht die tatsächliche CPU widerspiegeln, die von der Datenbank verwendet wird.
	
	So schätzen Sie die verfügbaren Kerne mithilfe des AWR-Berichts
	
	Sie können die CPU-Auslastung auch aus dem ersten Abschnitt des AWR-Berichts	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ableiten. Hier ist ein Auszug aus dem Bericht. D DB- Inst Inst Star Ver RA N ID num lichu g X <DE XX) 1 05- 12.1 NO Sep 0 23:(Hos Plat CPU Ker Soc Arbei Nar eiche (Ho (GB)) <ho Linu 80 80 2 441,7 e> x86 64- Bit In diesem Beispiel beträgt die Anzahl der CPUs 80, was darauf hinweist, dass es sich um logische (virtuelle) CPUs handelt. Sie können auch sehen, dass diese Konfigura tion zwei Sockets hat, einen physischen Prozessor auf jedem Socket (insgesamt zwei physische Prozessoren) und 40 Kerne für jeden physischen Prozessor oder Socket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Schätzen der CPU-Auslastung mithilfe von Betriebssystemstatistiken.	Sie können die Statistiken zur Betriebssystem-CPU-Auslastung entweder direkt im Betriebssystem (mit sar oder einem anderen Host-Betriebssystemdienstprogramm) oder durch Überprüfen der IDLE/(IDLE+BusY)-Werte im Abschnitt Betriebssystemstatistiken des AWR-Berichts überprüfen. Sie können die Sekunden der CPU sehen, die direkt von v$osstat verbraucht wird. Die AWR- und Statspack-Berichte zeigen diese Daten auch im Abschnitt Betriebssystemstatistiken an. Wenn sich mehrere Datenbanken im selben Feld befinden, haben sie alle die gleichen v$osstat-Werte für Y_TIME. Statistik Wert Endwert Ker_MEM 6 810 12.280.79 Y_BYTE 677 9.232 248 INAKTIV 175 160 EMORY_ 627 380 ES 333 653 632 568	DBA

Aufgabe	Beschreibung		Erforderliche Fähigkeiten
	SWAP_F _BYTES	17.145.6 4.336	17.145.87 2.384
	PASSY_ E	1 305 569 937	
	IDLE_TI	4.312.71 .839	
	IOWAIT_ ME	53.417.1 4	
	NICE_TI	29 815	
	SYS_TIM	148 567 570	
	USER_T	1.146.91 .783	
	LOAD	25	29
	VM_IN_E ES	593.920	
	VM_OUT TES	327 680	
	PHYSIC_ MORY_E S	474 362 417 152	
	NUM_CF	80	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	NUM_CF 80 ORES NUM_CF 2 OCKETS GLOBAL 4.194.30 CEIVE_S E_MAX GLOBAL 2 097 ND_SIZE 152 AX TCP_RE 87 380 VE_SIZE EFAULT TCP_RE 6.291.45 VE_SIZE AX TCP_RE 4.096 VE_SIZE IN TCP_SE 16.384 SIZE_DE ULT TCP_SE 4.194.30 SIZE_MA TCP_SE 4.096 SIZE_MI	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn es keine weiteren wichtigen CPU-Verbraucher im System gibt, berechnen Sie mit der folgenden Formel den Prozentsatz der CPU-Auslastung: Auslastung = Auslastungszeit/Gesamtzeit Ausgelastete Zeit = Anforderungen = v$osstat.Y_TIME C = Gesamtzeit (ausgelastet + im Leerlauf) C = Kapazität = v$.Y_TIME + v$.IDLE_TIME Auslastung = BusY_TIME / (BusY_TIME + IDLE_TIME) = -1.305.569.937 / (1.305.569.937 + 4.312.718.839) = 23 % genutzt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 3: Schätzen der CPU-Auslastung mithilfe von Datenbankmetriken.	Wenn mehrere Datenbanken im System ausgeführt werden, können Sie die Datenbank metriken verwenden, die am Anfang des Berichts angezeigt werden. Snap ID / Snap Zeit / Sitzu / Curso Si tzung Snap begi 1846 28-Sep-09:0(1226 35.8 Snap been 1854 06-Oct-2 13:0(1876 41.1 Vers en: 11.7! (Min(DB-Zeit: 312 625,4 (min. Verwenden Sie diese Formel, um Metriken zur CPU-Ausla stung abzurufen: Datenbank-CPU-Auslastung (% der verfügbaren CPU-Leistung) = CPU-Zeit / NUM_CPUS / verstrichene Zeit	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hier wird die CPU-Auslastung durch die CPU-Zeit beschrieben und stellt die für die CPU aufgewendete Zeit dar, nicht die Zeit, die auf die CPU wartet. Diese Berechnung führt zu: = 312 625,40/11 759,64/80 = 33 % der CPU werden verwendet Anzahl der Kerne (33 %) * 80 = 26,4 Kerne Gesamtzahl der Kerne = 26,4 * (120 %) = 31,68 Kerne Sie können den höheren dieser beiden Werte verwenden, um die CPU-Auslastung der Amazon RDS- oder Aurora-DB-Instance zu berechnen. Hinweis: Bei IBM AIX stimmt die berechnete Auslastung nicht mit den Werten aus dem Betriebssystem oder der Datenbank überein. Diese Werte stimmen auf anderen Betriebssystemen überein.	

Schätzung des Speicherbedarfs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie den Speicherbedarf mithilfe von Speicherstatistiken.	Sie können den AWR-Bericht verwenden, um den Speicher der Quelldatenbank zu berechnen und in der Zieldatenbank abzugleichen. Sie sollten auch die Leistung der vorhandenen Datenbank überprüfen und Ihre Speicheranforderungen reduzieren, um Kosten zu sparen, oder Ihre Anforderungen erhöhen, um die Leistung zu verbessern. Dies erfordert eine detaillierte Analyse der AWR-Antwortzeit und des Service Level Agreement (SLA) der Anwendung. Verwenden Sie die Summe aus Oracle System Global Area (SGA) und Program Global Area (PGA) als geschätzte Speicherauslastung für Oracle. Fügen Sie zusätzliche 20 Prozent für das Betriebssystem hinzu, um eine Anforderung an die Zielspeichergröße zu ermitteln. Verwenden Sie für Oracle RAC die Summe der geschätzten Speicherauslastung auf allen RAC-Knoten und reduzieren Sie den gesamten Speicher, da	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	er auf gemeinsamen Blöcken gespeichert ist. 1. Überprüfen Sie die Metriken in der Tabelle Instance-Effizienz in Prozent. Die Tabelle verwendet die folgenden Begriffe: • Puffer-Treffer in % ist der Prozentsatz der Fälle, in denen ein bestimmte r Block im Puffer-Ca che gefunden wurde, anstatt eine physische E/A durchzuführen. Für eine bessere Leistung sollten Sie 100 Prozent anvisieren. • Puffer-Nowait % liegen nahe bei 100 Prozent. • Latch-Treffer in % liegen nahe bei 100 Prozent. • % Nicht-Parse-CPU ist der Prozentsatz der CPU-Zeit, die für nicht analysierende Aktivität en aufgewendet wurde. Dieser Wert sollte nahe 100 Prozent liegen. Prozentsatz der Instance-Effizienz (Ziel 100 %)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Puffer No wait %: 99,99 Wieder en NoWa %: 100,00 Puffer Treffer in %: 99,84 In-Memo - Sortie orgän in %: 100,00 Biblio ks-Treffe r in %: 748,7 Soft Parse %: 99,81 Zum Analy en von % ausfü : 96,61 Latch Tre ffer in %: 100,00 Analy en von CPU zu Parse 72,73 % nicht parse CPU: 99,21	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Elaps %:	
	Flash Cache-Treffer in %: 0,00	
	In diesem Beispiel sehen alle Metriken gut aus, sodass Sie den SGA und den PGA für die vorhandene Datenbank als Kapazitätsplanungsanforderung verwenden können.	
	2. Überprüfen Sie den Abschnitt Speicherstatistiken und berechnen Sie den SGA/PGA.	
	Beginne Ende Host-Mem (MB): 452.387 452.387,3 SGA-Verwendung (MB): 220 544,0 220 544,0 PGA-Verwe 36 874,9 45.270,0	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ndung (MB): Gesamter verwendeter Instance-Speicher = SGA + PGA = 220 GB + 45 GB = 265 GB Fügen Sie 20 Prozent des Puffers hinzu: Gesamter Instance-Speicher = 1,2 * 265 GB = 318 GB Da SGA und PGA 70 Prozent des Host-Speichers ausmachen, ist der Gesamtspeicherbedarf: Gesamtspeicher des Hosts = 318/0,7 = 464 GB Hinweis: Wenn Sie zu Amazon RDS für Oracle migrieren, werden PGA und SGA basierend auf einer vordefinierten Formel vorab berechnet. Stellen Sie sicher, dass die vorberechneten Werte Ihren Schätzungen entsprechen.	

Ermitteln des DB-Instance-Typs der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie den DB-Instance-Typ basierend auf Festplatten-I/O-, CPU- und Speicherschätzungen.	Basierend auf den Schätzungen in den vorherigen Schritten sollte die Kapazität der Amazon-RDS- oder Aurora-Zieldatenbank wie folgt lauten: • 68 CPU-Kerne • 143 MB/s Durchsatz • 4 367 IOPS für Festplatten-I/O • 464 GB Arbeitsspeicher In der Amazon RDS- oder Aurora-Zieldatenbank können Sie diese Werte dem Instance-Typ db.r5.16xlarge zuordnen, der eine Kapazität von 32 Kernen, 512 GB RAM und 13.600 Mbit/s Durchsatz hat. Weitere Informationen finden Sie im AWS-BlogbeitragRight-size Amazon RDS instances in großem Umfang basierend auf Oracle-Leistungsmetriken.	DBA

Zugehörige Ressourcen

- Aurora-DB-Instance-Klasse (Amazon-Aurora-Dokumentation)
- Amazon RDS-DB-Instance-Speicher (Amazon RDS-Dokumentation)
- AWS Miner-Tool (GitHub Repository)

Exportieren von Amazon RDS for SQL Server-Tabellen in einen S3-Bucket mithilfe von AWS DMS

Erstellt von Subhani Shaik (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: RDS	Ziel: S3
R-Typ: N/A	Workload: Microsoft	Technologien: Datenbanken; Cloudnativ
AWS-Services: AWS DMS; Amazon RDS; Amazon S3; AWS Secrets Manager ;AWS Identity and Access Management		

Übersicht

Amazon Relational Database Service (Amazon RDS) für SQL Server unterstützt das Laden von Daten auf andere mit der DB-Engine verknüpfte Server in der Amazon Web Services (AWS) Cloud nicht. Stattdessen können Sie AWS Database Migration Service (AWS DMS) verwenden, um Amazon RDS für SQL Server-Tabellen in einen Amazon Simple Storage Service (Amazon S3)-Bucket zu exportieren, in dem die Daten für andere DB-Engines verfügbar sind.

AWS DMS unterstützt Sie bei der schnellen und sicheren Migration von Datenbanken zu AWS. Die Quelldatenbank bleibt während der Migration voll funktionsfähig und minimiert Ausfallzeiten für Anwendungen, die auf der Datenbank basieren. AWS DMS kann Ihre Daten zu und von den gängigsten kommerziellen und Open-Source-Datenbanken migrieren.

Dieses Muster verwendet AWS Secrets Manager bei der Konfiguration der AWS DMS-Endpunkte. Secrets Manager hilft Ihnen, Geheimnisse zu schützen, die für den Zugriff auf Ihre Anwendungen, Services und IT-Ressourcen erforderlich sind. Sie können den Service verwenden, um Datenbankanmeldeinformationen, API-Schlüssel und andere Secrets während ihres gesamten Lebenszyklus zu rotieren, zu verwalten und abzurufen. Benutzer und Anwendungen rufen Secrets mit einem Aufruf an Secrets Manager ab, wodurch keine Hartcodierung sensibler Informationen

erforderlich ist. Secrets Manager bietet Secret-Rotation mit integrierter Integration für Amazon RDS, Amazon Redshift und Amazon DocumentDB. Außerdem ist der Service auf andere Arten von Secrets erweiterbar, einschließlich API-Schlüsseln und OAuth-Token. Mit Secrets Manager können Sie den Zugriff auf Secrets steuern, indem Sie detaillierte Berechtigungen verwenden und die Rotation von Secrets zentral für Ressourcen in der AWS Cloud, Services von Drittanbietern und On-Premises prüfen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket
- Eine Virtual Private Cloud (VPC)
- Ein DB-Subnetz
- Amazon RDS für SQL Server
- Eine AWS Identity and Access Management (IAM)-Rolle mit Zugriff (Auflisten, Abrufen und Ablegen von Objekten) auf den S3-Bucket im Namen der Amazon RDS-Instance.
- Secrets Manager zum Speichern der RDS-Instance-Anmeldeinformationen.

Architektur

Technologie-Stack

- Amazon RDS für SQL Server
- AWS DMS
- Amazon S3
- AWS Secrets Manager

Zielarchitektur

Das folgende Diagramm zeigt die Architektur zum Importieren von Daten aus der Amazon RDS-Instance in den S3-Bucket mithilfe von AWS DMS.

1. Die AWS DMS-Migrationsaufgabe, die über den Quellendpunkt eine Verbindung zur Amazon RDS-Quell-Instance herstellt
2. Kopieren von Daten aus der Amazon-RDS-Quell-Instance
3. Die AWS DMS-Migrationsaufgabe, die über den Zielendpunkt eine Verbindung zum Ziel-S3-Bucket herstellt
4. Exportieren kopierter Daten in den S3-Bucket im CSV-Format (durch Kommas getrennte Werte)

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.

Andere -Services

- Microsoft SQL Server Management Studio (SSMS) ist ein Tool zur Verwaltung von SQL Server, einschließlich Zugriff, Konfiguration und Verwaltung von SQL Server-Komponenten.

Polen

Konfigurieren der Instance von Amazon RDS für SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Instance von Amazon RDS für SQL Server.	1. Öffnen Sie die AWS-Management konsole, wählen Sie RDS und verwenden Sie die Option Standarderstellung, um eine Amazon RDS-Instance mit der erforderlichen Edition zu erstellen, z. B. SQL Server Express Edition, SQL Server Standard Edition oder SQL Server Enterprise Edition. Wählen Sie für die Version 2016 oder höher aus. 2. Wählen Sie unter Vorlagen die Option Entwicklung/Test aus.	DBA, DevOps Techniker
Richten Sie Anmeldeinformationen für die Instance ein.	1. Geben Sie einen Namen für die Instance ein. 2. Geben Sie einen Benutzernamen und ein Passwort für die Amazon-RDS-Instance an.	DBA, DevOps Techniker
Konfigurieren Sie die Instance-Klasse, den Speicher, die automatische Skalierung und die Verfügbarkeit.	1. Wählen Sie die DB-Instance-Klasse aus der Liste aus: Standard-, speicheroptimierte und Burstable-Klassen. Wählen Sie den DB-Instance-Typ aus, der	DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Rechen-, Netzwerk- und Speicherkapazität zuweist, die für die für diese DB-Instance geplanten Workloads erforderlich sind. Weitere Informationen finden Sie in der AWS-Dokumentation. 2. Wählen Sie den Speichert yp aus der Liste aus: Allzweck-SSD, Bereitges tellte IOPS-SSD oder Magnetfestplatten. Weisen Sie die Standardspeichergr öße nach Bedarf zu. 3. Wählen Sie Automatische Speicherskalierung aktiviere n, um den Amazon-RDS-Speicher basierend auf Ihrer Kapazitätsplanung zu erhöhen. 4. Eine Multi-AZ-Bereitste llung mit einer Replikati ons-Instance wird von AWS DMS unterstützt. Im Falle eines Ausfalls der Availability Zone, der internen Hardware oder des Netzwerks erstellt AWS DMS eine Standby-Instance und stellt durch automatisches Failover für die Standby-Replikate Hochverfügbarkeit (HA)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereit. Wählen Sie je nach Größe Ihres Imports die entsprechende Option aus.	
Geben Sie die VPC, die Subnetzgruppe, den öffentlichen Zugriff und die Sicherheitsgruppe an.	Wählen Sie die VPC , die DB-Subnetzgruppen und die VPC-Sicherheitsgruppe nach Bedarf aus, um die Amazon-RDS-Instance zu erstellen . Folgen Sie den bewährten Methoden, zum Beispiel: • Aktivieren Sie keinen öffentlichen Zugriff auf die RDS-DB-Instance. • Verwenden Sie das CIDR 0.0.0.0/0 nicht in den Sicherheitsgruppen. • Verwenden Sie nur die erforderliche IP-Adresse und Portdetails für den Zugriff auf die RDS-Instance.	DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Überwachung, Sicherung und Wartung.	1. Geben Sie die gewünschten Backup-Optionen an. Standardmäßig sind automatische Backups mit einer Aufbewahrungsdauer von 7 Tagen aktiviert. 2. Wählen Sie die entsprechenden Einstellungen für automatische Nebenversions-Upgrades und Wartungsfenster aus, um die ausstehenden Änderungen oder Wartungsarbeiten von Amazon RDS auf die Datenbank anzuwenden. 3. Wählen Sie Datenbank erstellen aus.	DBA, DevOps Techniker

Einrichten der Datenbank und der Beispieldaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle und laden Sie die Beispieldaten.	Erstellen Sie in der neuen Datenbank eine Tabelle. Verwenden Sie den Beispielcode im Abschnitt Zusätzliche Informationen, um Daten in die Tabelle zu laden.	DBA, DevOps Techniker

Einrichten von Anmeldeinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Geheimnis.	1. Wählen Sie in der Konsole Secrets Manager und dann Neues Secret speichern aus. 2. Geben Sie einen Benutzern amen und ein Passwort für die Datenbank von Amazon RDS für SQL Server ein. Dieses Secret wird für den AWS DMS-Quellendpunkt verwendet.	DBA, DevOps Techniker

Einrichten des Zugriffs zwischen der Datenbank und dem S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den Zugriff auf Amazon RDS.	1. Wählen Sie in der Konsole IAM aus und erstellen Sie eine IAM-Rolle, die einem S3-Bucket Lese-/Schreibzugriff auf Amazon RDS gewährt. 2. Wählen Sie unter Feature die Option S3-Integration aus.	DBA, DevOps Techniker

Erstellen des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Um die Daten aus Amazon RDS für SQL Server zu speichern, wählen Sie in der Konsole S3 und dann Bucket erstellen aus. Stellen Sie sicher, dass der S3-Bucket nicht öffentlich verfügbar ist.	DBA, DevOps Techniker

Einrichten des Zugriffs zwischen AWS DMS und dem S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für AWS DMS, um auf Amazon S3 zuzugreifen.	Erstellen Sie eine IAM-Rolle , mit der AWS DMS Objekte aus dem S3-Bucket auflisten, abrufen und ablegen kann.	DBA, DevOps Techniker

Konfigurieren von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS DMS-Quellendpunkt.	1. Wählen Sie in der -Konsole Database Migration Service und dann Endpunkte aus. Erstellen Sie den Quellendpunkt und aktivieren Sie das Kontrollkästchen RDS-DB-Instance auswählen. 2. Wählen Sie für die Quell-Engine Microsoft SQL Server aus.	DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie unter Zugriff auf die Endpunktdatenbank AWS Secrets Manager aus und geben Sie das Secret und die IAM-Rolle ein, die Sie zuvor erstellt haben, sowie den Datenbank namen. 4. Testen Sie den Quellendp unkt.	
Erstellen Sie den AWS DMS-Zielendpunkt.	Erstellen Sie den Zielendpunkt und wählen Sie Amazon S3 als Ziel-Engine aus. Geben Sie den S3-Bucket-Namen und den Ordnernamen für die IAM-Rolle an, die Sie zuvor erstellt haben.	DBA, DevOps Techniker
Erstellen Sie die AWS DMS-Replikations-Instance.	Erstellen Sie in derselben VPC, demselben Subnetz und derselben Sicherheitsgruppe die AWS DMS-Replikations-Instance. Weitere Informati onen zur Auswahl einer Instance-Klasse finden Sie in der AWS-Dokumentation.	DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Migrationsaufgabe.	Um die Daten von Amazon RDS für SQL Server in den S3-Bucket zu exportieren, erstellen Sie eine Datenbank migrationsaufgabe. Wählen Sie für den Migrationstyp Migrieren vorhandener Daten aus. Wählen Sie die AWS DMS-Endpunkte und die Replikations-Instance aus, die Sie erstellt haben.	DBA, DevOps Techniker

Exportieren der Daten in den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Datenbank migrationsaufgabe aus.	Um die SQL Server-Ta bellendaten zu exportieren, starten Sie die Datenbank migrationsaufgabe. Die Aufgabe exportiert die Daten im CSV-Format aus Amazon RDS für SQL Server in den S3-Bucket.	DBA, DevOps Techniker

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Ressourcen.	Um zusätzliche Kosten zu vermeiden, verwenden Sie die -Konsole, um die Ressourcen	DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der folgenden Reihenfolge zu löschen: 1. Migrationsaufgabe 2. Replikations-Instance 3. Endpunkte 4. S3-Bucket 5. Datenbank-Instance	

Zugehörige Ressourcen

- AWS DMS
- Amazon S3
- Amazon RDS für SQL Server
- Amazon S3-Integration

Zusätzliche Informationen

Verwenden Sie den folgenden Code, um die Datenbank und Tabelle zu erstellen und die Beispieldaten zu laden.

```
--Step1: Database creation in RDS SQL Server
CREATE DATABASE [Test_DB]
 ON  PRIMARY
( NAME = N'Test_DB', FILENAME = N'D:\rdsdbdata\DATA\Test_DB.mdf' , SIZE = 5120KB ,
 FILEGROWTH = 10%)
 LOG ON
( NAME = N'Test_DB_log', FILENAME = N'D:\rdsdbdata\DATA\Test_DB_log.ldf' , SIZE =
 1024KB , FILEGROWTH = 10%)
GO

--Step2: Create Table
USE Test_DB
GO
Create Table Test_Table(ID int, Company Varchar(30), Location Varchar(20))
```

```
--Step3: Load sample data.
USE Test_DB
GO
Insert into Test_Table values(1,'AnyCompany','India')
Insert into Test_Table values(2,'AnyCompany','USA')
Insert into Test_Table values(3,'AnyCompany','UK')
Insert into Test_Table values(4,'AnyCompany','Hyderabad')
Insert into Test_Table values(5,'AnyCompany','Banglore')
```

Behandlung anonymer Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL

Erstellt von Anuradha Chitha (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Database Relational	Ziel: PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle; Open-Source	Technologien: Datenbanken; Migration
AWS-Services: Amazon Aurora; Amazon RDS		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie den Fehler vermeiden, den Sie beim Umgang mit anonymen Blöcken in dynamischen SQL-Anweisungen erhalten. Sie erhalten eine Fehlermeldung, wenn Sie das AWS Schema Conversion Tool verwenden, um eine Oracle-Datenbank in eine Aurora PostgreSQL -kompatible Edition-Datenbank zu konvertieren. Um den Fehler zu vermeiden, müssen Sie den Wert einer 0UT Bind-Variablen kennen, aber Sie können den Wert einer 0UT Bind-Variablen erst kennen, nachdem Sie die SQL-Anweisung ausgeführt haben. Der Fehler ergibt sich daraus, dass das AWS Schema Conversion Tool (AWS SCT) die Logik innerhalb der Dynamic SQL-Anweisung nicht versteht. AWS SCT kann die dynamische SQL-Anweisung nicht in PL/SQL-Code (d. h. Funktionen, Prozeduren und Pakete) konvertieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktives AWS-Konto
- Aurora-PostgreSQL-Datenbank (DB)-Instance
- Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance
- Interaktives PostgreSQL-Terminal (psql)
- SQL *Plus

- `AWS_ORACLE_EXT` -Schema (Teil des AWS SCT-Erweiterungspakets) in Ihrer Zieldatenbank
- Neueste Version von AWS Schema Conversion Tool (AWS SCT) und die erforderlichen Treiber

Architektur

Quelltechnologie-Stack

- Lokale Oracle Database 10g und höhere Version

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL
- Amazon RDS für PostgreSQL
- AWS Schema Conversion Tool (AWS SCT)

Migrationsarchitektur

Das folgende Diagramm zeigt, wie Sie AWS SCT- und Oracle-0UTBindungsvariablen verwenden, um Ihren Anwendungscode nach eingebetteten SQL-Anweisungen zu scannen und den Code in ein kompatibles Format zu konvertieren, das eine Aurora-Datenbank verwenden kann.

Das Diagramm zeigt den folgenden Workflow:

1. Generieren Sie einen AWS SCT-Bericht für die Quelldatenbank, indem Sie Aurora PostgreSQL als Zieldatenbank verwenden.
2. Identifizieren Sie den anonymen Block im Block Dynamischer SQL-Code (für den AWS SCT den Fehler ausgelöst hat).
3. Konvertieren Sie den Codeblock manuell und stellen Sie den Code in einer Zieldatenbank bereit.

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.
- AWS Schema Conversion Tool (AWS SCT) hilft Ihnen dabei, heterogene Datenbankmigrationen vorhersehbar zu machen, indem das Quelldatenbankschema und die meisten Datenbankcodeobjekte automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Andere Tools

- Mit pgAdmin können Sie eine Verbindung zu Ihrem Datenbankserver herstellen und mit ihm interagieren.
- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, mit der Sie Datenbanken in Oracle Database entwickeln und verwalten können. Sie können entweder SQL *Plus oder Oracle SQL Developer für dieses Muster verwenden.

Polen

Konfigurieren der Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Oracle-Instance auf Amazon RDS oder Amazon EC2.	Informationen zum Erstellen einer Oracle-DB-Instance in Amazon RDS finden Sie unter Erstellen einer Oracle-DB-Instance und Herstellen einer Verbindung mit einer Datenbank in einer Oracle-DB-Instance in der Amazon-RDS-Dokumentation. Informationen zum Erstellen einer Oracle-DB-Instance	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in Amazon Elastic Compute Cloud (Amazon EC2) finden Sie unter Amazon EC2 for Oracle in der Dokumentation zu AWS Prescriptive Guidance.	
Erstellen Sie ein Datenbankschema und Objekte für die Migration.	Sie können Amazon Cloud Directory verwenden, um ein Datenbankschema zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Schemas in der Cloud Directory-Dokumentation.	DBA
Konfigurieren Sie ein- und ausgehende Sicherheitsgruppen.	Informationen zum Erstellen und Konfigurieren von Sicherheitsgruppen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen in der Amazon-RDS-Dokumentation.	DBA
Vergewissern Sie sich, dass die Datenbank ausgeführt wird.	Informationen zum Überprüfen des Status Ihrer Datenbank finden Sie unter Anzeigen von Amazon-RDS-Ereignissen in der Amazon-RDS-Dokumentation.	DBA

Konfigurieren der Aurora-PostgreSQL-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora-PostgreSQL-Instance in Amazon RDS.	Informationen zum Erstellen einer Aurora-PostgreSQL-Instance finden Sie unter Erstellen eines DB-Clusters und Herstellen einer Verbindung mit einer Datenbank in einem Aurora-PostgreSQL-DB-Cluster in der Amazon-RDS-Dokumentation.	DBA
Konfigurieren Sie eine Sicherheitsgruppe für ein- und ausgehenden Datenverkehr.	Informationen zum Erstellen und Konfigurieren von Sicherheitsgruppen finden Sie unter Gewähren des Zugriffs auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe in der Aurora-Dokumentation.	DBA
Vergewissern Sie sich, dass die Aurora-PostgreSQL-Datenbank ausgeführt wird.	Informationen zum Überprüfen des Status Ihrer Datenbank finden Sie unter Anzeigen von Amazon-RDS-Ereignissen in der Aurora-Dokumentation.	DBA

Einrichten von AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbinden Sie AWS SCT mit der Quelldatenbank.	Informationen zum Verbinden von AWS SCT mit Ihrer Quelldatenbank finden Sie unter Connecting to	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PostgreSQL as Source in der AWS SCT-Dokumentation.	
Verbinden Sie AWS SCT mit der Zieldatenbank.	Informationen zum Verbinden von AWS SCT mit Ihrer Zieldatenbank finden Sie unter Was ist das AWS Schema Conversion Tool? im AWS Schema Conversion Tool-Benutzerhandbuch.	DBA
Konvertieren Sie das Datenbankschema in AWS SCT und speichern Sie den automatisch konvertierten Code als SQL-Datei.	Informationen zum Speichern konvertierter AWS SCT-Dateien finden Sie unter Speichern und Anwenden Ihres konvertierten Schemas in AWS SCT im AWS Schema Conversion Tool-Benutzerhandbuch.	DBA

Migrieren des Codes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die SQL-Datei für die manuelle Konvertierung ab.	Rufen Sie in der konvertierten AWS SCT-Datei die SQL-Datei ab, die eine manuelle Konvertierung erfordert.	DBA
Aktualisieren Sie das Skript.	Aktualisieren Sie die SQL-Datei manuell.	DBA

Zugehörige Ressourcen

- Amazon RDS

- Funktionen von Amazon Aurora

Zusätzliche Informationen

Der folgende Beispielcode zeigt, wie die Oracle-Quelldatenbank konfiguriert wird:

```
CREATE or replace PROCEDURE calc_stats_new1 (
  a NUMBER,
  b NUMBER,
  result out NUMBER)
IS
BEGIN
result:=a+b;
END;
/
```

```
set serveroutput on ;

DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;
  DBMS_OUTPUT.PUT_LINE('output:'||output);

END;
```

Der folgende Beispielcode zeigt, wie Sie die Aurora-PostgreSQL-Zieldatenbank konfigurieren:

```
 w integer,
 x integer)
RETURNS integer
AS
$BODY$
DECLARE
begin
return w + x ;
end;
```

```
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized
      ('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );

PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;


DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

Verarbeiten überlasteter Oracle-Funktionen in Aurora PostgreSQL – kompatibel

Erstellt von Sumana Yanamandra (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Datenbanken; Migration
AWS-Services: Amazon Aurora		

Übersicht

Der Code, den Sie von einer On-Premises-Oracle-Datenbank zu Amazon Aurora PostgreSQL - kompatible Edition migrieren, kann überlastete Funktionen enthalten. Diese Funktionen haben dieselbe Definition, d. h. denselben Funktionsnamen und dieselbe Anzahl und denselben Datentyp von Eingabeparametern (`IN`), aber der Datentyp oder die Anzahl der Ausgabeparameter (`OUT`) kann abweichen.

Diese Parameterkonflikte können zu Problemen in PostgreSQL führen, da es schwierig ist, zu bestimmen, welche Funktion ausgeführt werden soll. Dieses Muster veranschaulicht, wie Sie überlastete Funktionen behandeln, wenn Sie Ihren Datenbankcode zu Aurora PostgreSQL - kompatibel migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Datenbank-Instance als Quelldatenbank
- Eine mit Aurora PostgreSQL kompatible DB-Instance als Zieldatenbank (siehe Anweisungen in der Aurora-Dokumentation)

Produktversionen

- Oracle Database 9i oder höher
- Oracle SQL Developer Version 18.4.0.376
- pgAdmin 4-Client
- Aurora PostgreSQL – Kompatible Version 11 oder höher (siehe Identifizieren von Versionen von Amazon Aurora PostgreSQL in der Aurora-Dokumentation)

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.

Andere Tools

- Oracle SQL Developer ist eine kostenlose, integrierte Entwicklungsumgebung für die Arbeit mit SQL in Oracle-Datenbanken in herkömmlichen und Cloud-Bereitstellungen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.

Polen

Erstellen einer einfachen Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Funktion in PostgreSQL, die einen Eingabeparameter und einen Ausgabeparameter hat.	Das folgende Beispiel veranschaulicht eine Funktion namens `test_over loading` in Aurora PostgreSQL – kompatibe l. Diese Funktion hat zwei Parameter: einen Eingabete xtparameter und einen Ausgabetextparameter.	Dateningenieur, Aurora PostgreSQL – kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE BEGIN str2 := 'Success'; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Führen Sie die Funktion in PostgreSQL aus.	Führen Sie die -Funktion aus, die Sie im vorherigen Schritt erstellt haben.
	`select public.test_overloading('Test');`
	Es sollte die folgende Ausgabe angezeigt werden.
	`Success`
		Dateningenieur, Aurora PostgreSQL – kompatibel

Überladen der Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie denselben Funktionsnamen, um eine überladene Funktion in PostgreSQL zu erstellen.	Erstellen Sie eine überladene Funktion in Aurora PostgreSQL – kompatibel, die denselben Funktionsnamen wie Ihre vorherige Funktion verwendet. Das folgende Beispiel heißt auch `test_overloading`, hat jedoch drei Parameter: einen Eingabetextparameter, einen Ausgabetextparameter und einen Ausgabeganzzahlparameter. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN`	Dateningenieur, Aurora PostgreSQL – kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`RETURN ;`
	`END;`
	`$BODY$;`	

Führen Sie die Funktion in PostgreSQL aus.	Wenn Sie diese Funktion ausführen, schlägt sie mit der folgenden Fehlermeldung fehl.
	`ERROR: cannot change return type of existing function`
	`HINT: Use DROP FUNCTION test_overloading(text) first.`
	Dies geschieht, weil Aurora PostgreSQL – kompatibel das Überladen von Funktionen nicht direkt unterstützt. Es kann nicht identifizieren, welche Funktion ausgeführt werden soll, da die Anzahl der Ausgabeparameter in der zweiten Version der Funktion unterschiedlich ist, obwohl die Eingabeparameter identisch sind.
		Dateningenieur, Aurora PostgreSQL – kompatibel

Wenden Sie die Problemumgehung an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie INOUT zum ersten Ausgabeparameter hinzu.	Um dieses Problem zu umgehen, ändern Sie den	Dateningenieur, Aurora PostgreSQL – kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktionscode, indem Sie den ersten Ausgabeparameter als darstellen`INOUT`. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, INOUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die überarbeitete Funktion aus.	Führen Sie die Funktion aus, die Sie mit der folgenden Abfrage aktualisiert haben. Sie übergeben einen Nullwert als zweites Argument dieser Funktion, da Sie diesen Parameter als deklariert haben, `INOUT` um den Fehler zu vermeiden.
	`select public.test_overloading('Test', null);`
	Die Funktion wurde jetzt erfolgreich erstellt.
	`Success, 100`
		Dateningenieur, Aurora PostgreSQL – kompatibel

Validieren Sie die Abfrageergebnisse.	Stellen Sie sicher, dass der Code mit der überladenen Funktion erfolgreich konvertiert wurde.	Dateningenieur, Aurora PostgreSQL – kompatibel

Zugehörige Ressourcen

- Arbeiten mit Amazon Aurora PostgreSQL (Aurora-Dokumentation)
- Funktionsüberladung in Oracle (Oracle-Dokumentation)
- Funktionsüberladung in PostgreSQL (PostgreSQL-Dokumentation)

Helfen Sie mit, DynamoDB-Tagging durchzusetzen

Erstellt von Mansi Suratwala (AWS)

Umgebung: Produktion	Technologien: Datenbanken; Cloud-nativ; Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon CloudWatch; Amazon DynamoDB; AWS Lambda; Amazon SNS		

Übersicht

Dieses Muster richtet automatische Benachrichtigungen ein, wenn ein vordefiniertes Amazon DynamoDB-Tag fehlt oder aus einer DynamoDB-Ressource in der Amazon Web Services (AWS) -Cloud entfernt wird.

DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankdienst, der schnelle und vorhersehbare Leistung mit Skalierbarkeit bietet. Mit DynamoDB können Sie den administrativen Aufwand für den Betrieb und die Skalierung einer verteilten Datenbank verringern. Wenn Sie DynamoDB verwenden, müssen Sie sich keine Gedanken über Hardwarebereitstellung, Einrichtung und Konfiguration, Replikation, Software-Patches oder Clusterskalierung machen.

Das Muster verwendet eine CloudFormation AWS-Vorlage, die ein Amazon CloudWatch Events-Ereignis und eine AWS-Lambda-Funktion erstellt. Das Ereignis sucht mithilfe von AWS nach neuen oder vorhandenen DynamoDB-Tagging-Informationen. CloudTrail Wenn ein vordefiniertes Tag fehlt oder entfernt wird, wird eine Lambda-Funktion CloudWatch ausgelöst, die Ihnen eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung sendet, die Sie über den Verstoß informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Ein Amazon Simple Storage Service (Amazon S3) -Bucket für die Lambda-.zip-Datei, die das Python-Skript für die Ausführung der Lambda-Funktion enthält

Einschränkungen

- Die Lösung funktioniert nur, wenn die Ereignisse `TagResource` oder `UntagResource` CloudTrail eintreten. Es werden keine Benachrichtigungen für andere Ereignisse erstellt.

Architektur

Zieltechnologie-Stack

- Amazon-DynamoDB
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage in jeder Region oder jedem Konto nur einmal ausführen.

Tools

Tools

- Amazon DynamoDB — DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit Skalierbarkeit bietet.
- AWS CloudTrail — CloudTrail ist ein AWS-Service, der Sie bei der Steuerung, Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos unterstützt. Aktionen,

die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.

- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne dass Server bereitgestellt oder verwaltet werden müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Dieser S3-Bucket hostet die Lambda-Code-.zip-Datei. Ihr S3-Bucket muss sich in derselben AWS-Region befinden wie die DynamoDB-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ressource, die überwacht wird.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie die DynamoDB-Ressource, die überwacht wird.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie auf der CloudFormation AWS-Konsole die CloudFormation AWS-Vorlage bereit, die im Abschnitt Anlagen bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Parameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben.	Cloud-Architekt
Geben Sie den Amazon S3 S3-Schlüssel ein.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<folder>/<file-name>.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt
Geben Sie die erforderlichen DynamoDB-Tagschlüssel ein.	Achten Sie darauf, dass die Tags durch Kommas getrennt sind und keine	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Leerzeichen dazwischen stehen (z. B.). `ApplicationId,CreatedBy,Environment,Organization` Das Ereignis CloudWatch Ereignisse sucht nach diesen Tags und sendet eine Benachrichtigung, wenn sie nicht gefunden werden.	

Bestätigen Sie das Abonnement.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen über Verstöße zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Dateien in einen S3-Bucket hochladen
- Taggen von Ressourcen in DynamoDB
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Implementieren Sie regionsübergreifende Notfallwiederherstellung mit AWS DMS und Amazon Aurora

Erstellt von Mark Hudson (AWS)

Umgebung: Produktion	Technologien: Datenbanken	AWS-Dienste: AWS DMS; Amazon RDS; Amazon Aurora

Übersicht

Naturkatastrophen oder vom Menschen verursachte Katastrophen können jederzeit eintreten und sich auf die Verfügbarkeit von Services und Workloads auswirken, die in einer bestimmten Amazon Web Services (AWS) -Region ausgeführt werden. Um die Risiken zu minimieren, müssen Sie einen Notfallwiederherstellungsplan (DR) entwickeln, der die integrierten regionsübergreifenden Funktionen der AWS-Services beinhaltet. Für AWS-Services, die von Natur aus keine regionsübergreifende Funktionalität bieten, muss der DR-Plan auch eine Lösung für deren Failover in allen AWS-Regionen bieten.

Dieses Muster führt Sie durch ein Disaster Recovery-Setup mit zwei Amazon Aurora MySQL-Compatible Edition-Datenbankclustern in einer einzigen Region. Um die DR-Anforderungen zu erfüllen, sind die Datenbankcluster so konfiguriert, dass sie die globale Datenbankfunktion von Amazon Aurora verwenden, wobei sich eine einzige Datenbank über mehrere AWS-Regionen erstreckt. Eine AWS Database Migration Service (AWS DMS) -Aufgabe repliziert Daten zwischen den Clustern in der lokalen Region. AWS DMS unterstützt derzeit jedoch kein Task-Failover zwischen Regionen. Dieses Muster umfasst die Schritte, die erforderlich sind, um diese Einschränkung zu umgehen und AWS DMS in beiden Regionen unabhängig zu konfigurieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ausgewählte primäre und sekundäre AWS-Regionen, die globale Amazon Aurora Aurora-Datenbanken unterstützen.
- Zwei unabhängige Amazon Aurora MySQL-Compatible Edition-Datenbankcluster in einem einzigen Konto in der primären Region.
- Datenbank-Instance-Klasse db.r5 oder höher (empfohlen).

- Eine AWS-DMS-Aufgabe in der primären Region, die eine fortlaufende Replikation zwischen den vorhandenen Datenbankclustern durchführt.
- Ressourcen der DR-Region sind vorhanden, um die Anforderungen für die Erstellung von Datenbank-Instances zu erfüllen. Weitere Informationen finden Sie unter Arbeiten mit einer DB-Instance in einer VPC.

Einschränkungen

- Eine vollständige Liste der globalen Amazon Aurora Aurora-Datenbankbeschränkungen finden Sie unter Einschränkungen der globalen Amazon Aurora Aurora-Datenbanken.

Produktversionen

- Amazon Aurora MySQL-kompatible Edition 5.7 oder 8.0. Weitere Informationen finden Sie unter Amazon Aurora Aurora-Versionen.

Architektur

Zieltechnologie-Stack

- Globaler Datenbankcluster Amazon Aurora MySQL-Compatible Edition
- AWS DMS

Zielarchitektur

Das folgende Diagramm zeigt eine globale Datenbank für zwei AWS-Regionen, eine mit den primären Haupt- und Reporterdatenbanken und der AWS-DMS-Replikation und eine mit den sekundären Haupt- und Reporterdatenbanken.

Automatisierung und Skalierung

Sie können AWS verwenden CloudFormation , um die erforderliche Infrastruktur in der sekundären Region zu erstellen, z. B. die Virtual Private Cloud (VPC), Subnetze und Parametergruppen. Sie können AWS auch verwenden CloudFormation , um die sekundären Cluster in der DR-Region zu erstellen und sie der globalen Datenbank hinzuzufügen. Wenn Sie CloudFormation Vorlagen verwendet haben, um die Datenbankcluster in der primären Region zu erstellen, können Sie diese

aktualisieren oder mit einer zusätzlichen Vorlage erweitern, um die globale Datenbankressource zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora Aurora-DB-Clusters mit zwei DB-Instances und Erstellen eines globalen Datenbank-Clusters für Aurora MySQL.

Schließlich können Sie die AWS-DMS-Aufgaben in den primären und sekundären Regionen mithilfe von Ereignissen CloudFormation nach dem Auftreten von Failover- und Failback-Ereignissen erstellen. Weitere Informationen finden Sie unter. AWS::DMS::ReplicationTask

Tools

- Amazon Aurora — Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die mit MySQL und PostgreSQL kompatibel ist. Dieses Muster verwendet Amazon Aurora MySQL-Compatible Edition.
- Globale Amazon Aurora-Datenbanken — Die globalen Datenbanken von Amazon Aurora sind für global verteilte Anwendungen konzipiert. Eine einzelne globale Amazon Aurora Aurora-Datenbank kann sich über mehrere AWS-Regionen erstrecken. Sie repliziert Ihre Daten ohne Auswirkungen auf die Datenbankleistung. Es ermöglicht auch schnelle lokale Lesevorgänge mit geringer Latenz in jeder Region und ermöglicht die Notfallwiederherstellung nach regionsweiten Ausfällen.
- AWS DMS — Der AWS Database Migration Service (AWS DMS) ermöglicht eine einmalige Migration oder eine fortlaufende Replikation. Eine fortlaufende Replikationsaufgabe sorgt dafür, dass Ihre Quell- und Zieldatenbanken synchron bleiben. Nach der Einrichtung wendet die laufende Replikationsaufgabe kontinuierlich Quelländerungen mit minimaler Latenz auf das Ziel an. Alle Funktionen von AWS DMS, wie Datenvalidierung und Transformationen, sind für jede Replikationsaufgabe verfügbar.

Epen

Bereiten Sie die vorhandenen Datenbankcluster in der primären Region vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Parameter gruppe des Datenbank-Clusters.	Aktivieren Sie in der vorhandenen Parameter gruppe des Datenbank-Clusters die binäre Protokoll ierung auf Zeilenebene, indem Sie den **`binlog_format`**	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Parameter auf den Wert row setzen. AWS DMS erfordert binäre Protokollierung auf Zeilenebene für MySQL-kompatible Datenbanken, wenn laufende Replikationen oder Change Data Capture (CDC) durchgeführt werden. Weitere Informationen finden Sie unter Verwenden einer von AWS verwalteten MySQL-kompatiblen Datenbank als Quelle für AWS DMS.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie den Aufbewahrungszeitraum für das Binärprotokoll der Datenbank.	Führen Sie mithilfe eines auf Ihrem Endbenutzergerät installierten MySQL-Clients oder einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance die folgende von Amazon Relational Database Service (Amazon RDS) bereitgestellte gespeicherte Prozedur auf dem Writer-Node des Haupt-Datenbank-Clusters aus, wobei die Anzahl der Stunden für die Aufbewahrung der Protokolle angegeben XX ist.
	`call mysql.rds_set_configuration('binlog retention hours', XX)`
	Bestätigen Sie die Einstellung, indem Sie den folgenden Befehl ausführen.
	`call mysql.rds_show_configuration;`
	MySQL-kompatible Datenbanken, die von AWS verwaltet werden, löschen die Binärprotokolle so schnell wie möglich. Daher muss der Aufbewahrungszeitraum lang genug sein, um sicherzustellen, dass die Protokolle nicht gelöscht
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden, bevor die AWS DMS-Aufgabe ausgeführt wird. Ein Wert von 24 Stunden ist normalerweise ausreichend, der Wert sollte jedoch auf der Zeit basieren, die für die Einrichtung der AWS DMS-Aufgabe in der DR-Region erforderlich ist.	

Aktualisieren Sie die bestehende AWS DMS-Aufgabe in der primären Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Notieren Sie den ARN der AWS-DMS-Aufgabe.	Verwenden Sie den Amazon Resource Name (ARN), um den AWS DMS-Aufga bennamen für die spätere Verwendung abzurufen. Um den ARN der AWS-DMS-A ufgabe abzurufen, zeigen Sie die Aufgabe in der Konsole an oder führen Sie den folgenden Befehl aus.
	`aws dms describe-replication-tasks`
	Ein ARN sieht wie folgt aus.
	`arn:aws:dms:us-east-1:<accountid>:task:AN6HFFMPM246XOZVEUHCNSOVF7MQCLTOZUIRAMY`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Zeichen nach dem letzten Doppelpunkt entsprechen dem Aufgabennamen, der in einem späteren Schritt verwendet wird.	
Ändern Sie die bestehende AWS DMS-Aufgabe, um den Checkpoint aufzuzeichnen.	AWS DMS erstellt Prüfpunkte, die Informationen enthalten, sodass die Replikationsengine den Wiederherstellungspunkt für den Change-Stream kennt. Um Checkpoint-Informationen aufzuzeichnen, führen Sie die folgenden Schritte in der Konsole aus: 1. Beenden Sie die AWS DMS-Aufgabe. 2. Verwenden Sie den JSON-Editor in der Aufgabe, um den TaskRecoveryTableEnabled Parameter auf true zu setzen. 3. Starten Sie die AWS DMS-Aufgabe.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Checkpoint-Informationen.	Verwenden Sie einen MySQL-Client, der mit dem Writer-Endpunkt für den Cluster verbunden ist, und fragen Sie die neue Metadatentabelle im Reporter-Datenbank-Cluster ab, um zu überprüfen, ob sie existiert und die Informationen zum Replikationsstatus enthält. Führen Sie den folgenden Befehl aus. `select * from awsdms_control.awsdms_txn_state;` Der Aufgabenname aus dem ARN sollte in dieser Tabelle in der `Task_Name` Spalte zu finden sein.	DBA

Erweitern Sie beide Amazon Aurora Aurora-Cluster auf eine DR-Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schaffen Sie eine Basisinfrastruktur in der DR-Region.	Erstellen Sie die Basiskomponenten, die für die Erstellung von und den Zugriff auf die Amazon Aurora Aurora-Cluster erforderlich sind: • Virtual Private Cloud (VPC) • Subnetze • Sicherheitsgruppe	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Listen zur Kontrolle des Netzwerkzugriffs • Subnetzgruppe • DB-Parametergruppe • DB-Cluster-Paramet ergruppe Stellen Sie sicher, dass die Konfiguration beider Parametergruppen mit der Konfiguration in der primären Region übereinstimmt.	
Fügen Sie die DR-Region zu beiden Amazon Aurora Aurora-Clustern hinzu.	Fügen Sie eine sekundäre Region (die DR-Region) zu den Haupt- und Reporter-Clustern von Amazon Aurora hinzu. Weitere Informationen finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon Aurora Aurora-Datenbank.	AWS-Administrator

Failover durchführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die AWS DMS-Aufgabe.	Die AWS-DMS-Aufgabe in der primären Region funktioni ert nach einem Failover nicht ordnungsgemäß und sollte gestoppt werden, um Fehler zu vermeiden.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie ein verwaltetes Failover durch.	Führen Sie einen verwaltet en Failover des Hauptdate nbankclusters zur DR-Region durch. Anweisungen finden Sie unter Durchführen von verwalteten geplanten Failovers für globale Amazon Aurora Aurora-Datenbanken . Nachdem das Failover auf dem Haupt-Datenbank-Cluster abgeschlossen ist, führen Sie dieselbe Aktivität auf dem Reporter-Datenbank-Cluster durch.	AWS-Administrator, DBA
Daten in die Hauptdatenbank laden.	Fügen Sie Testdaten in den Writer-Knoten der Hauptdate nbank im DR-Datenbankcluste r ein. Diese Daten werden verwendet, um zu überprüfen, ob die Replikation ordnungsg emäß funktioniert.	DBA
Erstellen Sie die AWS DMS-Replikationsinstanz.	Informationen zum Erstellen der AWS DMS-Replikationsin stanz in der DR-Region finden Sie unter Erstellen einer Replikationsinstanz.	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Quell- und Zielendpunkte.	Informationen zum Erstellen der AWS DMS-Quell- und Zielendpunkte in der DR-Region finden Sie unter Quell- und Zielendpunkte erstellen. Die Quelle sollte auf die Writer-Instance des Haupt-Datenbank-Clusters verweisen. Das Ziel sollte auf die Writer-Instanz des Reporter-Datenbank-Clusters verweisen.	AWS-Administrator, DBA
Besorgen Sie sich den Replikationsprüfpunkt.	Um den Replikationsprüfpunkt zu erhalten, verwenden Sie einen MySQL-Client, um die Metadatentabelle abzufragen, indem Sie Folgendes für den Writer-Knoten im Reporter-Datenbank-Cluster in der DR-Region ausführen. `select * from awsdms_control.awsdms_txn_state;` Suchen Sie in der Tabelle nach dem Wert task_name, der dem ARN der AWS-DMS-Aufgabe entspricht, der in der primären Region existiert und den Sie im zweiten Epic abgerufen haben.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe.	Erstellen Sie mit der Konsole eine AWS DMS-Aufgabe in der DR-Region. Geben Sie in der Aufgabe die Migration smethode Nur Datenände rungen replizieren an. Weitere Informationen finden Sie unter Aufgabe erstellen. 1. Verwenden Sie den Assistenten, um in den Aufgabeneinstellungen Folgendes anzugeben: • CDC-Startmodus für Quelltransaktionen — Aktivieren Sie den benutzerdefinierten CDC-Startmodus • Benutzerdefinierter CDC-Startpunkt für Quelltran saktionen — Geben Sie einen Wiederherstellungs prüfpunkt an 2. Geben Sie in das Feld Wiederherstellungs-Checkpoint den Wert für den Replikationsprüfpunkt ein, der zuvor durch die Datenbankabfrage in der Tabelle abgerufen wurde. `awsdms_txn_state` 3. Wählen Sie im Bereich mit den Aufgabeneinstellungen den JSON-Editor aus und	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	setzen Sie den TaskRecov eryTableEnabledParameter auf true. Stellen Sie die Einstellu ng AWS DMS-Aufgabe Migrationsaufgabe starten auf Automatisch bei Erstellung ein.	
Notieren Sie den ARN der AWS-DMS-Aufgabe.	Verwenden Sie den ARN, um den AWS DMS-Aufga bennamen für die spätere Verwendung abzurufen. Führen Sie den folgenden Befehl aus, um den ARN für die AWS-DMS-Aufgabe abzurufen. `aws dms describe-replication-tasks`	AWS-Administrator, DBA
Validieren Sie die replizierten Daten.	Fragen Sie den Reporter-Datenbankcluster in der DR-Region ab, um zu bestätige n, dass die Testdaten, die Sie in den Haupt-Datenbank-Cl uster geladen haben, repliziert wurden.	DBA

Führen Sie ein Failback durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die AWS DMS-Aufgabe.	Die AWS-DMS-Aufgabe in der DR-Region funktioniert nach einem Failback nicht ordnungsgemäß und sollte gestoppt werden, um Fehler zu vermeiden.	AWS-Administrator
Führen Sie ein verwaltetes Failback durch.	Führen Sie ein Failback des Haupt-Datenbank-Clusters auf die primäre Region durch. Anweisungen finden Sie unter Durchführen von verwalteten geplanten Failovers für globale Amazon Aurora Aurora-Datenbanken. Nachdem das Failback auf dem Haupt-Datenbank-Cluster abgeschlossen ist, führen Sie dieselbe Aktivität auf dem Reporter-Datenbank-Cluster durch.	AWS-Administrator, DBA
Besorgen Sie sich den Replikationsprüfpunkt.	Um den Replikationsprüfpunkt zu erhalten, verwenden Sie einen MySQL-Client, um die Metadatentabelle abzufragen, indem Sie Folgendes für den Writer-Knoten im Reporter-Datenbank-Cluster in der DR-Region ausführen. `select * from awsdms_control.awsdms_txn_state;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Suchen Sie in der Tabelle nach dem `task_name` Wert, der dem ARN der AWS-DMS-Aufgabe entspricht, der in der DR-Region existiert und den Sie im vierten Epic erhalten haben.	
Aktualisieren Sie die AWS DMS-Quell- und Zielendpunkte.	Nachdem die Datenbank cluster ausgefallen sind, überprüfen Sie die Cluster in der primären Region, um festzustellen, welche Knoten die Writer-Instances sind. Stellen Sie anschließend sicher, dass die vorhandenen AWS-DMS-Quell- und Zielendpunkte in der primären Region auf die Writer-Instances verweisen. Falls nicht, aktualisieren Sie die Endpunkte mit den DNS-Namen (Domain Name System) der Writer-Instance.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe.	Erstellen Sie mit der Konsole eine AWS DMS-Aufgabe in der primären Region. Geben Sie in der Aufgabe die Migrationsmethode Nur Datenänderungen replizieren an. Weitere Informationen finden Sie unter Aufgabe erstellen. 1. Verwenden Sie in den Aufgabeneinstellungen den Assistenten und geben Sie Folgendes an: • CDC-Startmodus für Quelltransaktionen — Aktivieren Sie den benutzerdefinierten CDC-Startmodus • Benutzerdefinierter CDC-Startpunkt für Quelltransaktionen — Geben Sie einen Wiederherstellungsprüfpunkt an 2. Geben Sie in das Feld Wiederherstellungs-Checkpoint den Wert für den Replikationsprüfpunkt ein, der zuvor durch die Datenbankabfrage in der Tabelle abgerufen wurde. `awsdms_txn_state` 3. Wählen Sie ebenfalls im Bereich mit den Aufgabene	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	instellungen den JSON-Editor aus und setzen Sie den TaskRecoveryTableEnabledParameter auf true. 4. Stellen Sie abschließend die Einstellung AWS DMS-Aufgabe Migrationsaufgabe starten auf Automatisch bei Erstellung ein.	
Notieren Sie die AWS-DMS-Aufgabe Amazon Resource Name (ARN).	Verwenden Sie den ARN, um den AWS DMS-Aufga bennamen für die spätere Verwendung abzurufen. Führen Sie den folgenden Befehl aus, um den ARN für die AWS-DMS-Aufgabe abzurufen: `aws dms describe-replication-tasks` Der Aufgabenname wird bei der Durchführung eines weiteren verwalteten Failovers oder während eines DR-Szenarios benötigt.	AWS-Administrator, DBA
Löschen Sie AWS DMS-Aufgaben.	Löschen Sie die ursprüngliche (derzeit angehaltene) AWS DMS-Aufgabe in der primären Region und die bestehende AWS DMS-Aufgabe (derzeit gestoppt) in der sekundären Region.	AWS-Administrator

Zugehörige Ressourcen

- Konfiguration Ihres Amazon Aurora Aurora-DB-Clusters
- Verwendung globaler Amazon Aurora Aurora-Datenbanken
- Arbeiten mit Amazon Aurora MySQL
- Arbeiten mit einer AWS DMS-Replikationsinstanz
- Arbeiten mit AWS DMS-Endpunkten
- Arbeiten mit AWS DMS-Aufgaben
- Was ist AWS CloudFormation?

Zusätzliche Informationen

Die globalen Datenbanken von Amazon Aurora werden in diesem Beispiel für DR verwendet, da sie ein effektives Recovery Time Objective (RTO) von 1 Sekunde und ein Recovery Point Objective (RPO) von weniger als 1 Minute bieten. Beides ist niedriger als bei herkömmlichen replizierten Lösungen und ideal für DR-Szenarien.

Die globalen Datenbanken von Amazon Aurora bieten viele weitere Vorteile, darunter die folgenden:

- Globale Lesevorgänge mit lokaler Latenz — Verbraucher auf der ganzen Welt können mit lokaler Latenz auf Informationen in einer lokalen Region zugreifen.
- Skalierbare sekundäre Amazon Aurora Aurora-DB-Cluster — Sekundäre Cluster können unabhängig voneinander skaliert werden, sodass bis zu 16 schreibgeschützte Replikate hinzugefügt werden können.
- Schnelle Replikation vom primären zum sekundären Amazon Aurora Aurora-DB-Cluster — Die Replikation hat nur geringe Auswirkungen auf die Leistung des primären Clusters. Sie erfolgt auf der Speicherebene mit typischen regionsübergreifenden Replikationslatenzen von weniger als 1 Sekunde.

Dieses Muster verwendet auch AWS DMS für die Replikation. Amazon Aurora Aurora-Datenbanken bieten die Möglichkeit, Read Replicas zu erstellen, was den Replikationsprozess und die DR-Einrichtung vereinfachen kann. AWS DMS wird jedoch häufig zur Replikation verwendet, wenn Datentransformationen erforderlich sind oder wenn die Zieldatenbank zusätzliche Indizes benötigt, über die die Quelldatenbank nicht verfügt.

Migrieren von Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten zu PostgreSQL

Erstellt von Sivas Potlachervoo (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: PostgreSQL
R-Typ: Plattformwechsel	Workload: Open-Source; Oracle	Technologien: Datenbanken; Migration
AWS-Services: Amazon RDS; Amazon Aurora		

Übersicht

Dieses Muster zeigt, wie Oracle-Database-Funktionen und -Prozeduren mit mehr als 100 Argumenten zu PostgreSQL migriert werden. Sie können dieses Muster beispielsweise verwenden, um Oracle-Funktionen und -Prozeduren zu einem der folgenden mit PostgreSQL kompatiblen AWS-Datenbankservices zu migrieren:

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

PostgreSQL unterstützt keine Funktionen oder Prozeduren mit mehr als 100 Argumenten. Um dieses Problem zu umgehen, können Sie einen neuen Datentyp definieren, der Typfelder enthält, die den Argumenten der Quellfunktion entsprechen. Anschließend können Sie eine PL/pgSQL-Funktion erstellen und ausführen, die den benutzerdefinierten Datentyp als Argument verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon-RDS-Oracle-Datenbank-Instance (DB)

- Eine DB-Instance von Amazon RDS für PostgreSQL oder eine mit Aurora PostgreSQL kompatible DB-Instance

Produktversionen

- Amazon RDS Oracle DB-Instance-Versionen 10.2 und höher
- Amazon RDS PostgreSQL DB-Instance-Versionen 9.4 und höher oder Aurora PostgreSQL -kompatible DB-Instance-Versionen 9.4 und höher
- Oracle SQL Developer Version 18 und höher
- pgAdmin Version 4 und höher

Architektur

Quelltechnologie-Stack

- Amazon RDS Oracle DB-Instance-Versionen 10.2 und höher

Zieltechnologie-Stack

- Amazon RDS PostgreSQL DB-Instance-Versionen 9.4 und höher oder Aurora PostgreSQL -kompatible DB-Instance-Versionen 9.4 und höher

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.

Andere -Services

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.

Bewährte Methoden

Stellen Sie sicher, dass der von Ihnen erstellte Datentyp mit den Typfeldern übereinstimmt, die in der Oracle-Quellfunktion oder -Prozedur enthalten sind.

Polen

Ausführen einer Oracle-Funktion oder -Prozedur mit mehr als 100 Argumenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen oder identifizieren Sie eine vorhandene Oracle/PLSQL-Funktion oder -Prozedur mit mehr als 100 Argumenten.	Erstellen Sie eine Oracle/PLSQL-Funktion oder -Prozedur mit mehr als 100 Argumenten. –oder– Identifizieren Sie eine vorhandene Oracle/PLSQL-Funktion oder -Prozedur mit mehr als 100 Argumenten. Weitere Informationen finden Sie in den Abschnitten 14.7 CREATE FUNCTION Statement und 14.11 CREATE PROCEDURE Statement in der Oracle Database-Dokumentation.	Oracle/PLSQL-Kenntnisse
Kompilieren Sie die Oracle/PLSQL-Funktion oder -Prozedur.	Kompilieren Sie die Oracle/PLSQL-Funktion oder -Prozedur.	Oracle/PLSQL-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Kompilieren einer Funktion in der Oracle Database-Dokumentation.	
Führen Sie die Oracle/PLSQL-Funktion aus.	Führen Sie die Oracle/PL SQL-Funktion oder -Prozedur aus. Speichern Sie dann die Ausgabe.	Oracle/PLSQL-Kenntnisse

Definieren Sie einen neuen Datentyp, der den Argumenten der Quellfunktion oder der Prozedur entspricht

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie einen neuen Datentyp in PostgreSQL .	Definieren Sie einen neuen Datentyp in PostgreSQL, der alle Felder enthält, die in den Argumenten der Oracle-Qu ellfunktion oder Prozedur erscheinen. Weitere Informationen finden Sie unter CREATE TYPE in der PostgreSQL-Dokumen tation.	PostgreSQL-PL/pgSQL-Wissen

Erstellen einer PostgreSQL-Funktion, die das neue TYPE-Argument enthält

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine PostgreSQ L-Funktion, die den neuen Datentyp enthält.	Erstellen Sie eine PostgreSQ LTYPE-Funktion, die das neue Argument enthält.	PostgreSQL-PL/pgSQL-Wissen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Eine Beispielfunktion finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	
Kompilieren Sie die PostgreSQL-Funktion.	Kompilieren Sie die Funktion in PostgreSQL . Wenn die neuen Datentypfelder mit den Argumenten der Quellfunktion oder der Prozedur übereinst immen, wird die Funktion erfolgreich kompiliert.	PostgreSQL-PL/pgSQL-Wissen
Führen Sie die PostgreSQL-Funktion aus.	Führen Sie die PostgreSQL-Funktion aus.	PostgreSQL-PL/pgSQL-Wissen

Fehlerbehebung

Problem	Lösung
Die Funktion gibt den folgenden Fehler zurück: FEHLER: Syntaxfehler nahe „<statement>“	Stellen Sie sicher, dass alle Anweisungen der Funktion mit einem Semikolon () enden`;`.
Die Funktion gibt den folgenden Fehler zurück: FEHLER: „<variable>“ ist keine bekannte Variable	Stellen Sie sicher, dass die Variable, die im Funktionstext verwendet wird, im `DECLARE` Abschnitt der Funktion aufgeführt ist.

Zugehörige Ressourcen

- Arbeiten mit Amazon Aurora PostgreSQL (Amazon Aurora-Benutzerhandbuch für Aurora)
- CREATE TYPE (PostgreSQL-Dokumentation)

Zusätzliche Informationen

Beispiel für eine PostgreSQL-Funktion, die ein TYPE-Argument enthält

```
CREATE OR REPLACE FUNCTION test_proc_new
(
    IN p_rec type_test_proc_args
)
RETURNS void
AS
$BODY$
BEGIN

    /*
    **************
    The body would contain code to process the input values.
    For our testing, we will display couple of values.
    ***************
    */
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_acct_id: ', p_rec.p_acct_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_id: ', p_rec.p_ord_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_date: ', p_rec.p_ord_date);

END;
$BODY$
LANGUAGE plpgsql
COST 100;
```

Migrieren von DB-Instances von Amazon RDS für Oracle zu anderen Konten, die AMS verwenden

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for Oracle in AWS Managed Services
R-Typ: Hostwechsel	Workload: Oracle	Technologien: Datenbanken; Migration; Speicher und Backup
AWS-Services: Amazon RDS; AWS Managed Services		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Amazon Relational Database Service (Amazon RDS) for Oracle-DB-Instance von einem AWS-Konto zu einem anderen AWS-Konto migrieren. Das Muster gilt für Szenarien, in denen das AWS-Quellkonto AWS Managed Services (AMS) nicht verwendet, das Zielkonto jedoch AMS. Sie können die Migration abschließen, indem Sie eine RFC-Anforderung (Request for Change) in AMS verwenden, anstatt die AWS-Managementkonsole zur Durchführung von Datenbankoperationen zu verwenden. Dieser Ansatz bietet minimale Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen. Die Ausfallzeit für eine Datenbank mit 400–900 GB könnte beispielsweise etwa zwei oder drei Stunden dauern. Die Zeit für die Datenbankmigration ist direkt proportional zur Größe der DB-Instance von Amazon RDS für Oracle.

Wichtig: Für dieses Muster müssen Sie einen Datenbank-Snapshot der DB-Instance von Amazon RDS für Oracle in einem Quellkonto erstellen, den Snapshot in ein Zielkonto kopieren, das AMS verwendet, und dann eine neue DB-Instance aus diesem Snapshot erstellen, indem Sie RFCs auslösen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto für das Quellkonto
- Ein aktives AWS-Konto, das AMS für das Zielkonto verwendet
- DB-Instance von Amazon RDS für Oracle, hochfahren und ausführen

Einschränkungen

- Die gleichen Eigenschaften oder Konfigurationen für die DB-Instances im Quellkonto werden in eine neue Ziel-DB-Instance in AMS kopiert.
- Die RFC-Methode, die bei diesem Migrationsansatz verwendet wird, verfügt über begrenzte Funktionen zur Unterstützung von Amazon RDS für Oracle. Sie können auf alle Funktionen von Amazon RDS für Oracle zugreifen, indem Sie eine AWS- CloudFormation Vorlage verwenden, um die Datenbankmigration durchzuführen.
- Es kann mehrere Stunden lang zu einem Anwendungsausfall kommen, da die Migration bei geplanten Ausfallzeiten abgeschlossen werden muss. Während der Ausfallzeit halten Sie die DB-Instance im Quellkonto an und starten dann eine neue DB-Instance im Zielkonto.
- Dieser Migrationsansatz gilt nicht für die Migration einer DB-Instance von einer AWS-Region in eine andere Region innerhalb desselben AWS-Kontos.

Produktversionen

- Oracle Database Standard Edition 2 (SE2) 12.1.0.2.v2-Instance und höher auf Amazon RDS für Oracle
- Amazon RDS für Oracle 11g wird nicht mehr unterstützt (weitere Informationen finden Sie unter Amazon RDS für Oracle in der Amazon-RDS-Dokumentation.)

Architektur

Quelltechnologie-Stack

- Oracle Database SE2 12.1.0.2.v2-Instance auf Amazon RDS für Oracle
- Amazon RDS-Subnetzgruppe
- Amazon RDS-Optionsgruppe (falls erforderlich)
- Amazon-RDS-Parametergruppe (falls erforderlich)
- Amazon Virtual Private Cloud (Amazon VPC)-Sicherheitsgruppe

- AWS Key Management Service (AWS KMS) mit von AWS verwalteten Schlüsseln oder vom Kunden verwalteten Schlüsseln
- AWS Identity and Access Management (IAM)-Rolle (falls erforderlich)

Zieltechnologie-Stack

- Oracle Database SE2 12.1.0.2.v2-Instance auf Amazon RDS für Oracle
- Amazon RDS-Subnetzgruppe
- Amazon RDS-Optionsgruppe (falls erforderlich)
- Amazon-RDS-Parametergruppe (falls erforderlich)
- Amazon-VPC-Sicherheitsgruppe
- AWS Managed Services (AMS)
- AWS KMS mit von AWS verwalteten Schlüsseln und vom Kunden verwalteten Schlüsseln
- IAM-Rolle (falls erforderlich)

Quell- und Zielmigrationsarchitektur

Das folgende Diagramm zeigt die Migration einer DB-Instance von Amazon RDS für Oracle in einem AWS-Konto zu einer DB-Instance von Amazon RDS für Oracle in einem anderen AWS-Konto, das AMS verwendet.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen Sie einen Datenbank-Snapshot der DB-Instance von Amazon RDS für Oracle im Quellkonto.
2. Kopieren Sie den Snapshot in AMS im Zielkonto.
3. Erstellen Sie eine neue DB-Instance von Amazon RDS für Oracle aus dem Snapshot im Zielkonto.

Automatisierung und Skalierung

Sie können die Migration automatisieren und skalieren, indem Sie - CloudFormation Vorlagen verwenden und RFCs in AMS erstellen. CloudFormation Mit können Sie alle Funktionen von Amazon RDS für Oracle verwenden, einschließlich der Möglichkeit, die DB-Instance zu konfigurieren und

wiederherzustellen, wenn Sie eine DB-Instance von Amazon RDS für Oracle aus einem Snapshot erstellen.

Tools

- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Managed Services (AMS) hilft Ihnen, Ihre AWS-Infrastruktur effizienter und sicherer zu betreiben.

Polen

Vorbereiten des Cutover auf dem Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen benutzerdefinierten AWS KMS-Schlüssel.	1. Richten Sie ein automatisiertes RFC namens KMS-Schlüssel erstellen ein, um einen benutzerdefinierten KMS-Schlüssel aus Ihrem Zielkonto zu erstellen. 2. Teilen Sie Ihren benutzerdefinierten KMS-Schlüssel mit dem Quellkonto. Hinweis: Sie können keine DB-Instances von Amazon RDS für Oracle freigeben, die den standardmäßigen von AWS verwalteten Schlüssel für Amazon RDS (`aws/rds`) verwenden. Teilen Sie stattdessen die DB-Instance, indem Sie	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die DB-Instance mit Ihrem KMS-Schlüssel erneut verschlüsseln.	
Erstellen einer Sicherheitsgruppe.	Richten Sie ein automatisiertes RFC namens Create security group ein, um eine Sicherheitsgruppe für Ihre VPC aus Ihrem Zielkonto zu erstellen. Stellen Sie sicher, dass Sie Folgendes angeben: • Neuer Sicherheitsgruppenname • TCP- und UDP-Eingangs- und Ausgangsregeln • Standard-Tags	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Überprüfen Sie Ihre Amazon-RDS-Ressourcen.	Die folgenden Ressourcen werden erstellt, wenn eine DB-Instance von Amazon RDS für Oracle erstellt wird: • Amazon-RDS-Subnetz gruppe (basierend auf der Subnetz-ID) • Amazon RDS-Optio nsgruppe (basierend auf dem Snapshot der Quell-DB-Instance) • Amazon RDS-Param etergruppe (basierend auf dem Snapshot der DB-Instance) Wenn Sie die Amazon-RD S-Ressourcen überprüfen möchten, die beim Erstellen Ihrer DB-Instance erstellt wurden, können Sie eine Verbindung zu Ihrer Oracle-DB-Instance herstellen und Ihre Subnetzgruppe, Optionsgr uppe und Parametergruppe in der Amazon-RDS-Konsole finden.	AWS

Cutover für das Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die Anwendung an.	Halten Sie die Anwendung und ihre abhängigen Services an. Sie müssen den gesamten Datenverkehr zur Datenbank im Quellkonto beenden.	App-Besitzer
Erstellen Sie einen manuellen Snapshot.	Erstellen Sie manuell einen DB-Snapshot der DB-Instance von Amazon RDS für Oracle im Quellkonto.	AWS
Halten Sie die DB-Instance an.	Halten Sie die DB-Instance von Amazon RDS für Oracle an.	AWS
Kopieren Sie den Snapshot.	Kopieren Sie den DB-Snapshot in dasselbe Quellkonto und verwenden Sie dann den benutzerdefinierten KMS-Schlüssel, der vom Zielkonto freigegeben wurde, um die kopierte DB-Snapshot-Datei erneut zu verschlüsseln.	AWS
Teilen Sie den Snapshot.	Geben Sie den neuen Snapshot (mit dem benutzerdefinierten KMS-Schlüssel kopiert) für das Zielkonto frei.	AWS

Cutover auf dem Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie den Snapshot.	Richten Sie ein automatisiertes RFC namens RDS-Snapshot kopieren ein, um den DB-Snapshot in dasselbe Zielkonto zu kopieren und den standardmäßigen AWS-verwalteten KMS-Schlüssel zu verwenden, der für die erneute Verschlüsselung erstellt wurde. Dies ist erforderlich, um das Zielkonto zum Besitzer des neuen Snapshots zu machen und die aus dem Snapshot erstellte DB-Instance von Amazon RDS für Oracle bei Bedarf der Optionsgruppe zuzuordnen.	AWS, AMS
Erstellen Sie eine DB-Instance aus dem Snapshot.	Richten Sie ein automatisiertes RFC namens Create DB from Snapshot ein, um eine DB-Instance von Amazon RDS for Oracle aus dem Snapshot zu erstellen. Stellen Sie sicher, dass Sie Folgendes angeben: • Neue Snapshot-ID, die im vorherigen Schritt erstellt wurde • VPC-ID	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Subnetz-ID • RDS-Instance-ID • Standard-Tags	
Fügen Sie die Instance an die Sicherheitsgruppe an und nehmen Sie Konfigurationsaktualisierungen vor.	1. Führen Sie ein manuelles RFC namens Update Other aus, um die Amazon RDS for Oracle DB-Instance, die Sie zuvor erstellt haben, mit der zuvor erstellten VPC-Sicherheitsgruppe anzuhängen. 2. Nehmen Sie alle zusätzlichen Änderungen an der DB-Instance-Konfiguration von Amazon RDS für Oracle vor.	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die DB-Instance.	Testen Sie die Konnektivität des neuen Endpunkts der DB-Instance von Amazon RDS für Oracle, indem Sie sich bei einer beliebigen Instance oder einem Anwendungsserver anmelden, der in derselben Sicherheitsgruppe gehostet wird, und Telnet verwenden , um eine Verbindung zum 1521-Port herzustellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einer Amazon-RDS-DB-Instance in der Amazon-RDS-Dokumentation. Hinweis: Wenn die Anmeldeinformationen des primären Benutzers verfügbar sind, können Sie die DB-Instance von Amazon RDS für Oracle testen, indem Sie sich von einem beliebigen SQL-Client (z. B. Oracle SQL Developer) aus anmelden.	AWS, DBA

Zugehörige Ressourcen

- AWS Managed Services (AWS-Dokumentation)
- Funktionsweise von RFCs (Dokumentation zu AWS Managed Services)
- Freigeben verschlüsselter Snapshots (Amazon-RDS-Benutzerhandbuch)

- Wie kann ich einen verschlüsselten Amazon-RDS-DB-Snapshot für ein anderes -Konto freigeben? (AWS Knowledge Center)
- Was ist Amazon Relational Database Service (Amazon RDS)? (Amazon-RDS-Benutzerhandbuch)
- Amazon RDS für Oracle (Amazon-RDS-Benutzerhandbuch)
- Verwenden der AMS-Konsolen (Dokumentation zu AWS Managed Services)

Zusätzliche Informationen

Rollback der Migration

Wenn Sie die Migration rückgängig machen möchten, führen Sie die folgenden Schritte aus:

1. Führen Sie ein manuelles RFC (Update Other) aus dem Zielkonto aus, um den im Zielkonto erstellten Datenbank-Stack zu löschen.
2. Aktualisieren Sie die Anwendungskonfiguration so, dass sie auf die DB-Instance von Amazon RDS für Oracle im Quellkonto verweist.
3. Starten Sie die DB-Instance von Amazon RDS für Oracle im Quellkonto.

Migrieren von Oracle-OUT-Bindungsvariablen in eine PostgreSQL-Datenbank

Erstellt von Bikash Chandra Rout (AWS) und Vinaydi (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Database Relational	Ziel: RDS/Aurora Postgresql
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Datenbanken; Migration
AWS-Services: Amazon Aurora; Amazon RDS; AWS SCT		

Übersicht

Dieses Muster zeigt, wie Oracle Database-0UTBindungsvariablen zu einem der folgenden mit PostgreSQL kompatiblen AWS-Datenbankservices migriert werden:

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

PostgreSQL unterstützt keine `0UT` Bind-Variablen. Um dieselbe Funktionalität in Ihren Python-Anweisungen zu erhalten, können Sie eine benutzerdefinierte PL/pgSQL-Funktion erstellen, die stattdessen die Paketvariablen `GET` und `SET` verwendet. Um diese Variablen anzuwenden, verwendet das in diesem Muster bereitgestellte Beispiel-Wrapper-Funktionsskript ein AWS Schema Conversion Tool (AWS SCT)-Erweiterungspaket .

Hinweis: Wenn es sich bei der Oracle-`EXECUTE IMMEDIATE`Anweisung um eine `SELECT` Anweisung handelt, die maximal eine Zeile zurückgeben kann, empfiehlt es sich, Folgendes zu tun:

- Einfügen von `0UT` Bind-Variablen (definiert) in die -`INT0`Klausel
- Einfügen von `IN` Bind-Variablen in die -`USING`Klausel

Weitere Informationen finden Sie unter EXECUTE IMMEDIATE-Anweisung in der Oracle-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle Database 10g (oder neuer) Quelldatenbank in einem On-Premises-Rechenzentrum
- Eine DB-Instance von Amazon RDS für PostgreSQL oder eine mit Aurora PostgreSQL kompatible DB-Instance

Architektur

Quelltechnologie-Stack

- On-Premises Oracle Database 10g (oder neuer) Datenbank

Zieltechnologie-Stack

- Eine DB-Instance von Amazon RDS für PostgreSQL oder eine mit Aurora PostgreSQL kompatible DB-Instance

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Migration von Oracle Database-0UTBindungsvariablen in eine PostgreSQL-kompatible AWS-Datenbank:

Das Diagramm zeigt den folgenden Workflow:

1. AWS SCT konvertiert das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes in ein Format, das mit der PostgreSQL-kompatiblen AWS-Zieldatenbank kompatibel ist.
2. Alle Datenbankobjekte, die nicht automatisch konvertiert werden können, werden von der PL/pgSQL-Funktion markiert. Objekte, die markiert werden, werden dann manuell konvertiert, um die Migration abzuschließen.

Tools

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.

Polen

Migrieren von Oracle OUT-Bindvariablen mithilfe einer benutzerdefinierten PL/pgSQL-Funktion und AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung zu Ihrer PostgreSQL-kompatiblen AWS-Datenbank her.	Nachdem Sie Ihre DB-Instanz erstellt haben, können Sie jede Standard-SQL-Clientanwendung verwenden, um eine Verbindung zu einer Datenbank in Ihrem DB-Cluster herzustellen. Sie können beispielsweise pgAdmin verwenden, um eine Verbindung zu Ihrer DB-Instanz herzustellen. Weitere Informationen finden Sie unter einer der folgenden Themen:	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Herstellen einer Verbindung mit einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch • Herstellen einer Verbindung mit einem Amazon-Aurora-DB-Cluster im Amazon-Aurora-Benutzerhandbuch	
Fügen Sie das Beispiel-Wrapper-Funktionsskript aus diesem Muster zum Hauptschema der Zieldatenbank hinzu.	Kopieren Sie das PL/pgSQL-Beispiel-Wrapper-Funktionsskript aus dem Abschnitt Zusätzliche Informationen dieses Musters. Fügen Sie dann die Funktion zum Hauptschema der Zieldatenbank hinzu. Weitere Informationen finden Sie im Abschnitt CREATE FUNCTION der PostgreSQL-Dokumentation.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Aktualisieren Sie den Suchpfad im Hauptschema der Zieldatenbank, sodass das Schema Test_pg enthält.	Um die Leistung zu verbessern, können Sie die PostgreSQL search_path-Variable so aktualisieren, dass sie den Schemanamen Test_pg enthält. Wenn Sie den Schemanamen in den Suchpfad aufnehmen, müssen Sie den Namen nicht angeben, wenn Sie die PL/pgSQL-Funktion aufrufen. Weitere Informationen finden Sie in Abschnitt 5.9.3 Der Schemasuchpfad in der PostgreSQL-Dokumentation.	Migrationsingenieur

Zugehörige Ressourcen

- AWS Schema Conversion Tool
- OUT-Bind-Variablen (Oracle-Dokumentation)
- Verbesserung der SQL-Abfrageleistung mithilfe von Bind-Variablen (Oracle Blog)

Zusätzliche Informationen

Beispiel für eine PL/pgSQL-Funktion

```
/* Oracle */

CREATE or replace PROCEDURE test_pg.calc_stats_new1 (
                                                a NUMBER,
                                                b NUMBER,
                                                result out NUMBER
                                               )
```

```
IS
BEGIN
result:=a+b;
END;
/
/* Testing */
set serveroutput on
DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN test_pg.calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;  -- calc_stats(a, a, b, a)
  DBMS_OUTPUT.PUT_LINE('output:'||output);
END;

output:11


PL/SQL procedure successfully completed.

--Postgres--

/* Example : 1 */
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new1(
                                                    w integer,
                                                    x integer
                                                  )
RETURNS integer
AS
$BODY$
begin
      return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION aws_oracle_ext.set_package_variable(
                                                                package_name name,
                                                                variable_name name,
```

```
                                                                    variable_value
 anyelement
                                                                  )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
begin
    perform set_config
      ( format( '%s.%s',package_name, variable_name )
      , variable_value::text
      , false );
  end;
$BODY$;

CREATE OR REPLACE FUNCTION aws_oracle_ext.get_package_variable_record(
                                                                    package_name
 name,
                                                                    record_name name
                                                                 )
RETURNS text
LANGUAGE 'plpgsql'
    COST 100
    VOLATILE
AS $BODY$
begin
    execute 'select ' || package_name || '$Init()';

    return aws_oracle_ext.get_package_variable
        (
         package_name := package_name
        , variable_name := record_name || '$REC' );
end;
$BODY$;

--init()--
CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized('test_pg' ) then
```

```
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;

/* callable for 1st Example */

DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$

/*In above Postgres example we have set the value of v_output using v_output_l in the
 dynamic anonymous block to mimic the
  behaviour of oracle out-bind variable .*/

--Postgres Example : 2 --
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new2(
 w integer,
 x integer,
inout status text,
 out result integer)
AS
$BODY$
DECLARE
begin
```

```
result :=  w + x ;
status := 'ok';
end;
$BODY$
LANGUAGE  plpgsql;

/* callable for 2nd Example */
DO $$
declare
v_sql text;
v_output_loc int;
v_staus text:= 'no';
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
execute 'do $a$ declare v_output_l int; v_status_l text; begin select * from
 test_pg.calc_stats_new2('||a||','||b||','''||v_staus||''') into v_status_l,v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_status'', v_status_l) ;
end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
v_staus := aws_oracle_ext.get_package_variable('test_pg', 'v_status');
raise notice 'v_output_loc %',v_output_loc;
raise notice 'v_staus %',v_staus;
END ;
$$
```

Migrieren Sie SAP HANA zu AWS mithilfe von SAP HSR mit demselben Hostnamen

Erstellt von Pradeep Puliyampatta (AWS)

Umgebung: Produktion	Quelle: SAP HANA DB vor Ort	Ziel: SAP HANA DB auf AWS
R-Typ: Rehost	Arbeitslast: SAP	Technologien: Datenbanken; Migration
AWS-Services: AWS-Client-VPN; AWS Direct Connect; Amazon EBS		

Übersicht

SAP HANA-Migrationen zu Amazon Web Services (AWS) können mit mehreren Optionen durchgeführt werden, darunter Sicherung und Wiederherstellung, Export und Import sowie SAP HANA System Replication (HSR). Die Auswahl einer bestimmten Option hängt von der Netzwerkkonnektivität zwischen Quell- und Ziel-SAP-HANA-Datenbanken, der Größe der Quelldatenbank, Überlegungen zu Ausfallzeiten und anderen Faktoren ab.

Die SAP HSR-Option für die Migration von SAP HANA-Workloads zu AWS funktioniert gut, wenn zwischen Quell- und Zielsystem ein stabiles Netzwerk besteht und die gesamte Datenbank (SAP HANA DB-Replikationssnapshot) innerhalb eines Tages vollständig repliziert werden kann, wie von SAP für die Netzwerkdurchsatzanforderungen für SAP HSR festgelegt. Die Ausfallzeiten bei diesem Ansatz beschränken sich auf die Durchführung der Übernahme in der AWS Zielumgebung, die Sicherung der SAP HANA-DB und Aufgaben nach der Migration.

SAP HSR unterstützt die Verwendung verschiedener Hostnamen (Hostnamen, die unterschiedlichen IP-Adressen zugeordnet sind) für den Replikationsverkehr zwischen dem Primär- oder Quell- und dem Sekundär- oder Zielsystem. Sie können dies tun, indem Sie diese spezifischen Gruppen von Hostnamen im Abschnitt unter definieren. `[system_replication_hostname_resolution]` `global.ini` In diesem Abschnitt müssen alle Hosts des primären und des sekundären Standorts auf jedem Host definiert werden. Detaillierte Konfigurationsschritte finden Sie in der SAP-Dokumentation.

Eine wichtige Erkenntnis aus dieser Konfiguration ist, dass sich die Hostnamen im Primärsystem von den Hostnamen im Sekundärsystem unterscheiden müssen. Andernfalls können die folgenden Fehler beobachtet werden.

- `"each site must have a unique set of logical hostnames"`
- `"remoteHost does not match with any host of the source site. All hosts of source and target site must be able to resolve all hostnames of both sites correctly"`

Die Anzahl der Schritte nach der Migration kann jedoch reduziert werden, indem derselbe SAP HANA DB-Hostname in der AWS Zielumgebung verwendet wird.

Dieses Muster bietet eine Problemumgehung für die Verwendung desselben Hostnamens in Quell- und Zielumgebungen, wenn Sie die SAP HSR-Option verwenden. Mit diesem Muster können Sie die Option SAP HANA Hostname Rename verwenden. Sie weisen der SAP-HANA-Zieldatenbank einen temporären Hostnamen zu, um die Eindeutigkeit des Hostnamens für SAP HSR zu gewährleisten. Nachdem die Migration den Meilenstein der Übernahme in der SAP HANA-Zielumgebung abgeschlossen hat, können Sie den Hostnamen des Zielsystems wieder auf den Hostnamen des Quellsystems zurücksetzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Eine Virtual Private Cloud (VPC) mit einem Virtual Private Network (VPN) -Endpunkt oder einem Router.
- AWS Client VPN oder AWS Direct Connect so konfiguriert, dass Dateien von der Quelle zum Ziel übertragen werden.
- SAP HANA-Datenbanken sowohl in der Quell- als auch in der Zielumgebung. Das Ziel-Patch-Level für SAP HANA DB sollte innerhalb derselben SAP HANA Platform-Edition dem Quell-Patch-Level der SAP HANA-DB entsprechen oder höher sein. Beispielsweise kann die Replikation nicht zwischen HANA 1.0- und HANA 2.0-Systemen eingerichtet werden. Weitere Informationen finden Sie unter Frage 15 in SAP-Hinweis: 1999880 — Häufig gestellte Fragen: SAP HANA-Systemreplikation.
- SAP-Anwendungsserver in der Zielumgebung.
- Amazon Elastic Block Store (Amazon EBS) -Volumes in der Zielumgebung.

Einschränkungen

Die folgende Liste von SAP-Dokumenten behandelt bekannte Probleme im Zusammenhang mit dieser Problemumgehung, einschließlich Einschränkungen im Zusammenhang mit dynamischem SAP HANA-Tiering und Scale-out-Migrationen:

- 2956397 — Das Umbenennen des SAP HANA-Datenbanksystems ist fehlgeschlagen
- 2222694 — Beim Versuch, das HANA-System umzubenennen, wird der folgende Fehler angezeigt: „Die Quelldateien gehören nicht dem ursprünglichen sidadm-Benutzer (uid = xxxx)“
- 2607227 — hdblcm: register_rename_system: Das Umbenennen der SAP HANA-Instanz ist fehlgeschlagen
- 2630562 — Die Umbenennung des HANA-Hostnamens ist fehlgeschlagen und HANA wird nicht gestartet
- 2935639 — sr_register verwendet nicht den Hostnamen, der unter system_replication_hostname_resolution im Abschnitt global.ini angegeben ist
- 2710211 — Fehler: Quellsystem und Zielsystem haben überlappende logische Hostnamen
- 2693441 — Ein SAP HANA-System konnte aufgrund eines Fehlers nicht umbenannt werden
- 2519672 — Die primäre und die sekundäre Version von HANA haben unterschiedliche System-PKI-SSFS-Daten und -Schlüssel oder können nicht überprüft werden
- 2457129 — Das Umbenennen von SAP HANA-Systemhosts ist nicht zulässig, wenn dynamisches Tiering Teil der Landschaft ist
- 2473002 — Verwendung der HANA-Systemreplikation zur Migration von Scale-Out-Systemen (Bei der Verwendung dieses Ansatzes zur Umbenennung von Hostnamen für Scale-out-SAP-HANA-Systeme gibt es keine Einschränkungen durch SAP. Das Verfahren muss jedoch auf jedem einzelnen Host wiederholt werden. Für diesen Ansatz gelten auch andere Einschränkungen bei der Scale-Out-Migration.)

Produktversionen

- Diese Lösung gilt für die SAP HANA DB Platform Edition 1.0 und 2.0.

Architektur

Einrichtung der Quelle

In der Quellumgebung ist eine SAP HANA-Datenbank installiert. Alle SAP-Anwendungsserververbindungen und DB-Schnittstellen verwenden denselben Hostnamen für Client-Verbindungen. Das folgende Diagramm zeigt den Beispiel-Hostnamen der Quelle `hdbhost` und die entsprechende IP-Adresse.

Ziel-Setup

Die AWS Cloud Zielumgebung verwendet denselben Hostnamen, um eine SAP HANA-Datenbank auszuführen. Die Zielumgebung auf AWS umfasst Folgendes:

- SAP HANA-Datenbank
- SAP-Anwendungsserver
- EBS-Datenträger

Zwischenkonfiguration

In der folgenden Abbildung wird der Hostname in der AWS Zielumgebung vorübergehend umbenannt, `temp-host` sodass die Hostnamen in der Quelle und im Ziel eindeutig sind. Nachdem die Migration den Meilenstein der Übernahme in der Zielumgebung abgeschlossen hat, wird der virtuelle Hostname des Zielsystems unter Verwendung des ursprünglichen Namens, umbenannt. `hdbhost`

Die Zwischenkonfiguration umfasst eine der folgenden Optionen:

- AWS Client VPN mit einem Client-VPN-Endpunkt
- AWS Direct Connect Verbindung zu einem Router herstellen

SAP-Anwendungsserver in der AWS Zielumgebung können entweder vor der Einrichtung der Replikation oder nach der Übernahme installiert werden. Die Installation der Anwendungsserver vor der Einrichtung der Replikation kann jedoch dazu beitragen, die Ausfallzeiten während der Installation, der Konfiguration der Hochverfügbarkeit und der Backups zu reduzieren.

Tools

AWS-Services

- AWS Client VPNist ein verwalteter clientbasierter VPN-Dienst, mit dem Sie sicher auf AWS Ressourcen und Ressourcen in Ihrem lokalen Netzwerk zugreifen können.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zur Öffentlichkeit AWS-Services einrichten und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances. EBS-Volumes verhalten sich wie unformatierte Blockgeräte. Sie können diese Volumes als Geräte auf Ihren Instances mounten.

Andere Tools

- SAP-Anwendungsserver — SAP-Anwendungsserver bieten Programmierern die Möglichkeit, Geschäftslogik auszudrücken. Der SAP-Anwendungsserver führt die Datenverarbeitung auf der Grundlage der Geschäftslogik durch. Die eigentlichen Daten werden in einer Datenbank gespeichert, die eine separate Komponente ist.
- SAP HANA Cockpit und SAP HANA Studio — Sowohl SAP HANA Cockpit als auch SAP HANA Studio bieten eine administrative Schnittstelle zur SAP HANA-Datenbank. In SAP HANA Studio ist die SAP HANA-Verwaltungskonsole die Systemansicht, die relevante Inhalte für die SAP HANA-Datenbankadministration bereitstellt.
- SAP HANA-Systemreplikation — Die SAP HANA-Systemreplikation (SAP HSR) ist das von SAP bereitgestellte Standardverfahren für die Replikation von SAP HANA-Datenbanken. Die erforderlichen ausführbaren Dateien für SAP HSR sind Teil des SAP HANA-Serverkerns selbst.

Epen

Bereiten Sie die Quell- und Zielumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfiguri eren Sie die SAP HANA-Date nbanken.	Stellen Sie in der Quell- und Zielumgebung sicher, dass die SAP HANA DB gemäß den bewährten Methoden von SAP HANA installiert und konfiguri ert ist. Weitere Informationen finden Sie unter SAP HANA unter AWS.	SAP-Basisverwaltung
Ordnen Sie die IP-Adresse zu.	Stellen Sie in der Zielumgeb ung sicher, dass der temporäre Hostname einer internen IP-Adresse zugewiesen ist. 1. Weisen Sie der EC2-Instance in der AWS-Managementkonsole eine sekundäre IPv4-Adresse zu, indem Sie zu EC2, Instanz, Aktionen, Netzwerk, IP-Adresse verwalten, Neue IP-Adresse zuweisen navigieren. 2. Um dem EC2-Netzw erkadapter (NIC) dieselbe Adresse vom Betriebss ystem aus zuzuweisen, führen Sie als Root-Benu tzer den Befehl `ip addr add <IP>/32 dev eth0`	AWS-Verwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus und <IP> ersetzen Sie ihn durch die IP-Adresse aus Schritt 1.	
Ziel-Hostnamen auflösen.	Vergewissern Sie sich in der sekundären SAP HANA DB, dass beide Hostnamen (hdbhostundtemp-host) für die SAP HANA-Repl ikationsnetzwerke aufgelöst wurden, indem Sie die entsprechenden Hostnamen in der Datei aktualisieren. /etc/ hosts	Linux-Verwaltung
Sichern Sie die Quell- und Zieldatenbanken von SAP HANA.	Verwenden Sie SAP HANA Studio oder das SAP HANA Cockpit, um Backups auf den SAP HANA-Datenbanken durchzuführen.	SAP-Basisverwaltung
PKI-Zertifikate des Exchange-Systems.	(Gilt nur für SAP HANA 2.0 und höher) Exchange-Zertifika te im sicheren Speicher der Public-Key-Infrast ruktur (PKI) des Systems im Dateisystemspeicher (SSFS) zwischen der primären und der sekundären Datenbank. Weitere Informationen finden Sie im SAP-Hinweis 2369981 — Erforderliche Konfigura tionsschritte für die Authentif izierung mit SAP HANA System Replication.	SAP-Basisverwaltung

Benennen Sie die Zieldatenbank SAP HANA um

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Verbindungen zum Zielclient.	Fahren Sie in der Zielumgebung die SAP-Anwendungsserver und andere Client-Verbindungen herunter.	SAP-Basisverwaltung

Benennen Sie die Ziel-SAP HANA-Datenbank in den temporären Hostnamen um.	1. Benennen Sie als Root-Benutzer den Zielhostnamen der SAP HANA-DB mithilfe von resident in den temporären Hostnamen um. `hdblcm`
	`root $> cd /hana/shared/<SID/hdblcm`
	`root $> ./hdblcm`
	2. Wählen Sie eine Option. 9 `| rename_system | Rename the SAP HANA Database System`
	3. Geben Sie den neuen Namen ein: `temp-host .`
	4. Sie können andere Optionen nach Bedarf validieren. Achten Sie jedoch darauf, dass Sie die Host-Umbenennung nicht mit einer SID-Änderung verwechseln (SAP-Hinweis 2598814 — hdblcm: SID-Umbenennung schlägt fehl).
		SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Stopp und Start der SAP HANA-DB wird von gesteuert. `hdblcm`	
Weisen Sie Replikationsnetzwerke zu.	Geben Sie in der `global.ini` Datei des Quellsystems unter dem `[system_replication_hostname_resolution]` Header die Details zum Quell- und Zielreplikationsnetzwerk an. Kopieren Sie dann die Einträge in die `global.ini` Datei auf dem Zielsystem.	SAP-Basisverwaltung
Aktivieren Sie die Replikation auf der Primärseite.	Führen Sie den folgenden Befehl aus, um die Replikation auf der SAP HANA-Quelldatenbank zu aktivieren. `hdbnsutil -sr_enable --name=siteA`	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Registrieren Sie die Ziel-SAP HANA DB als Sekundärs ystem.	Um die SAP HANA-Ziel datenbank als sekundäres Quellsystem für SAP HSR zu registrieren, wählen Sie asynchrone Replikation.
	`(sid)adm $> HDB stop`
	`(sid)adm $> hdbnsutil -sr_register –name=sitB –remotehost=hdbhost /`
	`--remoteInstance=00 –replicationMode=async –operationMode=logreplay`
	`(sid)adm $> HDB start`
	Alternativ können Sie die `–online` Option zur Registrierung wählen. In diesem Fall müssen Sie die SAP HANA DB nicht stoppen und starten.
		SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Synchronisation validieren.	Stellen Sie in der SAP HANA-Quelldatenbank sicher, dass alle Protokolle auf das Zielsystem angewende t werden (da es sich um eine asynchrone Replikation handelt).
	
	Um die Replikation zu überprüfen, führen Sie auf der Quelle die folgenden Befehle aus.
	
	`(sid)adm $> cdpy`
	`(sidadm $> python systemReplicationStatus.py`
		SAP-Basisverwaltung

Fahren Sie die SAP-Quell anwendung und die SAP HANA DB herunter.	Führen Sie während der Umstellung auf die Migration das Quellsystem (die SAP-Anwendung und die SAP HANA-Datenbank) herunter.	SAP-Basisverwaltung
Führen Sie eine Übernahme am Ziel durch.	Führen Sie den Befehl aus, um eine Übernahme am Ziel auf AWS durchzufü hrenhdbnsutil -sr_takeover .	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schalten Sie auf der Ziel-SAP HANA-Datenbank die Replikation aus.	Um die Replikationsmetadaten zu löschen, beenden Sie die Replikation auf dem Zielsystem, indem Sie den Befehl ausführen`hdbnsutil -sr_disable` . Hinweis: Dies entspricht dem SAP-Hinweis 2693441 — Ein SAP HANA-System konnte aufgrund eines Fehlers nicht umbenannt werden.	SAP-Basisverwaltung
Sichern Sie die SAP HANA-Zieldatenbank.	Nach erfolgreicher Übernahme empfehlen wir, ein vollständiges SAP HANA DB-Backup durchzuführen.	SAP-Basisverwaltung

Kehren Sie zum ursprünglichen Hostnamen im Zielsystem zurück

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Setzt den Ziel-Hostnamen der SAP HANA DB auf den ursprünglichen Namen zurück.	1. Um den Zielhostnamen der SAP HANA DB auf den ursprünglichen virtuellen Hostnamen zurückzusetzen, verwenden Sie resident. `hdblcm`
	
	`root $> cd /hana/shared/<SID>/hdblcm`
	`root $> ./hdblcm`
	
	2. Wählen Sie eine Option. 9 `| rename_system |`
		SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Rename the SAP HANA Database System` 3. Geben Sie den neuen Namen ein:`hdbhost`. Sie können andere Optionen nach Bedarf validieren. Achten Sie jedoch darauf, dass Sie die Host-Umbenennung nicht mit einer SID-Änderung verwechseln (SAP-Hinweis 2598814 — hdblcm: SID-Umbenennung schlägt fehl).	
Passen Sie hdbuserstore an.	Passen Sie die `hdbuserstore` Details an, die auf die Quelldetails verweisen. `schema/user` Die detaillierten Schritte finden Sie in der SAP-Dokumentation. Führen Sie den Befehl aus, um diesen Schritt zu validieren`R3trans -d`. Das Ergebnis sollte eine erfolgreiche Verbindung zur SAP HANA-Datenbank widerspiegeln.	SAP-Basisverwaltung
Starten Sie die Client-Verbindungen.	Starten Sie in der Zielumgebung die SAP-Anwendungsserver und andere Client-Verbindungen.	SAP-Basisverwaltung

Zugehörige Ressourcen

SAP-Referenzen

Referenzen zur SAP-Dokumentation werden häufig von SAP aktualisiert. Um auf dem Laufenden zu bleiben, lesen Sie den SAP-Hinweis 2407186 — Anleitungen und Whitepapers für SAP HANA High Availability.

Zusätzliche SAP-Hinweise

- 2550327 — So benennen Sie ein SAP HANA-System um
- 1999880 — Häufig gestellte Fragen: SAP HANA-Systemreplikation
- 2078425 — Hinweis zur Fehlerbehebung für das Lifecycle-Management-Tool hdblcm für die SAP HANA-Plattform
- 2592227 — Änderung des FQDN-Suffixes in HANA-Systemen
- 2048681 — Durchführung von Verwaltungsaufgaben für das Lebenszyklusmanagement der SAP HANA-Plattform auf Systemen mit mehreren Hosts ohne SSH- oder Root-Anmeldeinformationen

SAP-Dokumente

- Netzwerkverbindung zur Systemreplikation
- Auflösung des Hostnamens für die Systemreplikation

AWS Verweise

- Migration von SAP HANA von anderen Plattformen auf AWS

Zusätzliche Informationen

Die Änderungen, die im `hdblcm` Rahmen der Aktivität zur Umbenennung von Hostnamen vorgenommen wurden, werden im folgenden ausführlichen Protokoll zusammengefasst.

Migrieren von SQL Server zu AWS mithilfe verteilter Verfügbarkeitsgruppen

Erstellt von Praveen Marthala (AWS)

Quelle: SQL Server On-Premises	Ziel: SQL Server auf EC2	R-Typ: Hostwechsel
Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Migration	Workload: Microsoft
AWS-Services: Amazon EC2		

Übersicht

Microsoft SQL Server Always On-Verfügbarkeitsgruppen bieten eine Hochverfügbarkeitslösung (HA) und eine Notfallwiederherstellungslösung (DR) für SQL Server. Eine Verfügbarkeitsgruppe besteht aus einem primären Replikat, das Lese-/Schreibdatenverkehr akzeptiert, und bis zu acht sekundären Replikaten, die Lesedatenverkehr akzeptieren. Eine Verfügbarkeitsgruppe ist auf einem Windows Server Failover Cluster (WSFC) mit zwei oder mehr Knoten konfiguriert.

Microsoft SQL Server Always On verteilte Verfügbarkeitsgruppen bieten eine Lösung zum Konfigurieren von zwei separaten Verfügbarkeitsgruppen zwischen zwei unabhängigen WFSCs. Die Verfügbarkeitsgruppen, die Teil der verteilten Verfügbarkeitsgruppe sind, müssen sich nicht im selben Rechenzentrum befinden. Eine Verfügbarkeitsgruppe kann On-Premises und die andere Verfügbarkeitsgruppe in der Amazon Web Services (AWS) Cloud auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances in einer anderen Domain sein.

Dieses Muster beschreibt die Schritte zur Verwendung einer verteilten Verfügbarkeitsgruppe zur Migration von lokalen SQL Server-Datenbanken, die Teil einer vorhandenen Verfügbarkeitsgruppe sind, zu SQL Server mit auf Amazon EC2 eingerichteten Verfügbarkeitsgruppen. Wenn Sie diesem Muster folgen, können Sie die Datenbanken mit minimalen Ausfallzeiten während des Cutover in die AWS Cloud migrieren. Die Datenbanken sind in AWS unmittelbar nach dem Cutover hochverfügbar. Sie können dieses Muster auch verwenden, um das zugrunde liegende Betriebssystem von On-Premises zu AWS zu ändern und dabei dieselbe Version von SQL Server beizubehalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Direct Connect oder AWS Site-to-Site VPN
- Die gleiche Version von SQL Server, die On-Premises und auf den beiden Knoten auf AWS installiert ist

Produktversionen

- SQL Server Version 2016 und höher
- SQL Server Enterprise Edition

Architektur

Quelltechnologie-Stack

- Microsoft SQL Server-Datenbank mit AlwaysOn-Verfügbarkeitsgruppen On-Premises

Zieltechnologie-Stack

- Microsoft SQL Server-Datenbank mit AlwaysOn-Verfügbarkeitsgruppen auf Amazon EC2 in der AWS Cloud

Migrationsarchitektur

Terminologie

- WSFC 1 – WSFC On-Premises
- WSFC 2 – WSFC in der AWS Cloud
- AG 1 – Erste Verfügbarkeitsgruppe, die sich in WSFC 1 befindet
- AG 2 – Zweite Verfügbarkeitsgruppe, die sich in WSFC 2 befindet
- SQL Server-Primärreplikat – Knoten in AG 1, der für alle Schreibvorgänge als globaler Primärknoten betrachtet wird

- SQL Server Forwarder – Knoten in AG 2, der Daten asynchron vom primären SQL Server-Replikat empfängt
- Sekundäres SQL Server-Replikat – Knoten in AG 1 oder AG 2, die Daten synchron vom primären Replikat oder vom Forwarder empfangen

Tools

- AWS Direct Connect – AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem AWS Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen, wodurch Internetdienstanbieter in Ihrem Netzwerkpfad umgangen werden.
- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können Amazon EC2 verwenden, um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können auf- oder abskalieren.
- AWS Site-to-Site VPN – AWS Site-to-Site VPN unterstützt das Erstellen eines site-to-site Virtual Private Network (VPN). Sie können das VPN so konfigurieren, dass der Datenverkehr zwischen Instances, die Sie in AWS starten, und Ihrem eigenen Remote-Netzwerk weitergeleitet wird.
- Microsoft SQL Server Management Studio – Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung der SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Polen

Einrichten einer zweiten Verfügbarkeitsgruppe in AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen WSFC in AWS.	Erstellen Sie WSFC 2 auf Amazon EC2-Instances mit zwei Knoten für HA. Sie verwenden diesen Failover-Cluster, um die zweite Verfügbarkeitsgruppe (AG 2) in AWS zu erstellen.	Systemadministrator, SysOps Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die zweite Verfügbarkeitsgruppe auf WSFC 2.	Erstellen Sie mithilfe von SSMS AG 2 auf zwei Knoten in WSFC 2. Der erste Knoten in WSFC 2 fungiert als Weiterleitung. Der zweite Knoten in WSFC 2 fungiert als sekundäres Replikat von AG 2. Derzeit sind in AG 2 keine Datenbanken verfügbar. Dies ist der Ausgangspunkt für die Einrichtung der verteilten Verfügbarkeitsgruppe.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Datenbanken ohne Wiederherstellungsoption auf AG 2.	Sichern Sie Datenbanken in der On-Premises-Verfügbarkeitsgruppe (AG 1). Stellen Sie die Datenbanken sowohl im Forwarder als auch im sekundären Replikat von AG 2 ohne Wiederherstellungsoption wieder her. Geben Sie beim Wiederherstellen der Datenbanken einen Speicherort mit genügend Speicherplatz für die Datenbankdatendateien und die Protokolldateien an. In dieser Phase befinden sich die Datenbanken im Wiederherstellungsstatus. Sie sind nicht Teil von AG 2 oder der verteilten Verfügbarkeitsgruppe und werden nicht synchronisiert.	DBA, Entwickler

Konfigurieren der verteilten Verfügbarkeitsgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die verteilte Verfügbarkeitsgruppe auf AG 1.	Um die verteilte Verfügbarkeitsgruppe auf AG 1 zu erstellen, verwenden Sie die `CREATE AVAILABILITY GROUP` mit der `DISTRIBUTED` Option .	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Verwenden Sie `LISTENER_URL` Endpunktadressen für AG 1 und AG 2. 2. Verwenden Sie für `AVAILABILITY-MODE` , `ASYNCHRONOUS_COMMIT` um Netzwerklatenz zu vermeiden, falls vorhanden . Dies wirkt sich nicht auf die Leistung der Datenbank aus. 3. Geben Sie als `FAILOVER_MODE` `MANUAL`ein. Es ist der einzige Verfügbar keitsmodus, der mit verteilte n Verfügbarkeitsgruppen funktioniert. 4. Um die Datenbanken manuell auf AG 2 wiederher zustellen und mehr Kontrolle über größere Datenbanken zu haben, verwenden Sie `MANUAL` für `SEEDING_MODE` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die verteilte Verfügbarkeitsgruppe auf AG 2.	Um die verteilte Verfügbar keitsgruppe auf AG 2 zu erstellen, verwenden Sie `ALTER AVAILABILITY GROUP` mit der `DISTRIBUT ED` Option . 1. Verwenden Sie `LISTENER_ URL` Endpunktadressen für AG 1 und AG 2. 2. Verwenden Sie für `AVAILABILITY-MODE` , `ASYNCHRONOUS_COMMI T` um Netzwerklatenz zu vermeiden, falls vorhanden . Dies wirkt sich nicht auf die Leistung der Datenbank aus. 3. Geben Sie als `FAILOVER_ MODE` `MANUAL`ein. Es ist der einzige Verfügbar keitsmodus, der mit verteilte n Verfügbarkeitsgruppen funktioniert. 4. Um die Datenbanken manuell auf AG 2 wiederher zustellen und mehr Kontrolle über größere Datenbanken zu haben, verwenden Sie `MANUAL` für `SEEDING_MODE` .	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die verteilte Verfügbar keitsgruppe wird zwischen AG 1 und AG 2 erstellt. Die Datenbanken in AG 2 sind noch nicht für die Teilnahme am Datenfluss von AG 1 zu AG 2 konfiguriert.	
Fügen Sie der Weiterleitung und dem sekundären Replikat auf AG 2 Datenbanken hinzu.	Fügen Sie die Datenbank en der verteilten Verfügbar keitsgruppe hinzu, indem Sie `ALTER DATABASE` mit der `SET HADR AVAILABIL ITY GROUP` Option sowohl im Forwarder als auch im sekundären Replikat auf AG 2 verwenden. Dadurch wird der asynchron e Datenfluss zwischen Datenbanken in AG 1 und AG 2 gestartet. Der globale primäre Cluster nimmt Schreibvorgänge entgegen, sendet Daten synchron an das sekundäre Replikat auf AG 1 und sendet Daten asynchron an den Forwarder auf AG 2. Die Weiterleitung auf AG 2 sendet Daten synchron an das sekundäre Replikat auf AG 2.	DBA, Entwickler

Überwachen des asynchronen Datenflusses zwischen AG 1 und AG 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie DMVs und SQL Server-Protokolle.	Überwachen Sie den Status des Datenflusses zwischen zwei Verfügbarkeitsgrup pen mithilfe dynamischer Verwaltungsansichten (DMVs) und SQL Server-Protokollen. Zu den DMVs, die für die Überwachung von Interesse sind, gehören `sys.dm_ha dr_availability_re plica_states` und `sys.dm_hadr_automa tic_seeding` . Überwachen Sie den Status der Weiterleitungssync hronisierung im SQL Server-Protokoll auf der Weiterleitung.	DBA, Entwickler

Durchführen von Cutover-Aktivitäten für die endgültige Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie den gesamten Datenverkehr zum primären Replikat.	Stoppen Sie den eingehenden Datenverkehr zum primären Replikat in AG 1, damit keine Schreibaktivität in den Datenbanken stattfindet und die Datenbanken für die Migration bereit sind.	App-Besitzer, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie den Verfügbar keitsmodus der verteilten Verfügbarkeitsgruppe auf AG 1.	Legen Sie im primären Replikat den Verfügbar keitsmodus der verteilten Verfügbarkeitsgruppe auf synchron fest. Nachdem Sie den Verfügbar keitsmodus auf synchron geändert haben, werden die Daten synchron vom primären Replikat in AG 1 an den Forwarder in AG 2 gesendet.	DBA, Entwickler
Überprüfen Sie die LSNs in beiden Verfügbarkeitsgruppen.	Überprüfen Sie die letzten Log Sequence Numbers (LSNs) sowohl in AG 1 als auch in AG 2. Da keine Schreibvorgänge im primären Replikat in AG 1 stattfinden, werden die Daten synchronisiert und die letzten LSNs für beide Verfügbar keitsgruppen sollten übereinst immen.	DBA, Entwickler
Aktualisieren Sie AG 1 auf die sekundäre Rolle.	Wenn Sie AG 1 auf die sekundäre Rolle aktualisi eren, verliert AG 1 die primäre Replikatrolle und akzeptiert keine Schreibvorgänge, und der Datenfluss zwischen zwei Verfügbarkeitsgruppen wird beendet.	DBA, Entwickler

Failover zur zweiten Verfügbarkeitsgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Manuelles Failover auf AG 2.	Ändern Sie in der Weiterlei tung in AG 2 die verteilte Verfügbarkeitsgruppe, um Datenverlust zuzulassen. Da Sie bereits überprüft und bestätigt haben, dass die letzten LSNs auf AG 1 und AG 2 übereinstimmen, ist der Datenverlust kein Problem. Wenn Sie Datenverlust auf dem Forwarder in AG 2 zulassen, ändern sich die Rollen von AG 1 und AG 2: • AG 2 wird zur Verfügbar keitsgruppe mit dem primären Replikat und dem sekundären Replikat. • AG 1 wird zur Verfügbar keitsgruppe mit der Weiterlei tung und dem sekundären Replikat.	DBA, Entwickler
Ändern Sie den Verfügbar keitsmodus der verteilten Verfügbarkeitsgruppe auf AG 2.	Ändern Sie auf dem primären Replikat in AG 2 den Verfügbarkeitsmodus auf asynchron. Dadurch wird die Datenvers chiebung von AG 2 auf AG 1 geändert, von synchron zu asynchron. Dieser Schritt ist erforderlich, um die Netzwerkl	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	atenz zwischen AG 2 und AG 1 zu vermeiden, sofern vorhanden, und beeinträchtigt nicht die Leistung der Datenbank.	
Beginnen Sie mit dem Senden von Datenverkehr an das neue primäre Replikat.	Aktualisieren Sie die Verbindungszeichenfolge, um den Listener-URL-Endpunkt auf AG 2 zum Senden von Datenverkehr an die Datenbanken zu verwenden. AG 2 akzeptiert jetzt Schreibvorgänge und sendet Daten an den Forwarder in AG 1 sowie Daten an ein eigenes sekundäres Replikat in AG 2. Daten werden asynchron von AG 2 auf AG 1 verschoben.	App-Besitzer, Entwickler

Durchführen von Aktivitäten nach dem Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die verteilte Verfügbarkeitsgruppe auf AG 2.	Überwachen Sie die Migration für den geplanten Zeitraum. Entfernen Sie dann die verteilte Verfügbarkeitsgruppe auf AG 2, um die Einrichtung der verteilten Verfügbarkeitsgruppe zwischen AG 2 und AG 1 zu entfernen. Dadurch wird die Konfiguration der verteilten Verfügbar	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	keitsgruppe entfernt und der Datenfluss von AG 2 zu AG 1 wird beendet. Zu diesem Zeitpunkt ist AG 2 auf AWS hochverfügbar, mit einem primären Replikat, das Schreibvorgänge entgegenn immt, und einem sekundäre n Replikat in derselben Verfügbarkeitsgruppe.	
Außerbetriebnahme der On-Premises-Server.	Außerbetriebnahme der On-Premises-Server in WSFC 1, die Teil von AG 1 sind.	Systemadministrator, SysOps Administrator

Zugehörige Ressourcen

- Verteilte Verfügbarkeitsgruppen
- SQL Docs: Verteilte Verfügbarkeitsgruppen
- SQL Docs: Always On availability groups: eine Lösung mit hoher Verfügbarkeit und Notfallwiederherstellung

Migrieren von Oracle 8i oder 9i zu Amazon RDS für Oracle mit SharePlex und AWS DMS

Erstellt von Ramu Jagini (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS
R-Typ: Plattformwechsel	Workload: Open-Source; Oracle	Technologien: Datenbanken; Cloudnativ; Migration
AWS-Services: AWS DMS; Amazon RDS		

Übersicht

Dieses Muster beschreibt, wie Sie eine lokale Oracle 8i- oder 9i-Datenbank zu einer Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbank migrieren. Sie können dieses Muster verwenden, um Ihre Migration mit reduzierter Ausfallzeit abzuschließen, indem Sie Bol SharePlex für die synchrone Replikation verwenden.

Sie müssen für Ihre Migration eine Zwischen-Oracle-Datenbank-Instance verwenden, da AWS Database Migration Service (AWS DMS) Oracle 8i oder 9i nicht als Quellumgebung unterstützt. Sie können SharePlex 7.6.3 verwenden, um von früheren Oracle-Datenbankversionen auf spätere Oracle-Datenbankversionen zu replizieren. Die Oracle-Zwischendatenbank-Instance ist als Ziel für SharePlex 7.6.3 kompatibel und wird als Quelle für AWS DMS oder neuere Versionen von unterstützt SharePlex. Diese Unterstützung ermöglicht die weitere Replikation von Daten in die Zielumgebung von Amazon RDS für Oracle.

Beachten Sie, dass sich mehrere veraltete Datentypen und Funktionen auf eine Migration von Oracle 8i oder 9i auf die neueste Version von Oracle Database auswirken können. Um diese Auswirkungen zu minimieren, verwendet dieses Muster Oracle 11.2.0.4 als Zwischendatenbankversion, um den Schemacode vor der Migration in die Zielumgebung von Amazon RDS für Oracle zu optimieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle 8i- oder 9i-Quelldatenbank in einer On-Premises-Umgebung
- Oracle Database 12c Release 2 (12CR2) für das Staging auf Amazon Elastic Compute Cloud (Amazon EC2)
- Bol SharePlex 7.6.3 (kommerzielle Klasse)

Einschränkungen

- Einschränkungen von RDS für Oracle

Produktversionen

- Oracle 8i oder 9i für die Quelldatenbank
- Oracle 12CR2 für die Staging-Datenbank (muss mit der Version von Amazon RDS für Oracle übereinstimmen)
- Oracle 12CR2 oder höher für die Zieldatenbank (Amazon RDS für Oracle)

Architektur

Quelltechnologie-Stack

- Oracle 8i- oder 9i-Datenbank
- SharePlex

Zieltechnologie-Stack

- Amazon RDS für Oracle

Migrationsarchitektur

Das folgende Diagramm zeigt, wie Sie eine Oracle 8i- oder 9i-Datenbank von einer On-Premises-Umgebung zu einer Amazon RDS for Oracle-DB-Instance in der AWS Cloud migrieren.

Das Diagramm zeigt den folgenden Workflow:

1. Aktivieren Sie die Oracle-Quelldatenbank mit Archivprotokollmodus, erzwungener Protokollierung und zusätzlicher Protokollierung.
2. Stellen Sie die Oracle-Staging-Datenbank aus der Oracle-Quelldatenbank mithilfe von Recovery Manager (RMAN) point-in-time -Wiederherstellung und FLASHBACK_SCN wieder her.
3. Konfigurieren Sie SharePlex zum Lesen von Redo-Protokollen aus der Oracle-Quelldatenbank mithilfe von `FLASHBACK_SCN` (verwendet in RMAN).
4. Starten Sie die SharePlex Replikation, um Daten aus der Oracle-Quelldatenbank mit der Oracle-Staging-Datenbank zu synchronisieren.
5. Stellen Sie die Zieldatenbank von Amazon RDS für Oracle mithilfe von EXPDP und microSDDP mit wieder her`FLASHBACK_SCN`.
6. Konfigurieren Sie AWS DMS und seine Quellaufgaben als Oracle-Staging-Datenbank und Amazon RDS für Oracle als Zieldatenbank mithilfe von `FLASHBACK_SCN` (verwendet in EXPDP).
7. Starten Sie AWS DMS-Aufgaben, um Daten aus der Oracle-Staging-Datenbank mit der Oracle-Zieldatenbank zu synchronisieren.

Tools

- Amazon Relational Database Service (Amazon RDS) unterstützt Sie beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Bol SharePlex ist ein Oracle-zu-Oracle-Datenreplikationstool zum Verschieben von Daten mit minimalen Ausfallzeiten und ohne Datenverlust.
- Recovery Manager (RMAN) ist ein Oracle Database-Client, der Sicherungs- und Wiederherstellungsaufgaben für Ihre Datenbanken ausführt. Es vereinfacht das Sichern, Wiederherstellen und Wiederherstellen von Datenbankdateien erheblich.
- Data Pump Export hilft Ihnen beim Hochladen von Daten und Metadaten in eine Reihe von Betriebssystemdateien, die als Dump-Dateisatz bezeichnet werden. Der Dump-Dateisatz kann nur über das Data Pump Import-Dienstprogramm oder das Paket DBMS_DATAPUMP importiert werden.

Polen

Einrichten von SharePlex und der Oracle-Staging-Datenbank auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine EC2-Instance.	1. Erstellen Sie eine EC2-Instance. 2. Installieren Sie Oracle 12CR2 auf der EC2-Instance, um als Oracle-Staging-Datenbank zu dienen.	Oracle-Verwaltung
Bereiten Sie die Staging-Datenbank vor.	Bereiten Sie die Oracle-Staging-Datenbank für die Wiederherstellung als Upgrade auf Oracle 12CR2 vor, indem Sie das RMAN-Backup aus der Oracle 8i- oder 9i-Datenbank-Quellumgebung nehmen. Weitere Informationen finden Sie im Benutzerhandbuch für Oracle 9i Recovery Manager und im Benutzerhandbuch für Datenbank-Backup und Wiederherstellung in der Oracle-Dokumentation.	Oracle-Verwaltung
Konfigurieren Sie SharePlex.	Konfigurieren Sie die SharePlex Quelle als lokale Oracle 8i- oder 9i-Datenbank und konfigurieren Sie das Ziel als Oracle 12CR2-Staging-Datenbank, die auf Amazon EC2 gehostet wird.	SharePlex, Oracle-Verwaltung

Einrichten von Amazon RDS für Oracle als Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Oracle-DB-Instance.	Erstellen Sie eine Datenbank von Amazon RDS für Oracle und verbinden Sie dann Oracle 12CR2 mit der Datenbank. Weitere Informationen finden Sie unter Erstellen einer Oracle-DB-Instance und Herstellen einer Verbindung mit einer Datenbank auf einer Oracle-DB-Instance in der Amazon-RDS-Dokumentation.	DBA
Stellen Sie Amazon RDS für Oracle aus der Staging-Datenbank wieder her.	1. Erstellen Sie ein EXPDP-Backup vom Oracle-Staging-Datenbankserver mithilfe von `FLASHBACK_SCN` . 2. Stellen Sie Amazon RDS für Oracle aus der Staging-Datenbank wieder her. Weitere Informationen finden Sie unter54 DBMS_DATA PUMP in der Oracle-Dokumentation.	DBA

Einrichten von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Endpunkte für die Datenbanken.	Erstellen Sie einen Quellendpunkt für die Oracle-Staging-Datenbank und einen Zielendpunkt für die Datenbank von Amazon RDS für Oracle. Weitere Informationen finden Sie unter Wie erstelle ich Quell- oder Zielendpunkte mit AWS DMS? im AWS Knowledge Center.	DBA
Erstellen Sie eine Replikations-Instance.	Verwenden Sie AWS DMS, um eine Replikations-Instance für die Oracle-Staging-Datenbank in der Datenbank von Amazon RDS für Oracle zu starten. Weitere Informationen finden Sie unter Wie erstelle ich eine AWS DMS-Replikations-Instance? im AWS Knowledge Center.	DBA
Erstellen und starten Sie Replikationsaufgaben.	Erstellen Sie AWS DMS-Replikationsaufgaben für die Erfassung von Datenänderungen (Change Data Capture, CDC) mithilfe `FLASHBACK_SCN` von aus EXPDP (da der vollständige	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ladevorgang bereits über EXPDP erfolgt ist). Weitere Informationen finden Sie unter Erstellen einer Aufgabe in der AWS DMS-Dokumentation.	

Umstellung auf Amazon RDS für Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Anwendungs-Workload.	Halten Sie die Anwendung sserver und ihre Anwendung en während des geplanten Cutover-Fensters an.	App-Entwickler, DBA
Validieren Sie die Synchroni sierung der lokalen Oracle-St aging-Datenbank mit der EC2-Instance.	Vergewissern Sie sich, dass alle Nachrichten für Replikationsaufgaben von der SharePlex Replikations-Insta nce in die Oracle-Staging-Datenbank auf Amazon EC2 gepostet wurden, indem Sie einige Protokollwechsel für die On-Premises-Quelldatenbank durchführen. Weitere Informationen finden Sie unter 6.4.2 Wechseln einer Protokolldateien in der Oracle-Dokumentation.	DBA
Validieren Sie die Synchroni sierung der Oracle-Staging-	Vergewissern Sie sich, dass alle Ihre AWS DMS-Aufga ben keine Verzögerung und	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Datenbank mit der Datenbank von Amazon RDS für Oracle.	keine Fehler aufweisen, und überprüfen Sie dann den Validierungsstatus der Aufgaben.	
Halten Sie die Replikation von SharePlex und Amazon RDS an.	Wenn sowohl die SharePlex als auch AWS DMS-Repli kationen keine Fehler anzeigen, halten Sie beide Replikationen an.	DBA
Ordnen Sie die Anwendung Amazon RDS neu zu.	Teilen Sie die Endpunktdetails von Amazon RDS für Oracle mit dem Anwendungsserver und seinen Anwendung en und starten Sie dann die Anwendung, um den Geschäftsbetrieb fortzusetzen.	App-Entwickler, DBA

Testen der AWS-Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Oracle-Staging-Datenbankumgebung in AWS.	1. Testen Sie die SharePlex Replikation und stellen Sie sicher, dass es keine Synchronisierungslücken oder Replikationsfehler in der Oracle-Staging-Dat enbank gibt. 2. Stellen Sie sicher, dass sich die Anwendung durch Benchmarks, die in der On-Premises-Umgebung	SharePlex, Oracle-Administrat ion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	definiert sind, wie erwartet verhält.	
Testen Sie die Amazon RDS-Umgebung.	1. Stellen Sie sicher, dass alle Daten, die nach der Replikation an Amazon RDS weitergegeben werden, fehlerfrei sind. 2. Verweisen Sie eine andere Anwendung auf die Amazon RDS-DB-Instance und führen Sie dann Leistungs tests durch, um das erwartete Verhalten zu überprüfen. Weitere Informationen finden Sie unter Amazon RDS für Oracle in der Amazon-RDS-Dokumentation.	Oracle-Verwaltung

Zugehörige Ressourcen

- Migrieren Sie sicher
- Amazon EC2
- Amazon RDS für Oracle
- AWS Database Migration Service
- Debuggen Ihrer AWS DMS-Migrationen: Was ist zu tun, wenn Dinge schief laufen (Teil 1)
- Debuggen Ihrer AWS DMS-Migrationen: Was ist zu tun, wenn Dinge schief laufen (Teil 2)
- Debuggen Ihrer AWS DMS-Migrationen: Was ist zu tun, wenn Dinge schief gehen? (Teil 3)
- SharePlex für die Datenbankreplikation
- SharePlex: Datenbankreplikation für jede Umgebung

Überwachen von Amazon Aurora auf Instances ohne Verschlüsselung

Erstellt von Mansi Suratwala (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Speicher und Backup; Datenbanken	Workload: Open-Source; Alle anderen Workloads
AWS-Services: Amazon SNS; Amazon Aurora; AWS CloudTrail; Amazon CloudWatch; AWS Lambda		

Übersicht

Dieses Muster bietet eine Amazon Web Services (AWS)- CloudFormation Vorlage, die Sie bereitstellen können, um automatische Benachrichtigungen einzurichten, wenn eine Amazon Aurora-Instance ohne aktivierte Verschlüsselung erstellt wird.

Aurora ist eine vollständig verwaltete, mit MySQL und PostgreSQL kompatible relationale Datenbank-Engine. Bei manchen Workloads kann Aurora einen bis zu fünfmal höheren Durchsatz als MySQL und einen bis zu dreimal höheren Durchsatz als PostgreSQL liefern, ohne dass die meisten Ihrer bestehenden Anwendungen geändert werden müssen.

Die CloudFormation Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS Lambda-Funktion. Das Ereignis verwendet AWS CloudTrail , um auf jede Aurora-Instance-Erstellung oder eine zeitpunktbezogene Wiederherstellung einer vorhandenen Instance zu überwachen. Das Cloudwatch Events-Ereignis initiiert die Lambda-Funktion, die prüft, ob die Verschlüsselung aktiviert ist. Wenn die Verschlüsselung nicht aktiviert ist, sendet die Lambda-Funktion eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung, die Sie über den Verstoß informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

Einschränkungen

- Diese Servicesteuerung funktioniert nur mit Amazon-Aurora-Instances. Es unterstützt keine anderen Amazon Relational Database Service (Amazon RDS)-Instances.
- Die CloudFormation Vorlage darf nur für `CreateDBInstance`und `RestoreDBClusterToPointInTime` bereitgestellt werden.

Produktversionen

- PostgreSQL-Versionen, die in Amazon Aurora unterstützt werden
- MySQL-Versionen, die in Amazon Aurora unterstützt werden

Architektur

Zieltechnologie-Stack

- Amazon Aurora
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation Vorlage mehrmals für verschiedene Regionen und Konten verwenden. Sie müssen sie nur einmal in jeder Region oder jedem Konto ausführen.

Tools

Tools

- Amazon Aurora – Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die mit MySQL und PostgreSQL kompatibel ist.
- AWS CloudTrail – AWS CloudTrail unterstützt Sie bei der Verwaltung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos. Aktionen eines Benutzers, einer Rolle oder eines AWS-Services werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events – Amazon CloudWatch Events liefert einen near-real-time Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung mithilfe von Lambda, HTTP, E-Mail, mobilen Push-Benachrichtigungen und mobilen Textnachrichten (SMS) bereitstellt.

Code

Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Polen

Erstellen des S3-Buckets für das Lambda-Skript

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Öffnen Sie die Amazon S3-Konsole und wählen oder erstellen Sie einen S3-Bucket . Dieser S3-Bucket hostet die ZIP-Datei des Lambda-Codes. Ihr S3-Bucket muss sich in derselben Region wie Aurora befinden. Der S3-Bucket-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Name darf keine führenden Schrägstriche enthalten.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code hoch.	Laden Sie die im Abschnitt Anhänge bereitgestellte ZIP-Datei mit dem Lambda-Code in den von Ihnen definierten S3-Bucket hoch.	Cloud-Architekt

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Stellen Sie in der - CloudFormation Konsole die `RDS_Aurora_Encryption_At_Rest.yml` CloudFormation Vorlage bereit, die als Anhang zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt

Vervollständigen der Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen des S3-Buckets an.	Geben Sie den Namen des S3-Buckets ein, den Sie im	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ersten Epos erstellt oder ausgewählt haben.	
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket ohne voranstehende Schrägstriche an (z. B. `<directory>/<file-name>.zip`).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info` bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. `Error` bezeichnet Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. `Warning` bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde,	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sendet sie eine Abonnemen t-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätige n.	

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Hochladen von Dateien in einen S3-Bucket
- Erstellen eines Amazon Aurora-DB Clusters
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen von Oracle- GoldenGate Protokollen mithilfe von Amazon CloudWatch

Erstellt von Chithra KrishnamurSpeed (AWS)

Umgebung: Produktion	Technologien: Datenbanken	Workload: Oracle
AWS-Services: Amazon CloudWatch; Amazon SNS		

Übersicht

Oracle GoldenGate bietet eine Replikation in Echtzeit zwischen Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken oder zwischen Oracle-Datenbanken, die in Amazon Elastic Compute Cloud (Amazon EC2) gehostet werden. Es unterstützt sowohl die unidirektionale als auch die bidirektionale Replikation.

Wenn Sie GoldenGate für die Replikation verwenden, ist die Überwachung von entscheidender Bedeutung, um sicherzustellen, dass der GoldenGate Prozess betriebsbereit ist, um sicherzustellen, dass die Quell- und Zieldatenbanken synchron sind.

Dieses Muster erklärt die Schritte zur Implementierung der Amazon- CloudWatch Überwachung für ein GoldenGate Fehlerprotokoll und wie Sie Alarme einrichten, um Benachrichtigungen für bestimmte Ereignisse wie `STOP` oder zu senden, `ABEND` damit Sie geeignete Maßnahmen ergreifen können, um die Replikation schnell fortzusetzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- GoldenGate ist auf einer EC2-Instance installiert und konfiguriert, sodass Sie die CloudWatch Überwachung auf diesen EC2-Instances einrichten können. Wenn Sie AWS- GoldenGate regionsübergreifend für die bidirektionale Replikation überwachen möchten, müssen Sie den CloudWatch Agenten in jeder EC2-Instance installieren, in der der GoldenGate Prozess ausgeführt wird.

Einschränkungen

- In diesem Muster wird erläutert, wie Sie den GoldenGate Prozess überwachen, indem Sie CloudWatch. CloudWatch doesn während der Replikation keine Probleme mit der Replikationsverzögerung oder Datensynchronisierung überwachen. Sie müssen separate SQL-Abfragen ausführen, um die Replikationsverzögerung oder datenbezogene Fehler zu überwachen, wie in der GoldenGate Dokumentation beschrieben.

Produktversionen

- Dieses Dokument basiert auf der Implementierung von Oracle GoldenGate 19.1.0.0.4 für Oracle unter Linux x86-64. Diese Lösung gilt jedoch für alle Hauptversionen von GoldenGate.

Architektur

Zieltechnologie-Stack

- GoldenGate Binärdateien für Oracle, die auf einer EC2-Instance installiert sind
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)

Zielarchitektur

Tools

AWS-Services

- Amazon CloudWatch ist ein Überwachungsservice, der in diesem Muster zur Überwachung von GoldenGate Fehlerprotokollen verwendet wird.
- Amazon SNS ist ein Benachrichtigungsservice, der in diesem Muster zum Senden von E-Mail-Benachrichtigungen verwendet wird.

Andere Tools

- Oracle GoldenGate ist ein Datenreplikationstool, das Sie für Datenbanken von Amazon RDS für Oracle oder für Oracle-Datenbanken verwenden können, die auf Amazon EC2 gehostet werden.

Schritte zur Implementierung auf hoher Ebene

1. Erstellen Sie eine AWS Identity and Access Management (IAM)-Rolle für den CloudWatch Agenten.
2. Fügen Sie die IAM-Rolle an die EC2-Instance an, in der GoldenGate Fehlerprotokolle generiert werden.
3. Installieren Sie den CloudWatch Agenten auf der EC2-Instance.
4. Konfigurieren Sie die CloudWatch Agentenkonfigurationsdateien: `awscli.conf` und `awslogs.conf`.
5. Starten Sie den CloudWatch Agenten.
6. Erstellen Sie Metrikfilter in der Protokollgruppe.
7. Richten Sie Amazon SNS ein.
8. Erstellen Sie einen Alarm für die Metrikfilter. Amazon SNS sendet E-Mail-Benachrichtigungen, wenn diese Filter Ereignisse erfassen.

Detaillierte Anweisungen finden Sie im nächsten Abschnitt.

Polen

Schritt 1. Erstellen einer IAM-Rolle für den CloudWatch Agenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle.	Für den Zugriff auf AWS-Ressourcen sind Berechtigungen erforderlich. Daher erstellen Sie IAM-Rollen, um die Berechtigungen einzuschließen, die für jeden Server erforderlich sind, um den CloudWatch Agenten auszuführen. So erstellen Sie die IAM-Rolle:	AWS allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/. 2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen). 3. Wählen Sie für Vertrauen swürdiger Entitätstyp die Option AWS-Service aus. 4. Wählen Sie für Häufige Anwendungsfälle EC2 und dann Weiter aus. 5. Aktivieren Sie in der Richtlinienliste das Kontrollkästchen neben CloudWatchAgentServerPolicy. Verwenden Sie ggf. das Suchfeld, um die Richtlinie zu finden. 6. Wählen Sie Weiter aus. 7. Geben Sie unter Role name (Rollenname) einen Namen für Ihre neue Rolle, wie z. B. `goldengate-cw-monitoring-role` , oder einen anderen von Ihnen bevorzugten Namen ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein. 9. Bestätigen Sie, dass unter Richtlinienname CloudWatchAgentSer verPolicy angezeigt wird. 10. (Optional) Fügen Sie ein oder mehrere Tags (Schlüssel-Wert-Paare) hinzu, um den Zugriff für diese Rolle zu organisie ren, zu verfolgen oder zu steuern, und wählen Sie dann Rolle erstellen aus.	

Schritt 2. Anfügen der IAM-Rolle an die GoldenGate EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die IAM-Rolle an die EC2-Instance an, in der GoldenGate Fehlerprotokolle generiert werden.	Die von generierten Fehlerpro tokolle GoldenGate müssen ausgefüllt CloudWatch und überwacht werden. Daher müssen Sie die IAM-Rolle , die Sie in Schritt 1 erstellt haben, an die EC2-Instance anhängen, auf der ausgeführt GoldenGate wird. So fügen Sie eine IAM-Rolle an eine Instance an:	AWS allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. 2. Wählen Sie im Navigationsbereich Instances und suchen Sie dann die Instance, in der ausgeführt GoldenGate wird. 3. Wählen Sie die Instance und dann Aktionen , Sicherheit , IAM-Rolle ändern aus. 4. Wählen Sie die im ersten Schritt erstellte IAM-Rolle aus, die an Ihre Instance angefügt werden soll, und wählen Sie dann Speichern aus.	

Schritte 3-5. Installieren und Konfigurieren des CloudWatch Agenten auf der Goldengate-EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den CloudWatch Agenten auf der GoldenGate EC2-Instance.	Führen Sie den Befehl aus, um den Agenten zu installieren: `sudo yum install -y awslogs`	AWS allgemein
Bearbeiten Sie die Agentenkonfigurationsdateien.	1. Führen Sie den folgenden Befehl aus.	AWS allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`sudo su -`
	2. Bearbeiten Sie diese Datei, um die AWS-Region nach Bedarf zu aktualisieren.
	`cat /etc/awslogs/conf`
	`[plugins]`
	`cwlogs = cwlogs`
	`[default]`
	`region = us-east-1`
	3. Bearbeiten Sie die `/etc/awslogs/awslogs.conf` Datei, um den Dateinamen, den Namen der Protokollgruppe und das Datums-/Uhrzeitformat zu aktualisieren. Sie müssen das Datum/die Uhrzeit angeben, das/die dem Datumsformat in entsprechen soll. `ggserror.log` Andernfalls fließt der Protokollstream nicht in CloudWatch. Beispielsweise:
	`datetime_format = %Y-%m-%dT%H:%M:%S%z`
	`file = /u03/oracle/oragg/ggserr.log`
	`log_group_name = goldengate_monitor`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den CloudWatch Agenten.	Verwenden Sie den folgenden Befehl, um den Agenten zu starten. `$ sudo service awslogsd start` Nachdem Sie den Agenten gestartet haben, können Sie die Protokollgruppe in der CloudWatch Konsole anzeigen. Der Protokollstream enthält den Inhalt der Datei.	AWS allgemein

Schritt 6: Erstellen von Metrikfiltern für die Protokollgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Metrikfilter für die Schlüsselwörter ABEND und STOPPED.	Wenn Sie Metrikfilter für die Protokollgruppe erstellen und die Filter im Fehlerprotokoll identifiziert werden, wird ein Alarm gestartet und eine E-Mail-Benachrichtigung basierend auf der Amazon SNS-Konfiguration gesendet. So erstellen Sie Metrikfilter: 1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/. 2. Wählen Sie den Namen der Protokollgruppe aus.	CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Aktionen und dann Metrikfilter erstellen. 4. Geben Sie für das Filtermuster ein Muster wie an`ABEND`. 5. Wählen Sie Next (Weiter) aus und geben Sie einen Namen für Ihren Metrikfilter ein. 6. Geben Sie unter Metrikdet ails für Metrik-Namespace einen Namen für den CloudWatch Namespace ein, in dem die Metrik veröffentlicht werden soll. Wenn der Namespace noch nicht vorhanden ist, stellen Sie sicher, dass Create new (Neu erstellen) ausgewählt ist. 7. Geben Sie für Metrikwer t ein`1`, da Ihr Metrikfilter Vorkommen der Schlüssel wörter im Filter zählt. 8. Setzen Sie Unit auf None . 9. Wählen Sie Metrikfilter erstellen aus. Sie finden den Metrikfilter, den Sie über den Navigatio nsbereich erstellt haben. 10. Erstellen Sie einen weiteren Metrikfilter für das `STOPPED` Muster. Innerhalb einer	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protokollgruppe können Sie mehrere Metrikfil ter erstellen und Alarme einzeln festlegen.	

Schritt 7. Einrichten von Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	In diesem Schritt konfiguri eren Sie Amazon SNS so, dass Alarme für die Metrikfilter erstellt werden. So erstellen Sie ein SNS-Thema: 1. Melden Sie sich bei der Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/home an. 2. Geben Sie im Feld Thema erstellen einen Themennam en wie ein `goldengate-alert`und wählen Sie dann Nächster Schritt aus. 3. Wählen Sie unter Type (Typ) die Option Standard aus. 4. Scrollen Sie zum Ende des Formulars und wählen Sie Create topic (Erstelle n eines Themas) aus. In	Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Konsole wird die Seite Details geöffnet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Abonnement.	So erstellen Sie ein Abonnement für das Thema: 1. Wählen Sie im linken Navigationsbereich Subscriptions (Abonnements). 2. Wählen Sie auf der Seite Subscriptions (Abonnements) die Option Create subscription (Abonnement erstellen)aus. 3. Wählen Sie auf der Seite Abonnement erstellen das Feld Themen-ARN aus, um eine Liste der Themen in Ihrem AWS-Konto anzuzeigen. 4. Wählen Sie das Mesh aus, das Sie im vorherigen Schritt erstellt haben. 5. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. 6. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen. 7. Wählen Sie Abonnement erstellen aus. Die Konsole öffnet die Seite Details des neuen Abonnements.	Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Überprüfen Sie Ihren E-Mail-Posteingang auf eine Nachricht von AWS Notifications und wählen Sie dann in der E-Mail Abonnement bestätigen aus. Amazon SNS öffnet Ihren Webbrowser und zeigt eine Abonnementbestätigung mit Ihrer Abonnement-ID an.	

Schritt 8. Erstellen eines Alarms zum Senden von Benachrichtigungen für die Metrikfilter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Alarm für das SNS-Thema.	So erstellen Sie einen Alarm basierend auf einem Protokoll gruppen-Metrikfilter: 1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/. 2. Wählen Sie ausgehend vom Navigationsbereich Logs (Protokolle) und dann Log groups (Protokollgruppen) aus. 3. Wählen Sie die Protokoll gruppe aus, die Ihren Metrikfilter enthält.	CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Metric filters (Metrikfilter) aus. 5. Aktivieren Sie auf der Registerkarte Metrikfilter das Kontrollkästchen für den Metrikfilter, auf dem Sie Ihren Alarm basieren möchten. 6. Wählen Sie Alarm erstellen aus. 7. Geben Sie für Bedingungen in jedem Abschnitt Folgendes an: • Wählen Sie für Threshold type (Schwellenwerttyp) die Option Static (Statisch) aus. • Wählen Sie für Wann immer <metric-name> ist....., Größeraus. • Geben Sie für als . . . 0 an. 8. Wählen Sie Weiter aus. 9. Unter Benachrichtigung: • Wählen Sie für Alarmstatusauslöser die Option Im Alarm aus. • Wählen Sie unter Benachrichtigung an folgendes SNS-Thema senden die Option Ein vorhandenes Thema auswählen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie im E-Mail-Feld das Amazon SNS-Thema aus, das Sie im vorherigen Schritt erstellt haben. 10. Wählen Sie Weiter aus. 11. Geben Sie unter Name und Beschreibung einen Namen und eine Beschreibung für Ihren Alarm ein. Hinweis: Für die Beschreibung können Sie den Instance-Namen angeben, damit die Benachrichtigungs-E-Mail beschreibend ist. 12. Überprüfen Sie für Vorschau und erstellen , ob Ihre Konfiguration korrekt ist, und wählen Sie dann Alarm erstellen aus. Wenn diese Muster in der von Ihnen überwachten GoldenGate Fehlerprotokolldatei (`ggserr.log`) erkannt werden, erhalten Sie nach diesen Schritten eine E-Mail-Benachrichtigung.	

Fehlerbehebung

Problem	Lösung
Der Protokollstream aus dem GoldenGate Fehlerprotokoll fließt nicht in CloudWatch.	Überprüfen Sie die `/etc/awslogs/awslogs.conf` Datei, um den Dateinamen, den Namen der Protokollgruppe und das Datums-/Uhrzeitformat zu überprüfen. Sie müssen das Datum/die Uhrzeit angeben, das/die dem Datumsformat in entsprichtgg`serror.log` . Andernfalls fließt der Protokollstream nicht in CloudWatch.

Zugehörige Ressourcen

- Amazon- CloudWatch Dokumentation
- Erfassen von Metriken und Protokollen mit dem CloudWatch Agenten
- Amazon SNS-Dokumentation

Plattformwechsel von Oracle Database Enterprise Edition auf Standard Edition 2 auf Amazon RDS für Oracle

Erstellt von Bolre showunmi (AWS) und Tarun Chawla (AWS)

Umgebung: Produktion	Quelle: On-Premises	Ziel: Amazon RDS
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Oracle Database Enterprise Edition (EE) ist eine beliebte Wahl für die Ausführung von Anwendungen in vielen Unternehmen. In einigen Fällen verwenden Anwendungen jedoch nur wenige oder keine Features von Oracle Database EE, sodass es keinen Grund für hohe Lizenzkosten gibt. Sie können Kosteneinsparungen erzielen, indem Sie diese Datenbanken bei der Migration zu Amazon RDS auf Oracle Database Standard Edition 2 (SE2) herunterstufen.

Dieses Muster beschreibt, wie Sie bei der Migration von On-Premises zu Amazon RDS für Oracle ein Downgrade von Oracle Database EE auf Oracle Database SE2 durchführen. Die in diesem Muster vorgestellten Schritte gelten auch, wenn Ihre EE Oracle-Datenbank bereits auf Amazon RDS oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance ausgeführt wird.

Weitere Informationen finden Sie im Leitfaden AWS Prescriptive Guidance zur Bewertung des Downgrades von Oracle-Datenbanken auf Standard Edition 2 in AWS .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Oracle Database Enterprise Edition
- Ein Client-Tool wie Oracle SQL Developer oder SQL*Plus zum Herstellen einer Verbindung mit und Ausführen von SQL-Befehlen in der Oracle-Datenbank
- Datenbankbenutzer für die Durchführung der Bewertung, z. B. eine der folgenden Optionen:

  - Benutzer mit ausreichenden Berechtigungen für die Ausführung der AWS Schema Conversion Tool (AWS SCT)-Bewertung
  - Benutzer mit ausreichenden Berechtigungen zum Ausführen von SQL-Abfragen für Oracle-Datenbankwörterbuchtabellen
- Datenbankbenutzer für die Durchführung der Datenbankmigration, z. B. eine der folgenden Optionen:
  - Benutzer mit ausreichenden Berechtigungen für die Ausführung von AWS Database Migration Service (AWS DMS)
  - Benutzer mit ausreichenden Berechtigungen zum Ausführen von Oracle Data Pump-Export und -Import
  - Benutzer mit ausreichenden Berechtigungen für die Ausführung von Oracle GoldenGate

Einschränkungen

- Amazon RDS für Oracle hat eine maximale Datenbankgröße. Weitere Informationen finden Sie unter Amazon-RDS-DB-Instance Speicher.

Produktversionen

Die in diesem Dokument beschriebene allgemeine Logik gilt für Oracle-Versionen ab 9i. Unterstützte Versionen von selbstverwalteten Datenbanken und Datenbanken von Amazon RDS für Oracle finden Sie in der AWS DMS-Dokumentation.

Um die Nutzung von Funktionen in Fällen zu identifizieren, in denen AWS SCT nicht unterstützt wird, führen Sie SQL-Abfragen in der Quelldatenbank aus. Um von früheren Versionen von Oracle zu migrieren, in denen AWS DMS und Oracle Data Pump nicht unterstützt werden, verwenden Sie die Oracle-Export- und Import-Dienstprogramme .

Eine aktuelle Liste der unterstützten Versionen und Editionen finden Sie unter Oracle in Amazon RDS in der AWS-Dokumentation. Einzelheiten zu Preisen und unterstützten Instance-Klassen finden Sie unter Amazon RDS für Oracle – Preise.

Architektur

Quelltechnologie-Stack

- Oracle Database Enterprise Edition wird On-Premises oder auf Amazon EC2 ausgeführt

Zieltechnologie-Stack mit nativen Oracle-Tools

- Amazon RDS for Oracle mit Oracle Database SE2

1. Exportieren Sie Daten mithilfe von Oracle Data Pump.
2. Kopieren Sie Dump-Dateien über einen Datenbanklink nach Amazon RDS.
3. Importieren Sie Dump-Dateien mithilfe von Oracle Data Pump in Amazon RDS.

Zieltechnologie-Stack mit AWS DMS

- Amazon RDS for Oracle mit Oracle Database SE2
- AWS DMS

1. Exportieren Sie Daten mithilfe von Oracle Data Pump mit FLASHBACK_SCN.
2. Kopieren Sie Dump-Dateien über einen Datenbanklink nach Amazon RDS.
3. Importieren Sie Dump-Dateien mithilfe von Oracle Data Pump in Amazon RDS.
4. Verwenden Sie AWS DMS Change Data Capture (CDC).

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud. Dieses Muster verwendet Amazon RDS für Oracle.
- AWS SCT bietet eine projektbasierte Benutzeroberfläche zum automatischen Bewerten, Konvertieren und Kopieren des Datenbankschemas Ihrer Oracle-Quelldatenbank in ein mit Amazon RDS für Oracle kompatibles Format. Mit AWS SCT können Sie potenzielle Kosteneinsparungen

analysieren, die durch die Änderung Ihres Lizenztyps von Enterprise auf Standard Edition von Oracle erzielt werden können. Der Abschnitt Lizenzbewertung und Cloud-Support des AWS SCT-Berichts enthält detaillierte Informationen zu den verwendeten Oracle-Funktionen, sodass Sie bei der Migration zu Amazon RDS für Oracle eine fundierte Entscheidung treffen können.

Andere Tools

- Native Oracle-Import- und Export-Dienstprogramme unterstützen das Verschieben von Oracle-Daten in und aus Oracle-Datenbanken. Oracle bietet zwei Arten von Datenbankimport- und Exportdienstprogrammen an: Original Export and Import (für frühere Versionen) und Oracle Data Pump Export and Import (verfügbar in Oracle Database 10g Version 1 und höher).
- Oracle GoldenGate bietet Replikationsfunktionen in Echtzeit, sodass Sie Ihre Zieldatenbank nach einem ersten Ladevorgang synchronisieren können. Diese Option kann dazu beitragen, die Ausfallzeiten von Anwendungen während der Inbetriebnahme zu reduzieren.

Polen

Durchführen einer Vormigrationsbewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Datenbank anforderungen für Ihre Anwendungen.	Stellen Sie sicher, dass Ihre Anwendungen für die Ausführung auf Oracle Database SE2 zertifiziert sind. Informieren Sie sich direkt bei dem Softwarea nbieter, Entwickler oder der Anwendungsdokumentation.	App-Entwickler, DBA, App-Besitzer
Untersuchen Sie die Verwendung von EE-Funkti onen direkt in der Datenbank.	Führen Sie einen der folgenden Schritte aus, um die Verwendung von EE-Features zu bestimmen: • Generieren Sie einen AWS SCT-Bewertungsberi	App-Besitzer, DBA, App-Entwi ckler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	cht für Ihre Oracle EE-Datenbank. Der Bericht informiert Sie darüber, welche Funktionen aus Ihrer aktuellen EE-Datenbank entfernt werden sollen, wenn Sie die Lizenztypen ändern möchten. • Wenn Sie über ein Oracle Support-Konto verfügen, rufen Sie das Skript `options_packs_usage_statistics.sql` im Support-Dokument 1317265.1 ab und führen Sie es aus, um einen Bericht über Optionen und Funktionen zu erstellen, die in Ihrer Oracle-Datenbank verwendet werden. • Fragen Sie DBA_FEATURE_USAGE_STATISTICS ab, um Details zu allen verwendeten Funktionen anzuzeigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Verwendung von EE-Funktionen für betriebliche Aktivitäten.	Datenbank- oder Anwendungsadministratoren verlassen sich manchmal auf reine EE-Funktionen für betriebliche Aktivitäten. Zu den häufigsten Beispielen gehören Online-Wartungsaktivitäten (Indexneuerstellung, Tabellenverschiebung) und die Verwendung von Parallelität durch Batch-Aufträge. Diese Abhängigkeiten können gemildert werden, indem Sie Ihre Abläufe nach Möglichkeit ändern. Identifizieren Sie die Verwendung dieser Features und treffen Sie eine Entscheidung auf der Grundlage der Kosten im Vergleich zu den Vorteilen. Verwenden Sie die Tabelle mit den Features von Oracle Database EE und SE2 als Leitfaden, um Funktionen zu identifizieren, die in Oracle Database SE2 verfügbar sind.	App-Entwickler, DBA, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Workload-Muster der EE-Oracle-Datenbank.	Oracle Database SE2 beschränkt die Nutzung automatisch auf maximal 16 CPU-Threads. Wenn Ihre Oracle EE-Datenbank für die Verwendung des Oracle Diagnostic Pack lizenziert ist, verwenden Sie das Tool Automatic Workload Repository (AWR) oder die Ansichten DBA_HIST_*, um Datenbank-Workload-Muster zu analysieren und festzustellen, ob sich die maximale Grenze von 16 CPU-Threads negativ auf die Servicelevel auswirkt, wenn Sie auf SE2 herabstufen. Stellen Sie sicher, dass Ihre Bewertung Zeiträume mit Spitzenaktivitäten abdeckt, z. B. am Ende des Tages, im Monat oder im Jahr.	App-Besitzer, DBA, App-Entwickler

Vorbereiten der Zielinfrastruktur in AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Netzwerkinfrastruktur bereit und konfigurieren Sie sie.	Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze , Sicherheitsgruppen	AWS-Administrator, Cloud-Architekt, Netzwerkadministrator, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Netzwerkzugriffskontrolllisten .	
Stellen Sie die Datenbank Amazon RDS für Oracle SE2 bereit.	Stellen Sie die Zieldatenbank von Amazon RDS für Oracle SE2 bereit, um die Leistungs-, Verfügbarkeits- und Sicherheitsanforderungen Ihrer Anwendungen zu erfüllen. Wir empfehlen die Multi-AZ-Konfiguration für Produktions-Workloads. Um die Migrationsleistung zu verbessern, können Sie die Aktivierung von Multi-AZ jedoch bis nach der Datenmigration aufschieben.	Cloud-Administrator, Cloud-Architekt, DBA, DevOps Techniker, AWS-Administrator
Passen Sie die Amazon-RDS-Umgebung an.	Konfigurieren Sie benutzerdefinierte Parameter und Optionen und aktivieren Sie zusätzliche Überwachung. Weitere Informationen finden Sie unter Bewährte Methoden für die Migration zu Amazon RDS für Oracle.	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator, DBA, Cloud-Architekt

Führen Sie den Migrations-Testlauf und die Anwendungstests durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten (Dry Run).	Migrieren Sie Daten von der Oracle EE-Quelldatenbank zur Datenbank-Instance von Amazon RDS für Oracle SE2	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit dem Ansatz, der für Ihre spezifische Umgebung am besten geeignet ist. Wählen Sie eine Migrationsstrategie aus, die auf Faktoren wie Größe, Komplexität und dem verfügbaren Ausfallzeitfenster basiert. Verwenden Sie eine oder eine Kombination der folgenden Optionen: • Native Oracle-Tools wie Oracle Data Pump (empfohlen), Oracle Import-Export-Dienstprogramme und Oracle GoldenGate. • AWS DMS unter Verwendung der Volllast mit kontinuierlicher Replikation über CDC.	
Validieren Sie die Zieldatenbank.	Führen Sie eine Validierung des Datenbankspeichers und der Codeobjekte nach der Migration durch. Überprüfen Sie die Migrationsprotokolle und beheben Sie alle identifizierten Probleme. Weitere Informationen finden Sie im Handbuch Migrieren von Oracle-Datenbanken in die AWS Cloud .	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendungen.	Anwendungs- und Datenbank administratoren sollten bei Bedarf Funktions-, Leistungs- und Betriebstests durchführen. Weitere Informationen finden Sie unter Bewährte Methoden für die Migration zu Amazon RDS für Oracle. Holen Sie sich abschließend die Abmeldung von Testergeb nissen von Stakeholdern.	App-Entwickler, App-Besitzer, DBA, Migrationsingenieur, Migrationsleiter

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Daten von Oracle Database EE.	Wählen Sie einen Ansatz zur Datenaktualisierung basierend auf der Anforderung an die Anwendungsverfügbarkeit aus. Weitere Informationen finden Sie unter Migration smethoden in Strategien für die Migration von Oracle-Da tenbanken zu AWS . Sie können beispielsweise nahezu null Ausfallzeiten erreichen, indem Sie Tools wie Oracle GoldenGate oder AWS DMS mit laufender Replikati on verwenden. Wenn das Ausfallzeitfenster dies zulässt, können Sie den endgültigen	App-Eigentümer, Cutover-Verantwortlicher, DBA, Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Daten-Cutover mit Offline-Methoden wie Oracle Data Pump oder Original-Export-Import-Dienstprogrammen durchführen.	
Verweisen Sie Anwendungen auf die Zieldatenbank-Instance.	Aktualisieren Sie die Verbindungsparameter in Anwendungen und anderen Clients so, dass sie auf die Datenbank von Amazon RDS für Oracle SE2 verweisen.	App-Entwickler, App-Besitzer, Migrationsingenieur, Migrationsleiter, Cutover-Verantwortlicher
Führen Sie Aktivitäten nach der Migration durch.	Führen Sie Aufgaben nach der Datenmigration durch, z. B. die Aktivierung von Multi-AZ, die Datenvalidierung und andere Prüfungen.	DBA, Migrationsingenieur
Führen Sie eine Überwachung nach dem Cutover durch.	Verwenden Sie Tools wie Amazon CloudWatch und Amazon RDS Performance Insights, um die Datenbank von Amazon RDS für Oracle SE2 zu überwachen.	App-Entwickler, App-Besitzer, AWS-Administrator, DBA, Migrationsingenieur

Zugehörige Ressourcen

AWS Prescriptive Guidance

- Migrieren von Oracle-Datenbanken in die AWS Cloud (Leitfaden)
- Auswerten des Downgrades von Oracle-Datenbanken auf Standard Edition 2 in AWS (Leitfaden)
- Migrieren einer On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle (Muster)
- Migrieren Sie eine On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle mit Oracle Data Pump (Muster)

Blog-Posts

- Migrieren von Oracle-Datenbanken mit nahezu Null Ausfallzeiten mit AWS DMS
- Analysieren des Leistungsmanagements in Oracle SE mit Amazon RDS für Oracle
- Verwalten Ihres SQL-Plans in Oracle SE mit Amazon RDS für Oracle
- Implementieren der Tabellenpartitionierung in Oracle Standard Edition: Teil 1

Replizieren von Mainframe-Datenbanken in AWS mithilfe von Precisely Connect

Erstellt von Lucio PereSpeed (AWS), Balaji Mohan (AWS) und Sayantan Giri (AWS)

Umgebung: Produktion	Quelle: On-Premises-Mainframe	Ziel: AWS-Datenbanken
R-Typ: Neuarchitektur	Workload: Alle anderen Workloads	Technologien: Datenbanken; Cloudnativ; Mainframe; Modernisierung
AWS-Services: Amazon DynamoDB; Amazon Keyspaces; Amazon MSK; Amazon RDS; Amazon ElastiCache		

Übersicht

Dieses Muster beschreibt die Schritte zum Replizieren von Daten aus Mainframe-Datenbanken in Amazon-Datenspeicher nahezu in Echtzeit mithilfe von Precisely Connect. Es implementiert eine ereignisbasierte Architektur mit Amazon Managed Streaming für Apache Kafka (Amazon MSK) und benutzerdefinierten Datenbank-Connectors in der Cloud, um Skalierbarkeit, Ausfallsicherheit und Leistung zu verbessern.

Precisely Connect ist ein Replikationstool, das Daten aus älteren Mainframe-Systemen erfasst und in Cloud-Umgebungen integriert. Daten werden über Change Data Capture (CDC) von Mainframes zu AWS repliziert, indem Nachrichtenflüsse nahezu in Echtzeit mit heterogenen Datenpipelines mit niedriger Latenz und hohem Durchsatz verwendet werden.

Dieses Muster deckt auch eine Notfallwiederherstellungsstrategie für belastbare Datenpipelines mit multiregionaler Datenreplikation und Failover-Routing ab.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene Mainframe-Datenbank, z. B. IBM DB2, IBM Information Management System (IMS) oder Virtual Storage Access Method (VSAM), die Sie in die AWS Cloud replizieren möchten
- Ein aktives AWS-Konto
- AWS Direct Connect oder AWS Virtual Private Network (AWS VPN) von Ihrer Unternehmensumgebung zu AWS
- Eine Virtual Private Cloud mit einem Subnetz, das von Ihrer Legacy-Plattform erreichbar ist

Architektur

Quelltechnologie-Stack

Eine Mainframe-Umgebung, die mindestens eine der folgenden Datenbanken enthält:

- IBM-IMS-Datenbank
- IBM DB2-Datenbank
- VSAM-Dateien

Zieltechnologie-Stack

- Amazon MSK
- Amazon Elastic Kubernetes Service (Amazon EKS) und Amazon EKS Anywhere
- Docker
- Eine relationale AWS- oder NoSQL-Datenbank wie die folgende:
  - Amazon DynamoDB
  - Amazon Relational Database Service (Amazon RDS) für Oracle, Amazon RDS für PostgreSQL oder Amazon Aurora
  - Amazon ElastiCache für Redis
  - Amazon Keyspaces (für Apache Cassandra)

Zielarchitektur

Replizieren von Mainframe-Daten in AWS-Datenbanken

Das folgende Diagramm veranschaulicht die Replikation von Mainframe-Daten in eine AWS-Datenbank wie DynamoDB , Amazon RDS ElastiCache, Amazon oder Amazon Keyspaces. Die

Replikation erfolgt nahezu in Echtzeit, indem Precisely Capture und Publisher in Ihrer On-Premises Mainframe-Umgebung, Precisely Dispatcher in Amazon EKS Anywhere in Ihrer On-Premises verteilten Umgebung und Precisely Apply Engine and Database Connectors in der AWS Cloud verwendet werden.

Das Diagramm zeigt den folgenden Workflow:

1. Präzise Erfassung ruft Mainframe-Daten aus CDC-Protokollen ab und verwaltet die Daten im internen vorübergehenden Speicher.
2. Präzise Herausgeber lauscht auf Änderungen im internen Datenspeicher und sendet CDC-Datensätze über eine TCP/IP-Verbindung an Precisely Dispatcher.
3. Präzise Dispatcher empfängt die CDC-Datensätze vom Publisher und sendet sie an Amazon MSK. Der Dispatcher erstellt Kafka-Schlüssel basierend auf der Benutzerkonfiguration und mehreren Worker-Aufgaben, um Daten parallel zu pushen. Der Dispatcher sendet eine Bestätigung zurück an den Publisher, wenn Datensätze in Amazon MSK gespeichert wurden.
4. Amazon MSK speichert die CDC-Datensätze in der Cloud-Umgebung. Die Partitionsgröße von Themen hängt von den Durchsatzanforderungen Ihres Transaktionsverarbeitungssystems (TPS) ab. Der Kafka-Schlüssel ist für die weitere Transformation und Transaktionsreihenfolge obligatorisch.
5. Die Precisely Apply Engine hört sich die CDC-Datensätze von Amazon MSK an und wandelt die Daten (z. B. durch Filtern oder Mapping) basierend auf den Anforderungen der Zieldatenbank um. Sie können den SQD-Skripten mit Präzision eine benutzerdefinierte Logik hinzufügen. (SQD ist die proprietäre Sprache von Precisely.) Die Precisely Apply Engine transformiert jeden CDC-Datensatz in das Apache Avro- oder JSON-Format und verteilt ihn an verschiedene Themen, je nach Ihren Anforderungen.
6. Die Ziel-Kafka-Themen enthalten CDC-Datensätze in mehreren Themen, die auf der Zieldatenbank basieren, und Kafka erleichtert die Transaktionsreihenfolge basierend auf dem definierten Kafka-Schlüssel. Die Partitionsschlüssel stimmen mit den entsprechenden Partitionen überein, um einen sequenziellen Prozess zu unterstützen.
7. Datenbank-Connectors (benutzerdefinierte Java-Anwendungen) hören die CDC-Datensätze von Amazon MSK und speichern sie in der Zieldatenbank.
8. Sie können eine Zieldatenbank basierend auf Ihren Anforderungen auswählen. Dieses Muster unterstützt sowohl NoSQL- als auch relationale Datenbanken.

Notfallwiederherstellung

Geschäftskontinuität ist der Schlüssel zum Erfolg Ihrer Organisation. Die AWS Cloud bietet Funktionen für Hochverfügbarkeit (HA) und Notfallwiederherstellung (DR) und unterstützt die Failover- und Fallback-Pläne Ihrer Organisation. Dieses Muster folgt einer aktiven/passiven DR-Strategie und bietet eine allgemeine Anleitung für die Implementierung einer DR-Strategie, die Ihren RTO- und RPO-Anforderungen entspricht.

Das folgende Diagramm veranschaulicht den DR-Workflow.

Das Diagramm zeigt Folgendes:

1. Ein halbautomatisches Failover ist erforderlich, wenn in AWS Region 1 ein Fehler auftritt. Im Falle eines Ausfalls in Region 1 muss das System Routing-Änderungen initiieren, um Precisely Dispatcher mit Region 2 zu verbinden.
2. Amazon MSK repliziert Daten durch Spiegelung zwischen Regionen. Aus diesem Grund muss der Amazon-MSK-Cluster in Region 2 während des Failovers als primärer Leader hochgestuft werden.
3. Die Precisely Apply Engine und Datenbank-Konnektoren sind zustandslose Anwendungen, die in jeder Region funktionieren können.
4. Die Datenbanksynchronisierung hängt von der Zieldatenbank ab. DynamoDB kann beispielsweise globale Tabellen und globale Datenspeicher ElastiCache verwenden.

Verarbeitung mit niedriger Latenz und hohem Durchsatz über Datenbank-Connectors

Datenbank-Konnektoren sind wichtige Komponenten in diesem Muster. Konnektoren folgen einem listenerbasierten Ansatz, um Daten von Amazon MSK zu sammeln und Transaktionen über Verarbeitung mit hohem Durchsatz und niedriger Latenz für geschäftskritische Anwendungen (Stufen 0 und 1) an die Datenbank zu senden. Das folgende Diagramm veranschaulicht diesen Prozess.

Dieses Muster unterstützt die Entwicklung einer benutzerdefinierten Anwendung mit Single-Thread-Verbrauch über eine Multi-Thread-Verarbeitungs-Engine.

1. Der Hauptthread des Konnektors verbraucht CDC-Datensätze von Amazon MSK und sendet sie zur Verarbeitung an den Thread-Pool.

2. Threads aus dem Thread-Pool verarbeiten CDC-Datensätze und senden sie an die Zieldatenbank.
3. Wenn alle Threads ausgelastet sind, werden die CDC-Datensätze von der Thread-Warteschlange in der Warteschleife gehalten.
4. Der Hauptthread wartet darauf, alle Datensätze aus der Thread-Warteschlange zu löschen, und führt Offsets in Amazon MSK aus.
5. Die untergeordneten Threads behandeln Fehler. Wenn während der Verarbeitung Fehler auftreten, werden die fehlgeschlagenen Nachrichten an das DLQ-Thema (Warteschlange für unzustellbare Nachrichten) gesendet.
6. Die untergeordneten Threads initiieren bedingte Aktualisierungen (siehe Bedingungsausdrücke in der DynamoDB-Dokumentation), basierend auf dem Mainframe-Zeitstempel, um Duplikationen oder out-of-order Aktualisierungen in der Datenbank zu vermeiden.

Informationen zur Implementierung einer Kafka-Konsumentenanwendung mit Multi-Threading-Funktionen finden Sie im Blogbeitrag Multi-Threaded Message Consumption with the Apache Kafka Consumer auf der Confluent-Website.

Tools

AWS-Services

- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- Amazon EKS Anywhere unterstützt Sie bei der Bereitstellung, Verwendung und Verwaltung von Kubernetes-Clustern, die in Ihren eigenen Rechenzentren ausgeführt werden.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- Amazon ElastiCache unterstützt Sie bei der Einrichtung, Verwaltung und Skalierung verteilter In-Memory-Cache-Umgebungen in der AWS Cloud.
- Amazon Keyspaces (für Apache Cassandra) ist ein verwalteter Datenbankservice, der Sie bei der Migration, Ausführung und Skalierung Ihrer Cassandra-Workloads in der AWS Cloud unterstützt.

Andere Tools

- Precisely Connect integriert Daten aus älteren Mainframe-Systemen wie VSAM-Datensätzen oder IBM-Mainframe-Datenbanken in Cloud- und Datenplattformen der nächsten Generation.

Bewährte Methoden

- Finden Sie die beste Kombination aus Kafka-Partitionen und Multi-Thread-Konnektoren, um optimale Leistung und Kosten auszugleichen. Mehrere Instances mit präziser Erfassung und Dispatcher können aufgrund des höheren MIPS-Verbrauchs (Millionenanweisungen pro Sekunde) die Kosten erhöhen.
- Vermeiden Sie das Hinzufügen von Datenmanipulations- und Transformationslogik zu den Datenbank-Konnektoren. Verwenden Sie dazu die Precisely Apply Engine, die Verarbeitungszeiten in Mikrosekunden bereitstellt.
- Erstellen Sie regelmäßige Anforderungs- oder Zustandsprüfungsaufrufe an die Datenbank (Heartbeats) in Datenbank-Connectors, um die Verbindung häufig aufzuwärmen und die Latenz zu reduzieren.
- Implementieren Sie eine Threadpool-Validierungslogik, um die ausstehenden Aufgaben in der Thread-Warteschlange zu verstehen und zu warten, bis alle Threads abgeschlossen sind, bevor Sie die nächste Kafka-Abfrage durchführen. Dies trägt dazu bei, Datenverlust zu vermeiden, wenn ein Knoten, Container oder Prozess abstürzt.
- Bereitstellung von Latenzmetriken über Zustandsendpunkte, um die Beobachtbarkeitsfunktionen durch Dashboards und Ablaufverfolgungsmechanismen zu verbessern.

Polen

Vorbereiten der Quellumgebung (On-Premises)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Mainframe-Prozess (Batch- oder Online-Dienstprogramm) ein, um den CDC-Prozess von Mainframe-Datenbanken aus zu starten.	1. Identifizieren Sie die Mainframe-Umgebung. 2. Identifizieren Sie die Mainframe-Datenban	Mainframe-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ken, die am CDC-Prozess beteiligt sein werden. 3. Entwickeln Sie in der Mainframe-Umgebung einen Prozess, der das CDC-Tool startet, um Änderungen in der Quelldatenbank zu erfassen. Anweisungen finden Sie in der Mainframe -Dokumentation. 4. Dokumentieren Sie den CDC-Prozess, einschlie ßlich der Konfiguration. 5. Stellen Sie den Prozess sowohl in Test- als auch in Produktionsumgebungen bereit.	
Aktivieren Sie Mainframe-Datenbank-Protokollstreams.	1. Konfigurieren Sie Protokoll streams in der Mainframe -Umgebung, um CDC-Protokolle zu erfassen. Anweisungen finden Sie in der Mainframe-Dokument ation. 2. Testen Sie die Protokoll streams, um sicherzus tellen, dass sie die erforderl ichen Daten erfassen. 3. Stellen Sie die Protokoll streams in Test- und Produktionsumgebungen bereit.	Mainframe-DB-Spezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Komponente Erfassung, um CDC-Datensätze zu erfassen.	1. Installieren und konfiguri eren Sie die Komponente Präzise Erfassung in der Mainframe-Umgebung. Anweisungen finden Sie in der Präzise Dokumentation . 2. Testen Sie die Konfigura tion, um sicherzustellen, dass die Capture-K omponente ordnungsg emäß funktioniert. 3. Richten Sie einen Replikati onsprozess ein, um die erfassten CDC-Daten sätze über die Capture-K omponente zu replizieren. 4. Dokumentieren Sie die Erfassungskonfiguration für jede Quelldatenbank. 5. Entwickeln Sie ein Überwachungssystem, um sicherzustellen, dass die Capture-Komponente im Laufe der Zeit ordnungsg emäß Protokolle erfasst. 6. Stellen Sie die Installat ion und Konfigurationen in den Test- und Produktio nsumgebungen bereit.	Mainframe-Techniker, KMU präzise verbinden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Publisher-Komponente so, dass sie die Capture-Komponente überwacht.	1. Installieren und konfigurieren Sie die Precisely Publisher-Komponente in der Mainframe-Umgebung. Anweisungen finden Sie in der Präzise Dokumentation. 2. Testen Sie die Konfiguration, um sicherzustellen, dass die Publisher-Komponente ordnungsgemäß funktioniert. 3. Richten Sie einen Replikationsprozess ein, um die CDC-Datensätze vom Herausgeber in der Precisely Dispatcher-Komponente zu veröffentlichen. 4. Dokumentieren Sie die Publisher-Konfiguration. 5. Entwickeln Sie ein Überwachungssystem, um sicherzustellen, dass die Herausgeberkomponente im Laufe der Zeit ordnungsgemäß funktioniert. 6. Stellen Sie die Installation und Konfigurationen in den Test- und Produktionsumgebungen bereit.	Mainframe-Techniker, KMU präzise verbinden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Amazon EKS Anywhere in der lokalen verteilten Umgebung bereit.	1. Installieren Sie Amazon EKS Anywhere auf der On-Premises-Infrastruktur und stellen Sie sicher, dass es ordnungsgemäß konfiguriert ist. Anweisungen finden Sie in der Dokumentation zu Amazon EKS Anywhere. 2. Richten Sie eine sichere Netzwerkumgebung für den Kubernetes-Cluster ein, einschließlich Firewalls. 3. Implementieren und testen Sie die Bereitstellung der Beispielanwendung im Amazon EKS Anywhere-Cluster. 4. Implementieren Sie automatische Skalierungsfunktionen für den Cluster. 5. Entwickeln und implementieren Sie Backup- und Notfallwiederherstellungsverfahren.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Dispatcher-Komponente in der verteilten Umgebung bereit und konfiguri eren Sie sie, um die Themen in der AWS Cloud zu veröffent lichen.	1. Konfigurieren und container isieren Sie die Precisely Dispatcher-Komponente. Anweisungen finden Sie in der Präzise Dokumentation. 2. Stellen Sie das Dispatcher-Docker-Image in der lokalen Amazon EKS Anywhere-Umgebung bereit. 3. Richten Sie eine sichere Verbindung zwischen der AWS Cloud und dem Dispatcher ein. 4. Entwickeln Sie ein Überwachungssystem, um sicherzustellen, dass die Dispatcher-Komponente im Laufe der Zeit ordnungsg emäß funktioniert. 5. Stellen Sie die Installat ion und Konfigurationen in den Test- und Produktio nsumgebungen bereit.	DevOps Techniker, KMU präzise verbinden

Vorbereiten der Zielumgebung (AWS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen Amazon EKS-Cluster in der angegeben en AWS-Region bereit.	1. Melden Sie sich bei Ihrem AWS-Konto an und konfigurieren Sie es, um sicherzustellen, dass die erforderlichen Berechtig	DevOps Techniker, Netzwerka dministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ungen zum Erstellen und Verwalten des Amazon EKS-Clusters vorhanden sind. 2. Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze in der ausgewählten AWS-Region. Anweisungen finden Sie in der Amazon-EKS-Dokumentation. 3. Erstellen und konfiguri eren Sie die erforderl ichen Netzwerksicherheit sgruppen, um die Kommunikation zwischen dem Amazon-EKS-Cluster und anderen Ressourcen in der VPC zu ermöglich en. Weitere Informationen finden Sie in der Amazon-EKS-Dokumentation. 4. Erstellen Sie den Amazon-EKS-Cluster und konfiguri eren Sie ihn mit der richtigen Knotengru ppengröße und Instance-Typen. 5. Validieren Sie den Amazon-EKS-Cluster, indem Sie eine Beispielanwendung bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen MSK-Cluster bereit und konfigurieren Sie relevante Kafka-Themen.	1. Konfigurieren Sie Ihr AWS-Konto, um sicherzustellen, dass die erforderlichen Berechtigungen zum Erstellen und Verwalten des MSK-Clusters vorhanden sind. 2. Erstellen und konfigurieren Sie die erforderlichen Netzwerksicherheitsgruppen, um die Kommunikation zwischen dem MSK-Cluster und anderen Ressourcen in der VPC zu ermöglichen. Weitere Informationen finden Sie in der Amazon-VPC-Dokumentation. 3. Erstellen Sie den MSK-Cluster und konfigurieren Sie ihn so, dass er die Kafka-Themen enthält, die von der Anwendung verwendet werden. Weitere Informationen finden Sie in der Amazon-MSK-Dokumentation.	DevOps Techniker, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Apply Engine-Komponente, um die replizierten Kafka-Themen zu hören.	1. Konfigurieren und containerisieren Sie die Komponente Precisely Apply Engine. 2. Stellen Sie das Apply Engine Docker-Image im Amazon EKS-Cluster in Ihrem AWS-Konto bereit. 3. Richten Sie die Apply Engine ein, um MSK-Themen zu hören. 4. Entwickeln und konfigurieren Sie ein SQD-Skript in der Apply Engine, um Filterung und Transformation zu bewältigen. Weitere Informationen finden Sie in der Präzise Dokumentation. 5. Stellen Sie die Apply Engine in Test- und Produktionsumgebungen bereit.	KMU präzise verbinden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie DB-Instances in der AWS Cloud bereit.	1. Konfigurieren Sie Ihr AWS-Konto, um sicherzustellen, dass die erforderlichen Berechtigungen zum Erstellen und Verwalten von DB-Clustern und -Tabellen vorhanden sind. Anweisungen finden Sie in der AWS-Dokumentation für den AWS-Datenbankservice, den Sie verwenden möchten. (Links finden Sie im Abschnitt Ressourcen.) 2. Erstellen Sie eine VPC und Subnetze in der ausgewählten AWS-Region. 3. Erstellen und konfigurieren Sie die erforderlichen Netzwerksicherheitsgruppen, um die Kommunikation zwischen den DB-Instances und anderen Ressourcen in der VPC zu ermöglichen. 4. Erstellen Sie die Datenbanken und konfigurieren Sie sie so, dass sie die Tabellen enthalten, die die Anwendung verwenden wird. 5. Entwerfen und validieren Sie die Datenbankschemata.	Dateningenieur, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und stellen Sie Datenbank-Connectors bereit, um die von der Apply Engine veröffentlichten Themen zu hören.	1. Entwerfen Sie Datenbank-Konnektoren, um die Kafka-Themen mit den AWS-Datenbanken zu verbinden , die Sie in den vorherigen Schritten erstellt haben. 2. Entwickeln Sie die Connectors basierend auf der Zieldatenbank. 3. Konfigurieren Sie die Konnektoren so, dass sie die Kafka-Themen hören, die von der Apply Engine veröffentlicht werden. 4. Stellen Sie die Konnektor en im Amazon-EKS-Cluster bereit.	App-Entwickler, Cloud-Arc hitekt, Dateningenieur

Einrichten von Geschäftskontinuität und Notfallwiederherstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie Notfallwi ederherstellungsziele für Ihre Geschäftsanwendungen.	1. Definieren Sie die RPO- und RTO-Ziele für CDC-Pipelines basierend auf Ihren Geschäftsanforderu ngen und Auswirkungen. 2. Definieren Sie die Kommunikations- und Benachrichtigungsv erfahren, um sicherzus tellen, dass alle Stakeholder	Cloud-Architekt, Dateninge nieur, App-Eigentümer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	über den Notfallwiederherstellungsplan informiert sind. 3. Bestimmen Sie das Budget und die Ressourcen, die für die Implementierung des Notfallwiederherstellungsplans erforderlich sind. 4. Dokumentieren Sie die Notfallwiederherstellungsziele, einschließlich der RPO- und RTO-Ziele.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwerfen Sie Notfallwiederherstellungsstrategien basierend auf definierten RTO/RPO.	1. Bestimmen Sie die am besten geeigneten Notfallwiederherstellungsstrategien für CDC-Pipelines basierend auf Ihren Wichtigkeits- und Wiederherstellungsanforderungen. 2. Definieren Sie die Notfallwiederherstellungsarchitektur und -topologie. 3. Definieren Sie die Failover- und Failover-Verfahren für CDC-Pipelines, um sicherzustellen, dass sie schnell und nahtlos auf die Backup-Region umgestellt werden können. 4. Dokumentieren Sie die Notfallwiederherstellungsstrategien und -verfahren und stellen Sie sicher, dass alle Stakeholder das Design klar verstehen.	Cloud-Architekt, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Cluster und Konfigurationen für die Notfallwiederherstellung bereit.	1. Stellen Sie eine sekundäre AWS-Region für die Notfallwiederherstellung bereit. 2. Erstellen Sie in der sekundären AWS-Region eine Umgebung, die mit der primären AWS-Region identisch ist. 3. Konfigurieren Sie Apache Kafka MirrorMaker zwischen der primären und der sekundären Region. Weitere Informationen finden Sie in der Amazon-MSK-Dokumentation. 4. Konfigurieren Sie Standby-Anwendungen in der sekundären Region. 5. Konfigurieren Sie Datenbankreplikationen zwischen der primären und der sekundären Region.	DevOps Ingenieur, Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die CDC-Pipeline auf Notfallwiederherstellung.	1. Definieren Sie den Umfang und die Ziele des Notfallwiederherstellungstests für die CDC-Pipeline, einschließlich der zu erreichenden Testszenarien und RTO. 2. Identifizieren Sie die Testumgebung und Infrastruktur für die Durchführung des Notfallwiederherstellungstests. 3. Bereiten Sie die Testdatensätze und das Skript vor, um Fehlerszenarien zu simulieren. 4. Überprüfen Sie die Datenintegrität und -konsistenz, um sicherzustellen, dass kein Datenverlust vorliegt.	App-Eigentümer, Dateningenieur, Cloud-Architekt

Zugehörige Ressourcen

AWS-Ressourcen

- Amazon DynamoDB
- Bedingungsausdrücke mit Amazon DynamoDB
- Amazon EKS
- Amazon EKS Anywhere
- Amazon ElasticCache
- Amazon Keyspaces
- Amazon MSK

- Amazon RDS und Amazon Aurora
- Amazon VPC

Präzise Ressourcen verbinden

- Übersicht über präzises Verbinden
- Ändern der Datenerfassung mit Precisely Connect

Confluent-Ressourcen

- Multi-Thread-Nachrichtennutzung mit dem Apache-Kafka-Verbraucher

Planen von Aufträgen für Amazon RDS for PostgreSQL und Aurora PostgreSQL mithilfe von Lambda und Secrets Manager

Erstellt von Yaser R Bol (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: PostgreSQL in AWS
R-Typ: N/A	Workload: Open-Source	Technologien: Datenbanken
AWS-Services: AWS Lambda; Amazon RDS; AWS Secrets Manager; Amazon Aurora		

Übersicht

Bei On-Premises-Datenbanken und Datenbanken, die auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances gehostet werden, verwenden Datenbankadministratoren häufig das Cron-Dienstprogramm, um Aufträge zu planen.

Beispielsweise kann ein Auftrag zur Datenextraktion oder ein Auftrag zum Bereinigen von Daten einfach mit Cron geplant werden. Für diese Aufträge werden Datenbankanmeldeinformationen in der Regel entweder fest codiert oder in einer Eigenschaftendatei gespeichert. Wenn Sie jedoch zu Amazon Relational Database Service (Amazon RDS) oder Amazon Aurora PostgreSQL -kompatible Edition migrieren, verlieren Sie die Möglichkeit, sich bei der Host-Instance anzumelden, um Cron-Aufträge zu planen.

Dieses Muster beschreibt, wie Sie AWS Lambda und AWS Secrets Manager verwenden, um Aufträge für Amazon RDS for PostgreSQL und Aurora PostgreSQL kompatible Datenbanken nach der Migration zu planen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Eine mit Amazon RDS for PostgreSQL oder Aurora PostgreSQL kompatible Datenbank

Einschränkungen

- Ein Auftrag muss innerhalb von 15 Minuten abgeschlossen werden, was dem Timeout-Limit der Lambda-Funktion entspricht. Weitere Limits finden Sie in der AWS Lambda-Dokumentation.
- Der Auftragscode muss in einer von Lambda unterstützten Sprache geschrieben werden.

Architektur

Quelltechnologie-Stack

Dieser Stack bietet Aufträge, die in Sprachen wie Bash, Python und Java geschrieben wurden. Die Datenbankanmeldeinformationen werden in der Eigenschaftendatei gespeichert und der Auftrag wird mit Linux Cron geplant.

Zieltechnologie-Stack

Dieser Stack verfügt über eine Lambda-Funktion, die die in Secrets Manager gespeicherten Anmeldeinformationen verwendet, um eine Verbindung zur Datenbank herzustellen und die Aktivität auszuführen. Die Lambda-Funktion wird im geplanten Intervall mithilfe von Amazon CloudWatch Events initiiert.

Zielarchitektur

Tools

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die Rechenzeit, die Sie verbrauchen. Es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird. Mit AWS Lambda können Sie Code für praktisch jede Art von Anwendung oder jeden Backend-Service ohne Administration ausführen. AWS Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und verwaltet alle Rechenressourcen, einschließlich Server- und Betriebssystemwartung, Kapazitätsbereitstellung und Auto Scaling, Codeüberwachung und Protokollierung. Sie müssen lediglich Ihren Code in einer der Sprachen bereitstellen, die AWS Lambda unterstützt.

- Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt. Mithilfe einfacher Regeln, die Sie schnell einrichten können, können Sie Ereignisse abgleichen und sie an eine oder mehrere Zielfunktionen oder Streams weiterleiten. CloudWatch Ereignisse erkennen betriebliche Änderungen, sobald sie auftreten. Es reagiert auf diese betrieblichen Änderungen und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um an die Umgebung zu reagieren, Funktionen zu aktivieren, Änderungen vorzunehmen und Statusinformationen zu erfassen. Sie können CloudWatch Ereignisse auch verwenden, um automatisierte Aktionen zu planen, die sich zu bestimmten Zeiten mithilfe von Cron- oder Rate-Ausdrücken selbst initiieren.
- AWS Secrets Manager hilft Ihnen, Secrets für den Zugriff auf Ihre Anwendungen, Services und IT-Ressourcen zu schützen. Sie können Datenbankanmeldeinformationen, API-Schlüssel und andere Secrets während ihres gesamten Lebenszyklus einfach rotieren, verwalten und abrufen. Benutzer und Anwendungen rufen Secrets ab, indem sie Secrets-Manager-APIs aufrufen, wodurch keine Hartcodierung sensibler Informationen im Klartext erforderlich ist. Secrets Manager bietet Secret-Rotation mit integrierter Integration für Amazon RDS, Amazon Redshift und Amazon DocumentDB. Der Service ist auf andere Arten von Secrets erweiterbar, einschließlich API-Schlüssel und OAuth-Token. Mit Secrets Manager können Sie den Zugriff auf Secrets mithilfe detaillierter Berechtigungen steuern und die Rotation von Secrets zentral für Ressourcen in der AWS Cloud, Services von Drittanbietern und On-Premises prüfen.

Polen

Speichern von Datenbankanmeldeinformationen in Secrets Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Datenbankbenutzer für die Lambda-Funktion.	Es ist eine bewährte Methode, separate Datenbankbenutzer für verschiedene Teile Ihrer Anwendung zu verwenden. Wenn bereits ein separater Datenbankbenutzer für Ihre Cron-Aufträge vorhanden ist, verwenden Sie diesen. Andernfalls erstellen Sie einen neuen Datenbankbenutzer.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Verwalten von PostgreSQL-Benutzern und -Rollen (AWS-Blogbeitrag).	
Speichern Sie Datenbank anmeldeinformationen als Secret in Secrets Manager.	Folgen Sie den Anweisung en unter Erstellen eines Datenbank-Secrets-Manager-Dokumentation).	DBA, DevOps

Erstellen des Codes für die Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine von AWS Lambda unterstützte Programmiersprache aus.	Eine Liste der unterstützten Sprachen finden Sie unter Lambda-Laufzeiten (Lambda-Dokumentation).	Developer
Schreiben Sie die Logik, um die Datenbankanmeldein formationen von Secrets Manager abzurufen.	Beispielcode finden Sie unter Sicheres Bereitstellen von Datenbankanmeldeinformation en für Lambda-Funktionen mithilfe von AWS Secrets Manager (AWS-Blogbeitrag).	Developer
Schreiben Sie die Logik, um die geplante Datenbank aktivität auszuführen.	Migrieren Sie Ihren vorhanden en Code für den Planungsa uftrag, den Sie On-Premis es verwenden, zur AWS Lambda-Funktion. Weitere Informationen finden Sie unter Bereitstellen von Lambda-Funktionen (Lambda-D okumentation).	Developer

Bereitstellen des Codes und Erstellen der Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Bereitste llungspaket für die Lambda-Fu nktion.	Dieses Paket enthält den Code und seine Abhängigk eiten. Weitere Informationen finden Sie unter Bereitste llungspakete (Lambda-D okumentation).	Developer
So erstellen Sie die Lambda-Funktion:	Wählen Sie in der AWS Lambda-Konsole Funktion erstellen aus, geben Sie einen Funktionsnamen ein, wählen Sie die Laufzeitumgebung und wählen Sie dann Funktion erstellen aus.	DevOps
Laden Sie das Bereitste llungspaket hoch.	Wählen Sie die Lambda-Fu nktion aus, die Sie erstellt haben, um ihre Konfiguration zu öffnen. Sie können Ihren Code direkt im Codeabschnitt schreiben oder Ihr Bereitste llungspaket hochladen. Um Ihr Paket hochzuladen, gehen Sie zum Abschnitt Funktionscode, wählen Sie den Eingabetyp Code aus, um eine ZIP-Datei hochzuladen, und wählen Sie dann das Paket aus.	DevOps
Konfigurieren Sie die Lambda-Funktion gemäß Ihren Anforderungen.	Sie können beispielsweise den Timeout-Parameter auf die Dauer festlegen, die Ihre Lambda-Funktion voraussic htlich in Anspruch nehmen	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird. Weitere Informationen finden Sie unter Konfigurieren von Funktionsoptionen (Lambda-Dokumentation).	
Legen Sie Berechtigungen für die Lambda-Funktionsrolle fest, um auf Secrets Manager zuzugreifen.	Anweisungen finden Sie unter Verwenden von Secrets in AWS Lambda-Funktionen (Secrets Manager-Dokumentation).	DevOps
Testen Sie die Lambda-Funktion.	Starten Sie die Funktion manuell, um sicherzustellen, dass sie wie erwartet funktioniert.	DevOps

Planen der Lambda-Funktion mithilfe von - CloudWatch Ereignissen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Regel, damit die Lambda-Funktion nach einem Zeitplan ausgeführt wird.	Planen Sie die Lambda-Funktion mithilfe von - CloudWatch Ereignissen. Anweisungen finden Sie unter Planen von Lambda-Funktionen mit CloudWatch Ereignissen (Tutorial für CloudWatch Ereignisse).	DevOps

Zugehörige Ressourcen

- AWS Secrets Manager
- Erste Schritte mit Lambda
- Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird

- AWS Lambda-Limits
- Abfragen Ihrer AWS-Datenbank von Ihrer Serverless-Anwendung (Blogbeitrag)

Sichern und optimieren Sie den Benutzerzugriff in einer Db2-Verbunddatenbank in AWS mithilfe vertrauenswürdiger Kontexte

Erstellt von Sai Parthasaradhi (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Sicherheit, Identität, Compliance	Workload: IBM
AWS-Services: Amazon EC2		

Übersicht

Viele Unternehmen migrieren ihre alten Mainframe-Workloads zu Amazon Web Services (AWS). Diese Migration umfasst die Umstellung von Datenbanken von IBM Db2 für z/OS auf Db2 für Linux, Unix und Windows (LUW) in Amazon Elastic Compute Cloud (Amazon EC2). Während einer schrittweisen Migration von On-Premises zu AWS müssen Benutzer möglicherweise auf Daten in IBM Db2 z/OS und in Db2 LUW auf Amazon EC2 zugreifen, bis alle Anwendungen und Datenbanken vollständig zu Db2 LUW migriert sind. In solchen Remote-Datenzugriffsszenarien kann die Benutzerauthentifizierung schwierig sein, da verschiedene Plattformen unterschiedliche Authentifizierungsmechanismen verwenden.

Dieses Muster behandelt, wie Sie einen Verbundserver auf Db2 für LUW mit Db2 für z/OS als Remote-Datenbank einrichten. Das Muster verwendet einen vertrauenswürdigen Kontext, um die Identität eines Benutzers von Db2 LUW auf Db2 z/OS zu übertragen, ohne sich bei der Remote-Datenbank erneut zu authentifizieren. Weitere Informationen zu vertrauenswürdigen Kontexten finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Db2-Instance, die auf einer Amazon EC2-Instance ausgeführt wird
- Eine Remote-Db2 für z/OS-Datenbank, die On-Premises ausgeführt wird

- Das On-Premises-Netzwerk, das über AWS Site-to-Site VPN oder AWS Direct Connect mit AWS verbunden ist

Architektur

Zielarchitektur

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Mit AWS Site-to-Site VPN können Sie Datenverkehr zwischen Instances, die Sie in AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleiten.

Andere -Services

- db2cli ist der interaktive Befehl der Db2-Befehlszeilenschnittstelle (CLI).

Polen

Aktivieren des Verbunds in der Db2 LUW-Datenbank, die auf AWS ausgeführt wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Verbund in der DB2-LUW-DB.	Führen Sie den folgenden Befehl aus, um den Verbund in DB2 LUW zu aktivieren. `update dbm cfg using federated YES`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die Datenbank neu.	Führen Sie den folgenden Befehl aus, um die Datenbank neu zu starten.
	`db2stop force;`
	`db2start;`
		DBA

Katalogisieren der Remote-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Katalogisieren Sie das Remote-Subsystem Db2 z/OS.	Verwenden Sie den folgenden Beispielbefehl, um die Db2 z/OS-Remote-Datenbank auf Db2 LUW zu katalogisieren, das auf AWS ausgeführt wird. `catalog TCPIP NODE tcpnode REMOTE mainframehost SERVER mainframeport`	DBA
Katalogisieren Sie die Remote-Datenbank.	Verwenden Sie den folgenden Beispielbefehl, um die Remote-Datenbank zu katalogisieren. `catalog db dbnam1 as ndbnam1 at node tcpnode`	DBA

Erstellen der Remote-Serverdefinition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfasst Benutzeranmeldeinformationen für die Db2-z/OS-Remote-Datenbank.	Sammeln Sie die folgenden Informationen, bevor Sie mit den nächsten Schritten fortfahren: • Db2 z/OS-Subsystemname – Der katalogisierte Db2 z/OS-Name in LUW aus dem vorherigen Schritt (z. B. `ndbnam1`) • Db2 z/OS-Version – Die Db2 z/OS-Subsystemversion (z. B. `12`) • Db2-z/OS-Benutzer-ID – Der Benutzer mit der BIND-Berechtigung, die benötigt wird, um nur die Serverdefinition zu erstellen (z. B. `dbuser1`) • Db2-z/OS-Passwort – Das Passwort für `dbuser1` (z. B. `dbpasswd`) • Db2-z/OS-Proxy-Benutzer – Die ID des Proxy-Benutzers, der zum Herstellen einer vertrauenswürdigen Verbindung verwendet wird (z. B. `zproxy`) • Db2-z/OS-Proxy-Passwort – Das Passwort für den `zproxy` Benutzer (z. B. `zproxy`)	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den DRDA-Wrapper.	Führen Sie den folgenden Befehl aus, um den DRDA-Wrapper zu erstellen. `CREATE WRAPPER DRDA;`	DBA
Erstellen Sie die Serverdefinition.	Führen Sie den folgenden Beispielbefehl aus, um die Serverdefinition zu erstellen. `CREATE SERVER ndbserver TYPE DB2/ZOS VERSION 12 WRAPPER DRDA AUTHORIZATION "dbuser1" PASSWORD "dbpasswd " OPTIONS ( DBNAME 'ndbnam1',FED_PROXY_USER 'ZPROXY' );` In dieser Definition `FED_PROXY_USER` gibt den Proxy-Benutzer an, der zum Herstellen vertrauenswürdiger Verbindungen mit der z/OS-Db2-Datenbank verwendet wird. Die ID und das Passwort des Autorisierungsbenutzers sind nur für die Erstellung des Remoteserverobjekts in der Db2-LUW-Datenbank erforderlich. Sie werden später während der Laufzeit nicht mehr verwendet.	DBA

Erstellen von Benutzerzuordnungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Benutzerzuordnung für den Proxy-Benutzer.	Führen Sie den folgenden Befehl aus, um eine Benutzerzuordnung für den Proxy-Benutzer zu erstellen. `CREATE USER MAPPING FOR ZPROXY SERVER ndbserver OPTIONS (REMOTE_AUTHID 'ZPROXY', REMOTE_PASSWORD 'zproxy');`	DBA
Erstellen Sie Benutzerzuordnungen für jeden Benutzer auf Db2 LUW.	Erstellen Sie Benutzerzuordnungen für alle Benutzer in der Db2 LUW-Datenbank in AWS, die über den Proxy-Benutzer auf Remote-Daten zugreifen müssen. Führen Sie den folgenden Befehl aus, um die Benutzerzuordnungen zu erstellen. `CREATE USER MAPPING FOR PERSON1 SERVER ndbserver OPTIONS (REMOTE_AUTHID 'USERZID', USE_TRUSTED_CONTEXT 'Y');` Die Anweisung gibt an, dass ein Benutzer auf Db2 LUW (PERS0N1) eine vertrauenswürdige Verbindung zur Db2-z/OS-Remote-Datenbank () herstellen kannUSE_TRUST	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ED_CONTEXT 'Y'` . Nachdem die Verbindung über den Proxy-Benutzer hergestellt wurde, kann der Benutzer mithilfe der z/OS-Benutzer-ID () von Db2 auf die Daten zugreifen`REMOTE_AUTHID 'USERZID'` .	

Erstellen des vertrauenswürdigen Kontextobjekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das vertrauenswürdige Kontextobjekt.	Verwenden Sie den folgenden Beispielbefehl, um das vertrauenswürdige Kontextobjekt in der Db2-z/OS-Remote-Datenbank zu erstellen. `CREATE TRUSTED CONTEXT CTX_LUW_ZOS BASED UPON CONNECTION USING SYSTEM AUTHID ZPROXY ATTRIBUTES ( ADDRESS '10.10.10.10' ) NO DEFAULT ROLE ENABLE WITH USE FOR PUBLIC WITHOUT AUTHENTICATION;` In dieser Definition `CTX_LUW_ZOS` ist ein beliebiger Name für das	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	vertrauenswürdige Kontextob jekt. Das Objekt enthält die Proxy-Benutzer-ID und die IP-Adresse des Servers, von dem die vertrauenswürdige Verbindung stammen muss. In diesem Beispiel der Server die Db2 LUW-Datenbank auf AWS. Sie können den Domänennamen anstelle der IP-Adresse verwenden . Die -Klausel `WITH USE FOR PUBLIC WITHOUT AUTHENTICATION` gibt an, dass das Umschalten der Benutzer-ID auf eine vertrauen swürdige Verbindung für jede Benutzer-ID zulässig ist. Ein Passwort muss nicht angegeben werden.	

Zugehörige Ressourcen

- IBM Resource Access Control facility (RACF)
- IBM-Db2-LUW-Verbund
- Vertrauenswürdige Kontexte

Zusätzliche Informationen

Vertrauenswürdige Db2-Kontexte

Ein vertrauenswürdiger Kontext ist ein Db2-Datenbankobjekt, das eine Vertrauensstellung zwischen einem Verbundserver und einem Remote-Datenbankserver definiert. Um eine Vertrauensstellung

zu definieren, gibt der vertrauenswürdige Kontext Vertrauensattribute an. Es gibt drei Arten von Vertrauensattributen:

- Die Systemautorisierungs-ID, die die erste Datenbankverbindungsanforderung stellt
- Die IP-Adresse oder der Domänenname, von der aus die Verbindung hergestellt wird
- Die Verschlüsselungseinstellung für die Datenkommunikation zwischen dem Datenbankserver und dem Datenbankclient

Eine vertrauenswürdige Verbindung wird hergestellt, wenn alle Attribute einer Verbindungsanforderung mit den Attributen übereinstimmen, die in einem vertrauenswürdigen Kontextobjekt angegeben sind, das auf dem Server definiert ist. Es gibt zwei Arten von vertrauenswürdigen Verbindungen: implizit und explizit. Nachdem eine implizite vertrauenswürdige Verbindung hergestellt wurde, erbt ein Benutzer eine Rolle, die ihm außerhalb des Bereichs dieser vertrauenswürdigen Verbindungsdefinition nicht zur Verfügung steht. Nachdem eine explizite vertrauenswürdige Verbindung hergestellt wurde, können Benutzer mit oder ohne Authentifizierung auf dieselbe physische Verbindung umgeschaltet werden. Darüber hinaus können Db2-Benutzern Rollen zugewiesen werden, die Berechtigungen angeben, die nur innerhalb der vertrauenswürdigen Verbindung verwendet werden sollen. Dieses Muster verwendet eine explizite vertrauenswürdige Verbindung.

Vertrauenswürdiger Kontext in diesem Muster

Nachdem das Muster abgeschlossen ist, greift PERSON1 auf Db2 LUW mithilfe eines vertrauenswürdigen Verbundkontexts auf Remote-Daten von Db2 z/OS zu. Die Verbindung für PERSON1 wird über einen Proxy-Benutzer hergestellt, wenn die Verbindung von der IP-Adresse oder dem Domänennamen stammt, die/der in der vertrauenswürdigen Kontextdefinition angegeben ist. Nachdem die Verbindung hergestellt wurde, wird die entsprechende Db2-z/OS-Benutzer-ID von PERSON1 ohne erneute Authentifizierung gewechselt, und der Benutzer kann auf die Daten oder Objekte zugreifen, die auf den für diesen Benutzer eingerichteten Db2-Berechtigungen basieren.

Vorteile von vertrauenswürdigen Verbundkontexten

- Bei diesem Ansatz wird das Prinzip der geringsten Berechtigung beibehalten, indem die Verwendung einer gemeinsamen Benutzer-ID oder Anwendungs-ID, die eine Obermenge aller Berechtigungen benötigen würde, die von allen Benutzern benötigt werden, vermieden wird.
- Die tatsächliche Identität des Benutzers, der die Transaktion sowohl in der Verbund- als auch in der Remote-Datenbank durchführt, ist immer bekannt und kann überprüft werden.

- Die Leistung verbessert sich, da die physische Verbindung für alle Benutzer wiederverwendet wird, ohne dass sich der Verbundserver erneut authentifizieren muss.

Senden von Benachrichtigungen für eine Datenbank-Instance von Amazon RDS für SQL Server mithilfe eines On-Premises-SMTP-Servers und Database Mail

Erstellt von Nishad Mankar (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Management und Governance	Workload: Microsoft
AWS-Services: Amazon RDS		

Übersicht

Database Mail (Microsoft-Dokumentation) sendet E-Mail-Nachrichten wie Benachrichtigungen oder Warnungen von einer Microsoft SQL Server-Datenbank unter Verwendung eines SMTP-Servers (Simple Mail Transfer Protocol). Die Dokumentation zu Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server enthält Anweisungen zur Verwendung von Amazon Simple Email Service (Amazon SES) als SMTP-Server für Database Mail. Weitere Informationen finden Sie unter Using Database Mail on Amazon RDS for SQL Server (Verwenden von Database Mail auf Amazon RDS für SQL Server). Als alternative Konfiguration erklärt dieses Muster, wie Database Mail so konfiguriert wird, dass E-Mails von einer Datenbank-Instance (DB) von Amazon RDS für SQL Server gesendet werden, indem ein On-Premises-SMTP-Server als Mail-Server verwendet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS-DB-Instance, auf der eine Standard- oder Enterprise-Edition von SQL Server ausgeführt wird
- Die IP-Adresse oder der Hostname des On-Premises-SMTP-Servers
- Eine eingehende Sicherheitsgruppenregel, die Verbindungen zur Amazon RDS for SQL Server-DB-Instance von der IP-Adresse des SMTP-Servers zulässt
- Eine Verbindung, z. B. eine AWS Direct Connect-Verbindung, zwischen Ihrem On-Premises-Netzwerk und der Virtual Private Cloud (VPC), die die Amazon RDS-DB-Instance enthält

Einschränkungen

- Express-Editionen von SQL Server werden nicht unterstützt.
- Weitere Informationen zu Einschränkungen finden Sie unter Einschränkungen in Using Database Mail on Amazon RDS for SQL Server in der Amazon-RDS-Dokumentation.

Produktversionen

- Standard- und Enterprise-Editionen von SQL Server-Versionen, die in RDS unterstützt werden

Architektur

Zieltechnologie-Stack

- Datenbank-Instance von Amazon RDS für SQL Server
- Weiterleitungsregel für Amazon Route 53
- Datenbank-E-Mail
- On-Premises-SMTP-Server
- Microsoft SQL Server Management Studio (SSMS)

Zielarchitektur

Die folgende Abbildung zeigt die Zielarchitektur für dieses Muster. Wenn ein Ereignis oder eine Aktion eintritt, die eine Benachrichtigung oder Warnung bezüglich der Datenbank-Instance auslöst, verwendet Amazon RDS for SQL Server Database Mail, um eine E-Mail-Benachrichtigung zu senden. Database Mail verwendet den On-Premises-SMTP-Server, um die E-Mail zu senden.

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) for Microsoft SQL Server unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen SQL Server-Datenbank in der AWS Cloud.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Andere Tools

- Database Mail ist ein Tool, das E-Mail-Nachrichten wie Benachrichtigungen und Warnungen von der SQL Server Database Engine an Benutzer sendet.
- Microsoft SQL Server Management Studio (SSMS) ist ein Tool zur Verwaltung von SQL Server, einschließlich Zugriff, Konfiguration und Verwaltung von SQL Server-Komponenten. In diesem Muster verwenden Sie SSMS, um die SQL-Befehle zum Einrichten von Database Mail auf einer DB-Instance von Amazon RDS für SQL Server auszuführen.

Polen

Aktivieren der Netzwerkkonnektivität mit dem On-Premises-SMTP-Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie Multi-AZ aus der RDS-DB-Instance.	Wenn Sie eine Multi-Zone-RDS-DB-Instance verwenden , konvertieren Sie die Multi-AZ-Instance in eine Single-AZ -Instance. Wenn Sie mit der Konfiguration von Database Mail fertig sind, konvertieren Sie die DB-Instance wieder in eine Multi-AZ-Bereitste llung. Die Database-Mail-Konfiguration funktioniert dann sowohl im primären als auch im sekundären Knoten. Anweisungen finden Sie unter Entfernen von Multi-AZ aus einer Microsoft SQL Server-DB-Instance.	DBA
Erstellen Sie eine Zulassung sliste für den Amazon-RDS-Endpunkt oder die IP-Adresse	Der SMTP-Server befindet sich außerhalb des AWS-Netzwerks. Erstellen Sie auf dem On-Premises-SMTP-S	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
auf dem On-Premises-SMTP-Server.	erver eine Zulassungsliste, die es dem Server ermöglicht, mit dem ausgehenden Endpunkt oder der ausgehenden IP-Adresse für die Amazon-RDS-Instance oder die Amazon Elastic Compute Cloud (Amazon EC2)-Instance zu kommunizieren, die auf Amazon RDS gehostet wird. Dieses Verfahren variiert von Organisation zu Organisation. Weitere Informationen zum Endpunkt der DB-Instance finden Sie unter Finden des Endpunkts der DB-Instance und der Portnummer .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Einschränkungen für Port 25.	Standardmäßig schränkt AWS Port 25 auf EC2-Instances ein. Gehen Sie wie folgt vor, um die Einschränkung für Port 25 zu entfernen: 1. Melden Sie sich mit Ihrem AWS-Konto an und öffnen Sie dann das Formular Anfrage zum Entfernen von E-Mail-Sendebeschränkungen. 2. Geben Sie Ihre E-Mail-Adresse ein, damit der AWS Support Sie mit Updates zu Ihrer Anfrage kontaktieren kann. 3. Geben Sie die erforderlichen Informationen im Feld Beschreibung des Anwendungsfalls ein. 4. Wählen Sie Absenden aus. Hinweis: • Wenn Sie Instances in mehr als einer AWS-Region haben, senden Sie eine separate Anforderung für jede Region. • Die Bearbeitung Ihrer Anfrage kann bis zu 48 Stunden dauern.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Route 53-Regel hinzu, um DNS-Abfragen für den SMTP-Server aufzulösen.	Verwenden Sie Route 53, um DNS-Abfragen zwischen Ihren AWS-Ressourcen und dem On-Premises-SMTP-Server aufzulösen. Sie müssen eine Regel erstellen, die die DNS-Abfragen an die SMTP-Server-Domain weiterleitet, z. B. `example.com` . Anweisungen finden Sie unter Erstellen von Weiterleitungsregeln in der Route 53-Dokumentation.	Netzwerkadministrator

Einrichten von Database Mail auf der DB-Instance von Amazon RDS für SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Database Mail.	Erstellen Sie eine Parametergruppe für Database Mail, setzen Sie den `database mail xps` Parameter auf `1`und ordnen Sie dann die Parametergruppe Database Mail der Ziel-RDS-DB-Instance zu. Anweisungen finden Sie unter Aktivieren von Database Mail in der Amazon-RDS-Dokumentation. Fahren Sie in diesen Anweisungen nicht mit dem Abschnitt Konfigurieren von Database Mail fort. Die Konfiguration für den On-Premises-SMTP-S	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erver unterscheidet sich von Amazon SES .	
Stellen Sie eine Verbindung mit der DB-Instance her.	Verwenden Sie von einem Bastion-Host aus Microsoft SQL Server Managemen t Studio (SSMS), um eine Verbindung zur Datenbank-Instance von Amazon RDS für SQL Server herzustellen. Anweisungen finden Sie unter Herstellen einer Verbindun g mit einer DB-Instance, auf der die Microsoft SQL Server-Datenbank-Engine ausgeführt wird. Wenn Sie auf Fehler stoßen, finden Sie weitere Informationen in den Referenzen zur Verbindun gsbehebung im Abschnitt Verwandte Ressourcen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Profil.	Geben Sie in SSMS die folgende SQL-Anweisung ein, um das Database-Mail-Profil zu erstellen. Ersetzen Sie die folgenden Werte: • `profile_name` Geben Sie für einen Namen für das neue Profil ein. • `description` Geben Sie für eine kurze Beschreibung des neuen Profils ein. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie unter sysmail_add_profile_sp in der Microsoft-Dokumentation. `EXECUTE msdb.dbo.sysmail_add_profile_sp @profile_name = 'SQL Alerts profile', @description = 'Profile used for sending outgoing notifications using OM SMTP Server.';`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie dem Profil Prinzipale hinzu.	Geben Sie die folgende SQL-Anweisung ein, um öffentliche oder private Prinzipale zum Database-Mail-Profil hinzuzufügen. Ein Prinzipal ist eine Entität, die SQL Server-Ressourcen anfordern kann. Ersetzen Sie die folgenden Werte: • Geben Sie für den Namen des Profils ein `profile_name`, das Sie zuvor erstellt haben. • `principal_name` Geben Sie für den Namen des Datenbankbenutzers oder der Datenbankrolle ein. Dieser Wert muss einem SQL Server-Authentifizierungsbenutzer, einem Windows-Authentifizierungsbenutzer oder einer Windows-Authentifizierungsgruppe zugeordnet werden. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie unter sysmail_add_principalprofile_sp in der Microsoft-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXECUTE msdb.dbo.sysmail_add_principalprofile_sp @profile_name = 'SQL Alerts profile', @principal_name = 'public', @is_default = 1 ;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Konto.	Geben Sie die folgende SQL-Anweisung ein, um das Database Mail-Konto zu erstellen. Ersetzen Sie die folgenden Werte: • `account_name` Geben Sie für einen Namen für das neue Konto ein. • `description` Geben Sie für eine kurze Beschreibung des neuen Kontos ein. • Geben Sie für die E-Mail-Adresse ein`email_address` , von der die Database-Mail-Nachrichten gesendet werden sollen. • Geben Sie für einen Anzeigenamen ein`display_address` , der für ausgehende Nachrichten für dieses Konto verwendet werden soll, z. B. `SQL Server Automated Notification` . Sie können auch den Wert verwenden, den Sie für eingegeben habe`email_address` . • `mailserver_name` Geben Sie für den Namen oder die IP-Adresse des SMTP-E-Mail-Servers ein.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `port`Behalten Sie für den Wert bei`25`. • Behalten Sie für den Wert bei 1 oder geben Sie ein`0`, wenn Sie nicht möchten`enable_ssl` , dass Database Mail die Kommunikation mit SSL verschlüsselt. • `username`Geben Sie für den Benutzernamen für die Anmeldung beim SMTP-E-Mail-Server ein. Wenn der Server keine Authentif izierung erfordert, geben Sie ein`NULL`. • `password`Geben Sie für das Passwort für die Anmeldung beim SMTP-E-Mail-Server ein. Wenn der Server keine Authentif izierung erfordert, geben Sie ein`NULL`. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie unter sysmail_add_accoun t_sp in der Microsoft-Dokumentation. `EXECUTE msdb.dbo. sysmail_add_accoun t_sp`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`@account_name = 'SQL Alerts account', @description = 'Database Mail account for sending outgoing notifications.', @email_address = 'xyz@example.com', @display_name = 'xyz@example.com', @mailserver_name = 'test_smtp.example.com', @port = 25, @enable_ssl = 1, @username = 'SMTP-username', @password = 'SMTP-password';`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Konto dem Profil hinzu.	Geben Sie die folgende SQL-Anweisung ein, um das Database-Mail-Konto zum Database-Mail-Profil hinzuzufügen. Ersetzen Sie die folgenden Werte: • Geben Sie für den Namen des Profils ein `profile_name`, das Sie zuvor erstellt haben. • Geben Sie für den Namen des Kontos ein `account_name`, das Sie zuvor erstellt haben. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie unter sysmail_add_profileaccount_sp in der Microsoft-Dokumentation. `EXECUTE msdb.dbo.sysmail_add_profileaccount_sp @profile_name = 'SQL Alerts profile', @account_name = 'SQL Alerts account', @sequence_number = 1;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Fügen Sie der RDS-DB-Instance Multi-AZ hinzu.	Wenn Sie Multi-AZ mit Database Mirroring (DBM) oder Always On Availabil ity Groups (AGs) hinzufüge n möchten, lesen Sie die Anweisungen unter Hinzufüge n von Multi-AZ zu einer Microsoft SQL Server-DB-Instance.	DBA

Zugehörige Ressourcen

- Verwenden von Database Mail auf Amazon RDS für SQL Server (Amazon-RDS-Dokumentation)
- Arbeiten mit Dateianhängen (Amazon-RDS-Dokumentation)
- Fehlerbehebung bei Verbindungen mit Ihrer SQL Server-DB-Instance (Amazon RDS-Dokumentation)
- Verbindung zur Amazon-RDS-DB-Instance nicht möglich (Amazon-RDS-Dokumentation)

Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten

Umgebung: Produktion	Technologien: Datenbanken; Betrieb	Arbeitslast: SAP
AWS-Services: Amazon EC2; AWS Elastic Disaster Recovery		

Übersicht

Dieses Muster beschreibt die Schritte zur Einrichtung eines Disaster Recovery-Systems (DR) für SAP-Workloads mit IBM Db2 als Datenbankplattform, das in der Amazon Web Services (AWS) Cloud ausgeführt wird. Ziel ist die Bereitstellung einer kostengünstigen Lösung zur Gewährleistung der Geschäftskontinuität im Falle eines Ausfalls.

Das Muster verwendet den Pilotlampenansatz. Durch die Implementierung von Pilot Light DR auf AWS können Sie Ausfallzeiten reduzieren und die Geschäftskontinuität aufrechterhalten. Der Pilot-Light-Ansatz konzentriert sich auf die Einrichtung einer minimalen DR-Umgebung in AWS, einschließlich eines SAP-Systems und einer Standby-Db2-Datenbank, die mit der Produktionsumgebung synchronisiert ist.

Diese Lösung ist skalierbar. Sie können sie nach Bedarf auf eine umfassende Notfallwiederherstellungsumgebung erweitern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine SAP-Instance, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance läuft
- Eine IBM Db2-Datenbank
- Ein Betriebssystem, das von der SAP Product Availability Matrix (PAM) unterstützt wird
- Verschiedene physische Datenbank-Hostnamen für Produktions- und Standby-Datenbankhosts
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket in jeder AWS-Region mit aktivierter regionsübergreifender Replikation (CRR)

Produktversionen

- IBM Db2-Datenbank Version 11.5.7 oder höher

Architektur

Zieltechnologie-Stack

- Amazon EC2
- Amazon-Simple-Storage-Service (Amazon-S3)
- Amazon Virtual Private Cloud (VPC-Peering)
- Amazon Route 53
- IBM Db2 Disaster Recovery (HADR) mit hoher Verfügbarkeit

Zielarchitektur

Diese Architektur implementiert eine DR-Lösung für SAP-Workloads mit Db2 als Datenbankplattform. Die Produktionsdatenbank wird in AWS-Region 1 bereitgestellt und eine Standby-Datenbank wird in einer zweiten Region bereitgestellt. Die Standby-Datenbank wird als DR-System bezeichnet. Db2-Datenbank unterstützt mehrere Standby-Datenbanken (bis zu drei). Es verwendet Db2 HADR für die Einrichtung der DR-Datenbank und die Automatisierung des Protokollversands zwischen der Produktions- und der Standby-Datenbank.

Im Notfall, bei dem Region 1 nicht verfügbar ist, übernimmt die Standby-Datenbank in der DR-Region die Rolle der Produktionsdatenbank. SAP-Anwendungsserver können im Voraus oder mithilfe von AWS Elastic Disaster Recovery oder einem Amazon Machine Image (AMI) erstellt werden, um die RTO-Anforderungen (Recovery Time Objective) zu erfüllen. Dieses Muster verwendet ein AMI.

Db2 HADR implementiert ein Produktions-Standby-Setup, bei dem die Produktion als primärer Server fungiert und alle Benutzer mit ihm verbunden sind. Alle Transaktionen werden in Protokolldateien geschrieben, die mithilfe von TCP/IP auf den Standby-Server übertragen werden. Der Standby-Server aktualisiert seine lokale Datenbank, indem er die übertragenen Protokolldatensätze weiterleitet. Dadurch wird sichergestellt, dass die Datenbank mit dem Produktionsserver synchron bleibt.

VPC-Peering wird verwendet, damit Instances in der Produktionsregion und der DR-Region miteinander kommunizieren können. Amazon Route 53 leitet Endbenutzer zu Internetanwendungen weiter.

1. Erstellen Sie ein AMI des Anwendungsservers in Region 1 und kopieren Sie das AMI in Region 2. Verwenden Sie das AMI, um im Notfall Server in Region 2 zu starten.
2. Richten Sie die Db2-HADR-Replikation zwischen der Produktionsdatenbank (in Region 1) und der Standby-Datenbank (in Region 2) ein.
3. Ändern Sie den EC2-Instance-Typ so, dass er im Notfall mit der Produktionsinstanz übereinstimmt.
4. In Region 1 `LOGARCHMETH1` ist auf `db2remote: S3 path` eingestellt.
5. In Region 2 `LOGARCHMETH1` ist auf gesetzt`db2remote: S3 path`.
6. Die regionsübergreifende Replikation wird zwischen den S3-Buckets durchgeführt.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS. Dieses Muster verwendet VPC-Peering.

Bewährte Methoden

- Das Netzwerk spielt eine Schlüsselrolle bei der Entscheidung über den HADR-Replikationsmodus. Für DR in allen AWS-Regionen empfehlen wir, den Modus Db2 HADR ASYNC oder SUPERASYNC zu verwenden.
- Weitere Informationen zu den Replikationsmodi für Db2 HADR finden Sie in der IBM-Dokumentation.
- Sie können die AWS-Managementkonsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden, um ein neues AMI Ihres vorhandenen SAP-Systems zu erstellen. Anschließend

können Sie das AMI verwenden, um Ihr vorhandenes SAP-System wiederherzustellen oder einen Clone zu erstellen.

- AWS Systems Manager Automation kann Sie bei den allgemeinen Wartungs- und Bereitstellungsaufgaben von EC2-Instances und anderen AWS-Ressourcen unterstützen.
- AWS bietet mehrere native Services zur Überwachung und Verwaltung Ihrer Infrastruktur und Anwendungen auf AWS. Dienste wie Amazon CloudWatch und AWS CloudTrail können verwendet werden, um Ihre zugrunde liegende Infrastruktur bzw. API-Operationen zu überwachen. Weitere Informationen finden Sie unter SAP on AWS — IBM Db2 HADR with Pacemaker.

Epen

Bereite die Umgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das System und die Protokolle.	1. Vergewissern Sie sich, dass das Produktionssystem SAP auf Db2 eingerichtet ist. 2. Vergewissern Sie sich, dass die Protokollsicherung aktiviert und so konfiguriert ist, dass die Protokolle im S3-Bucket gespeichert werden. Dies kann mit dem Db2-Parameter `LOGARCHMETH1` überprüft werden. 3. Erstellen Sie ein AMI des zusätzlichen Anwendungsservers.	AWS-Administrator, SAP-Basisadministrator

Richten Sie die Server und die Replikation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die SAP- und Datenbankserver.	1. Um die Infrastruktur für die DR-Region bereitzustellen, verwenden Sie ein CloudFormation AWS-Skript oder verwenden Sie ein AMI der Produktionsinstanz. Im Rahmen des Pilotprojekts können Sie eine kleinere EC2-Instance in derselben Familie wie die Produktionsinstanz verwenden. Wenn Ihr Produktions-Instance-Typ beispielsweise ist `r6i.12xlarge`, können Sie den `r6i.xlarge` Instance-Typ für den DR-Build verwenden. Stellen Sie jedoch sicher, dass Sie der DR-Instance dieselbe Speicherkapazität zuweisen, um das Backup der Produktionsdatenbank wiederherzustellen. 2. Erstellen Sie Bereitstellungspunkte für `/sapmnt/<SID>/` das Amazon Elastic File System (Amazon EFS) und stellen Sie sicher, dass die	SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Replikation vom Primärsystem aus konfiguriert ist. 3. Erstellen Sie ein VOLLSTÄNDIGES Datenbank-Backup (online oder offline) vom Produktionssystem. Sie werden dieses Backup verwenden, um die DR-Datenbank zu erstellen. 4. Verwenden Sie im DR-System die Systemkopiermethode SAP Software Provisioning Manager (SWPM) mit der Option Systemkopie mit Sicherung/Wiederherstellung für HA/DR-Zwecke verwenden, um das DR-SAP-System zu erstellen. 5. Wenn Sie von SWPM dazu aufgefordert werden, stellen Sie die Datenbank in DR mit dem Backup wieder her, das Sie aus der Produktion erstellt haben. Die DR-Datenbank wird sich im Status „Rollforward ausstehend“ befinden. Der Status „Rollforward ausstehend“ ist standardmäßig festgelegt, nachdem die vollständige Sicherung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wiederhergestellt wurde. Der Status „Rollforward ausstehend“ gibt an, dass die Datenbank gerade wiederhergestellt wird und dass möglicherweise einige Änderungen übernommen werden müssen. Weitere Informationen finden Sie in der IBM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Konfiguration.	1. Um die Protokollarchivierung für HADR einzurichten, müssen sowohl die Produktions- als auch die DR-Datenbank in der Lage sein, Protokolle automatisch von allen Protokollarchivspeicherorten abzurufen. Stellen Sie sicher, dass der `LOGARCHMETH1` Parameter in der DR-Datenbank auf denselben Speicherort wie in der Produktionsdatenbank gesetzt ist. Wenn auf denselben Standort aufgrund regionaler Beschränkungen nicht zugegriffen werden kann, stellen Sie sicher, dass das DR-System automatisch Protokolle vom Primärsystem abrufen kann. 2. Um TCP/IP-Ports für die Aktivierung der Datenbankreplikation zu aktivieren, ändern Sie `/etc/services` die Produktions- und DR-Hosts, indem Sie die folgenden beiden Einträge hinzufügen. `<SID>`Bezieht sich im Code auf die System-ID (SID) der Db2-Datenbank (z. B.). `PR1`	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<SID>_HADR_1 55001/tcp # DB2 HADR Port1 <SID>_HADR_2 55002/tcp # DB2 HADR Port2 Vergewissern Sie sich, dass beide Ports eingehenden und ausgehenden Verkehr zwischen dem Primär- und dem Standby-Port zulassen. 3. Überprüfen Sie `/etc/hosts` die Produktions- und DR-Hosts, um sicherzustellen, dass die Hostnamen sowohl für die Produktions- als auch für die Standby-Hosts auf die richtigen IP-Adressen verweisen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die Replikation von der Produktions-Datenbank zur DR-DB ein (im ASYNC-Modus).	1. Führen Sie in der Produktionsdatenbank die folgenden Befehle aus, um die Parameter zu aktualisieren.
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	2. Führen Sie in der DR-Datenbank die folgenden
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Befehle aus, um die Parameter zu aktualisieren.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	Diese Parameter sind erforderlich, um HADR-bezogene Informationen für beide Datenbanken bereitzustellen. In der Db2-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Datenbank wird HADR auf der Grundlage der Werte für jeden der zuvor festgeleg ten Parameter aktiviert. Weitere Informationen zu diesen Parametern finden Sie in der IBM-Dokum entation.
	3. Starten Sie HADR zunächst in der neu erstellten Standby-Datenbank, indem Sie den folgenden Befehl verwenden.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as standby`
	4. Starten Sie HADR in der Produktionsdatenbank mit dem folgenden Befehl.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as primary`
	5. Überprüfen Sie, ob die Produktions- und Standby-Db2-Datenbanken synchron sind und ob der Protokoll versand läuft.
	Verwenden Sie den folgenden db2pd Befehl, um den HADR-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Replikationsstatus zu überwachen. `db2pd -d <SID> -hadr` Weitere Informationen zur Überwachung von HADR finden Sie in der IBM-Dokumentation.	

Testen Sie DR-Failover-Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie die Ausfallzeiten des Produktionsbetriebs für den DR-Test ein.	Stellen Sie sicher, dass Sie die erforderlichen Betriebsausfälle in der Produktionsumgebung einplanen, um das DR-Failover-Szenario zu testen.	SAP-Basisadministrator
Erstellen Sie einen Testbenutzer.	Erstellen Sie einen Testbenutzer (oder beliebige Teständerungen), der auf dem DR-Host validiert werden kann, um die Protokollreplikation nach einem DR-Failover zu bestätigen.	SAP-Basisadministrator
Stoppen Sie auf der Konsole die EC2-Produktionsinstanzen.	In diesem Schritt wird ein unsachgemäßes Herunterfahren eingeleitet, um ein Katastrophenszenario nachzuahmen.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Skalieren Sie die DR EC2-Instance entsprechend den Anforderungen.	Ändern Sie auf der EC2-Konsole den Instance-Typ in der DR-Region. 1. Stoppen Sie die Instance: Wenn die Instance läuft, müssen Sie sie beenden, bevor Sie ihren Instance-Typ ändern können. Wählen Sie auf der EC2-Konsole die Instance aus und klicken Sie auf Stop. 2. Ändern Sie den Instance-Typ: Wählen Sie auf der EC2-Konsole die Instance aus und wählen Sie Actions, Instance Settings, Change Instance Type aus. Wählen Sie den Instance-Typ aus, der der primären Instance entspricht, und klicken Sie auf Apply. 3. Starten Sie die Instance: Nachdem die Änderung des Instance-Typs abgeschlossen ist, starten Sie die Instance von der EC2-Konsole aus, indem Sie die Instance auswählen und Start wählen. 4. Verwenden Sie den folgenden Befehl, um die Db2-Datenbank zu starten.	SAP-Basis-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`db2start`
	`    db2 start HADR on`
	` db <SID> as standby`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übernahme einleiten.	Initiieren Sie vom DR-System (`host2`) aus den Übernahme prozess und rufen Sie die DR-Datenbank als primäre Datenbank auf.
	`db2 takeover hadr on database <SID> by force`
	Optional können Sie die folgenden Parameter festlegen , um die Speicherzuweisung der Datenbank automatis ch auf der Grundlage des Instance-Typs anzupassen. Der `INSTANCE_MEMORY` Wert kann auf der Grundlage des dedizierten Speicherb ereichs festgelegt werden, der der Db2-Datenbank zugewiesen werden soll.
	`db2 update db cfg for <SID> using INSTANCE_MEMORY <FIXED VALUE> IMMEDIATE;`
	`db2 get db cfg for <SID> | grep -i DATABASE_MEMORY AUTOMATIC IMMEDIATE;`
	`db2 update db cfg for <SID> using self_tuning_mem ON IMMEDIATE;`
	Überprüfen Sie die Änderung mithilfe der folgenden Befehle.
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`db2 get db cfg for <SID> | grep -i MEMORY` `db2 get db cfg for <SID> | grep -i self_tuning_mem`	
Starten Sie den Anwendungsserver für SAP in der DR-Region.	Starten Sie mithilfe des AMI, das Sie aus dem Produktionssystem erstellt haben, einen neuen zusätzlichen Anwendungsserver in der DR-Region.	SAP-Basisadministrator
Führen Sie eine Validierung durch, bevor Sie die SAP-Anwendung starten.	1. Validieren Sie die `/etc/fstab` Einträge `/etc/hosts` und. 2. `/sapmnt/<SID>/` Auf dem DR-System montieren. 3. Stellen Sie sicher, dass das DR-Dateisystem mit der Produktion `/sapmnt/<SID>/` synchronisiert `/sapmnt/<SID>/` ist. 4. Melden Sie sich beim `<sid>adm` Benutzer an`R3trans -d`, führen Sie die Ausführung aus und überprüfen Sie die Ausgabe in der `trans.log` Datei. Die `trans.log` Datei wird an derselben Stelle generiert, an der Sie den `R3trans -d` Befehl ausgeführt haben.	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die SAP-Anwendung auf dem DR-System.	Starten Sie die SAP-Anwendung auf dem DR-System mithilfe von `<sid>adm` user. Verwenden Sie den folgenden Code, der die XX Instanznummer Ihres SAP ABAP SAP Central Services (ASCS) -Servers und die Instanznummer Ihres SAP-Anwendungsservers YY darstellt.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
		SAP-Basisadministrator

Führen Sie die SAP-Validierung durch.	Dies wird als DR-Test durchgeführt, um Beweise zu liefern oder um den Erfolg der Datenreplikation in die DR-Region zu überprüfen.	Testingenieur

Führen Sie DR-Failback-Aufgaben durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Produktions-SAP- und Datenbankserver.	Starten Sie auf der Konsole die EC2-Instances, die	SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SAP und die Datenbank im Produktionssystem hosten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die Produktionsdatenbank und richten Sie HADR ein.	Melden Sie sich beim Produktionssystem (`host1`) an und stellen Sie mithilfe des folgenden Befehls sicher, dass sich die Datenbank im Wiederherstellungsmodus befindet.
	`db2start`
	`db2 start HADR on db P3V as standby`
	`db2 connect to <SID>`
	Stellen Sie sicher, dass der HADR-Status lautet`connected` . Der Replikationsstatus sollte sein. `peer`
	`db2pd -d <SID> -hadr`
	Wenn die Datenbank nicht inkonsistent ist und sich nicht im `connected peer` Status N befindet, sind möglicher weise eine Sicherung und Wiederherstellung erforderl ich, um die Datenbank mit der aktuell aktiven Datenbank (`host2`in der DR-Region) zu synchronisieren (aktiviert). `host1` Stellen Sie in diesem Fall das DB-Backup aus der Datenbank in der `host2` DR-Region auf die Datenbank in
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der `host1` Produktionsregion wieder her.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie ein Failback der Datenbank auf die Produktio nsregion durch.	In einem normalen business-as-usual Szenario wird dieser Schritt während einer geplanten Ausfallze it ausgeführt. Anwendung en, die auf dem DR-System ausgeführt werden, werden gestoppt, und für die Datenbank wird ein Failback in die Produktionsregion (Region 1) durchgeführt, um den Betrieb von der Produktionsregion aus wieder aufzunehmen. 1. Melden Sie sich beim SAP-Anwendungsserver in der DR-Region an und beenden Sie die SAP-Anwendung. 2. Trennen Sie die `/sapmnt/<SID>` Installation vom DR-System und stellen Sie sicher, dass die Änderunge n auf das Produktio nssystem rückwirke nd repliziert werden. `/sapmnt/<SID>` 3. Melden Sie sich beim Datenbankserver (`host1`) in der Produktionsregion an, und führen Sie die Übernahme durch.	SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`db2 takeover hadr on database <SID>`
	4. Überprüfen Sie den HADR-Status: `HADR_ROLE` sollte aktiviert `host1` und `PRIMARY StandBy` aktiviert `host2` sein.
	`db2pd -d <SID> -hadr`	

Führen Sie eine Validierung durch, bevor Sie die SAP-Anwendung starten.	1. Validieren Sie die `/etc/fstab` Einträge `/etc/hosts` und. 2. `/sapmnt/<SID>/` Auf dem Produktionssystem montieren. 3. Stellen Sie sicher, dass es mit dem DR-System synchronisiert ist`/sapmnt/<SID>/` . 4. Melden Sie sich beim `<sid>adm` Benutzer an`R3trans -d`, führen Sie die `trans.log` Datei aus und überprüfen Sie die Ausgabe. Die `trans.log` Datei wird an derselben Stelle generiert, an der Sie den `R3trans -d` Befehl ausgeführt haben.	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die SAP-Anwendung.	1. Starten Sie die SAP-Anwendung auf dem Produktionssystem mit dem `<sid>adm` Benutzer. Verwenden Sie den folgenden Code, der die XX Instanznummer Ihres SAP ASCS-Servers und die Instanznummer Ihres SAP-Anwendungsservers YY darstellt.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
	2. Um zu überprüfen, ob Anwendungsserver verfügbar sind, melden Sie sich bei SAP an und führen Sie mithilfe der SICK- und SM51-Transaktionen Prüfungen durch.
		SAP-Basisadministrator

Fehlerbehebung

Problem	Lösung
Wichtige Protokolldateien und Befehle zur Behebung von Problemen im Zusammenhang mit HADR	• `db2 get db cfg | grep -i hadr` • `db2pd -d sid -hadr` • `Db2diag.log` (Diese Datei befindet sich in der Regel innerhalb des `db2dump` Verzeichnisses, und der `db2dump` Pfad wird durch den Parameter `DIAGPATH` definiert.)
SAP-Hinweis zur Behebung von HADR-Problemen auf Db2 UDB	Weitere Informationen finden Sie im SAP-Hinweis 1154013 — DB6: DB-Probleme in der HADR-Umgebung. (Sie benötigen Anmeldeinformationen für das SAP-Portal, um auf diesen Hinweis zugreifen zu können.)

Zugehörige Ressourcen

- Ansätze zur Notfallwiederherstellung für Db2-Datenbanken auf AWS (Blogbeitrag)
- SAP on AWS — IBM Db2 HADR mit Pacemaker
- Schrittweises Verfahren zum Einrichten der HADR-Replikation zwischen DB2-Datenbanken
- Db2 HADR Wiki

Zusätzliche Informationen

Mit diesem Muster können Sie ein Disaster-Recovery-System für ein SAP-System einrichten, das auf der Db2-Datenbank läuft. In einer Notfallsituation sollte das Geschäft in der Lage sein, die von Ihnen definierten Anforderungen an das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) einzuhalten:

- RTO ist die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes. Dies bestimmt, welches Zeitfenster als akzeptables Zeitfenster angesehen wird, wenn der Dienst nicht verfügbar ist.

- RPO ist die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Häufig gestellte Fragen zu HADR finden Sie in SAP-Hinweis #1612105 — DB6: Häufig gestellte Fragen zu Db2 High Availability Disaster Recovery (HADR). (Sie benötigen Zugangsdaten für das SAP-Portal, um auf diesen Hinweis zugreifen zu können.)

Einrichten einer HA/DR-Architektur für Oracle E-Business Suite in Amazon RDS Custom mit einer aktiven Standby-Datenbank

Erstellt von Cunningham (AWS) und Nitin Saxena

Umgebung: Produktion	Technologien: Datenbanken; Infrastruktur	Workload: Oracle
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster beschreibt, wie Sie Ihre Oracle-E-Business-Lösung auf Amazon Relational Database Service (Amazon RDS) Custom für Hochverfügbarkeit (HA) und Notfallwiederherstellung (DR) entwerfen können, indem Sie eine Amazon-RDS-Custom-Read Replica-Datenbank in einer anderen Availability Zone von Amazon Web Services (AWS) einrichten und sie in eine aktive Standby-Datenbank konvertieren. Die Erstellung des Amazon RDS Custom Read Replica ist über die AWS-Managementkonsole vollständig automatisiert.

Dieses Muster behandelt nicht die Schritte zum Hinzufügen zusätzlicher Anwendungsebenen und gemeinsam genutzter Dateisysteme, die auch Teil einer HA/DR-Architektur sein können. Weitere Informationen zu diesen Themen finden Sie in den folgenden Oracle Support Notes: 1375769.1, 1375670.1 und 1383621.1 (Abschnitt 5, Erweiterte Klonoptionen). (Zugriff erfordert ein Oracle Support-Konto.)

Informationen zur Migration des E-Business-Suite-Systems zu einer Single-AZ-Architektur mit einer Ebene auf Amazon Web Services (AWS) finden Sie im Muster Migrieren der Oracle E-Business Suite zu Amazon RDS Custom.

Oracle E-Business Suite ist eine Enterprise Resource Planning (ERP)-Lösung zur Automatisierung unternehmensweiter Prozesse wie Finanzen, Personalwesen, Lieferketten und Fertigung. Es verfügt über eine dreistufige Architektur: Client, Anwendung und Datenbank. Zuvor mussten Sie Ihre E-Business-Suite-Datenbank auf einer selbstverwalteten Amazon Elastic Compute Cloud (Amazon EC2)-Instance ausführen, aber Sie können jetzt von Amazon RDS Custom profitieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene E-Business-Suite-Installation auf Amazon RDS Custom; siehe das Muster Migrieren von Oracle E-Business Suite zu Amazon RDS Custom
- Wenn Sie das Lesereplikat auf schreibgeschützt ändern und es zum Auslagern von Berichten in den Standby-Modus, eine Datenbanklizenz von Oracle Active Data Guard, verwenden möchten (siehe kommerzielle Preisliste von Oracle Technology)

Einschränkungen

- Einschränkungen und nicht unterstützte Konfigurationen für Oracle-Datenbanken in Amazon RDS Custom
- Einschränkungen im Zusammenhang mit Lesereplikaten von Amazon RDS Custom für Oracle

Produktversionen

Informationen zu Oracle Database-Versionen und Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Anforderungen und Einschränkungen für Amazon RDS Custom für Oracle.

Architektur

Das folgende Diagramm zeigt eine repräsentative Architektur für E-Business Suite in AWS, die mehrere Availability Zones und Anwendungsebenen in einer aktiven/passiven Einrichtung enthält. Die Datenbank verwendet eine Amazon RDS Custom DB-Instance und ein Amazon RDS Custom Read Replica. Das Lesereplikat verwendet Active Data Guard, um in eine andere Availability Zone zu replizieren. Sie können das Lesereplikat auch verwenden, um Lesedatenverkehr in der Primärdatenbank auszulagern und zu Berichtszwecken.

Weitere Informationen finden Sie unter Arbeiten mit Lesereplikaten für Amazon RDS Custom für Oracle in der Amazon-RDS-Dokumentation.

Das Amazon RDS Custom Read Replica wird standardmäßig wie gemountet erstellt. Wenn Sie jedoch einige Ihrer schreibgeschützten Workloads in die Standby-Datenbank auslagern möchten,

um die Belastung Ihrer Primärdatenbank zu reduzieren, können Sie den Modus der aufgespielten Replikate manuell in schreibgeschützt ändern, indem Sie die Schritte im Abschnitt „Epics“ befolgen. Ein typischer Anwendungsfall dafür wäre die Ausführung Ihrer Berichte aus der Standby-Datenbank. Für den Wechsel zu schreibgeschützt ist eine aktive Standby-Datenbanklizenz erforderlich.

Wenn Sie ein Lesereplikat in AWS erstellen, verwendet das System den Oracle Data Guard-Broker unter den -Abdeckungen. Diese Konfiguration wird automatisch generiert und im Modus Maximale Leistung wie folgt eingerichtet:

```
DGMGRL> show configuration
Configuration - rds_dg
  Protection Mode: MaxPerformance
  Members:
  vis_a - Primary database
    vis_b - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS   (status updated 58 seconds ago)
```

Tools

AWS-Services

- Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Es automatisiert Aufgaben und Vorgänge der Datenbankverwaltung und ermöglicht Ihnen als Datenbankadministrator den Zugriff auf und die Anpassung Ihrer Datenbankumgebung und Ihres Betriebssystems.

Andere Tools

- Oracle Data Guard ist ein Tool, mit dem Sie Standby-Datenbanken von Oracle erstellen und verwalten können. Dieses Muster verwendet Oracle Data Guard, um eine aktive Standby-Datenbank auf Amazon RDS Custom einzurichten.

Polen

Erstellen eines Lesereplikats

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Lesereplikat der Amazon RDS Custom DB-Instance.	Um ein Lesereplikat zu erstellen, folgen Sie den Anweisungen in der Amazon-RDS-Dokumentation und verwenden Sie die von Ihnen erstellte Amazon-RDS-Custom-DB-Instance (siehe Abschnitt Voraussetzungen) als Quelldatenbank. Standardmäßig wird das Amazon RDS Custom Read Replica als physischer Standby erstellt und befindet sich im aufgespielten Zustand. Dies dient dazu, die Einhaltung der Oracle Active Data Guard-Lizenz sicherzustellen. Führen Sie die nächsten Schritte aus, um das Lesereplikat in den schreibgeschützten Modus zu konvertieren.	DBA

Ändern des Lesereplikats in einen schreibgeschützten aktiven Standby-Modus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung mit dem Amazon RDS Custom Read Replica her.	Verwenden Sie die folgenden Befehle, um Ihre physische Standby-Datenbank in eine	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	aktive Standby-Datenbank zu konvertieren.
	
	Wichtig: Für diese Befehle ist eine aktive Standby-L izenz von Oracle erforderlich. Um eine Lizenz zu erhalten, wenden Sie sich an Ihren Oracle-Mitarbeiter.
	
	`$ sudo su - rdsdb`
	`-bash-4.2$ sql`
	`SQL> select process,s tatus,sequence# from v $managed_standby;`
	
	`PROCESS STATUS SEQUENCE#`
	`--------- ------------ ----------`
	`ARCH CLOSING 3956`
	`ARCH CONNECTED 0`
	`ARCH CLOSING 3955`
	`ARCH CLOSING 3957`
	`RFS IDLE 0`
	`RFS IDLE 3958`
	`MRP0 APPLYING_LOG 3958`
	`SQL> select name, database_role, open_mode from v $database;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	NAME DATABASE_ ROLE OPEN_MODE --------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY MOUNTED SQL> alter database recover managed standby database cancel; Database altered. Open the standby database SQL> alter database open; Database altered. SQL> select name, database_role, open_mode from v $database; NAME DATABASE_ ROLE OPEN_MODE --------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY READ ONLY	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die Medienwie derherstellung mit Anwendung von Echtzeitprotokollen.	Verwenden Sie die folgenden Befehle, um die Funktion zur Protokollanwendung in Echtzeit zu aktivieren. Diese konvertieren und validieren den Standby (Lesereplikat) als aktive Standby-Datenbank, sodass Sie schreibgeschützte Abfragen verbinden und ausführen können.
	`SQL>  alter database recover managed standby database using current logfile disconnect from session;`
	`Database altered`
		DBA

Überprüfen Sie den Datenbankstatus.	Verwenden Sie den folgenden Befehl, um den Status der Datenbank zu überprüfen.
	`SQL> select name, database_role, open_mode from v$database;`
	`NAME DATABASE_ROLE OPEN_MODE`
	`--------- ---------- ----------`
	`VIS PHYSICAL STANDBY READ ONLY WITH APPLY`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie den Wiederholungsanwendungsmodus.	Verwenden Sie den folgenden Befehl, um den Redo-Anwendungsmodus zu überprüfen.
	
	`SQL> select process,status,sequence# from v$managed_standby;`
	`PROCESS STATUS SEQUENCE#`
	`--------- ------------ ----------`
	`ARCH CLOSING 3956`
	`ARCH CONNECTED 0`
	`ARCH CLOSING 3955`
	`ARCH CLOSING 3957`
	`RFS IDLE 0`
	`RFS IDLE 3958`
	`MRP0 APPLYING_LOG 3958`
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`READ ONLY WITH APPLY`
		DBA

Zugehörige Ressourcen

- Migrieren Sie Oracle E-Business Suite zu Amazon RDS Custom (AWS Prescriptive Guidance)
- Arbeiten mit Amazon RDS Custom (Amazon-RDS-Dokumentation)
- Arbeiten mit Lesereplikaten für Amazon RDS Custom for Oracle (Amazon-RDS-Dokumentation)

- Amazon RDS Custom für Oracle – Neue Kontrollfunktionen in der Datenbankumgebung (AWS-News-Blog)
- Migrieren der Oracle E-Business Suite in AWS (AWS-Whitepaper)
- Oracle E-Business Suite-Architektur in AWS (AWS-Whitepaper)

Einrichten der Datenreplikation zwischen Amazon RDS für MySQL und MySQL auf Amazon EC2 mithilfe von GTID

Erstellt von Rajesh Madiwale (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken	Workload: Open-Source

Übersicht

Dieses Muster beschreibt, wie Sie die Datenreplikation in der Amazon Web Services (AWS) Cloud zwischen einer Amazon Relational Database Service (Amazon RDS) for MySQL-DB-Instance und einer MySQL-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance mithilfe der nativen globalen MySQL-Transaktionskennung (GTID)-Replikation einrichten.

Mit GTIDs werden Transaktionen identifiziert und nachverfolgt, wenn sie auf dem ursprünglichen Server festgeschrieben und von Replikaten angewendet werden. Sie müssen nicht auf Protokolldateien verweisen, wenn Sie während des Failovers ein neues Replikat starten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine bereitgestellte Amazon Linux-Instance

Einschränkungen

- Für diese Einrichtung muss ein internes Team die schreibgeschützten Abfragen ausführen.
- Die MySQL-Quell- und Zielversionen müssen identisch sein.
- Die Replikation wird in derselben AWS-Region und Virtual Private Cloud (VPC) eingerichtet.

Produktversionen

- Amazon-RDS-Versionen 5.7.23 und höher, bei denen es sich um die Versionen handelt, die GTID unterstützen

Architektur

Quelltechnologie-Stack

- Amazon RDS für MySQL

Zieltechnologie-Stack

- MySQL auf Amazon EC2

Zielarchitektur

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) for MySQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen MySQL-Datenbank in der AWS Cloud.

Andere -Services

- Globale Transaktionskennungen (GTIDs) sind eindeutige IDs, die für festgeschriebene MySQL-Transaktionen generiert werden.
- mysqldump ist ein Client-Dienstprogramm zum Ausführen logischer Backups, indem SQL-Anweisungen erstellt werden, die ausgeführt werden können, um die Quelldatenbankobjektdefinitionen und Tabellendaten zu reproduzieren.
- mysql ist der Befehlszeilen-Client für MySQL .

Polen

Erstellen und Vorbereiten der DB-Instance von Amazon RDS für MySQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die RDS-für-MySQL-Instance.	Um die RDS-für-MySQL-Instance zu erstellen, führen Sie die Schritte in der Amazon-RDS-Dokumentation aus und verwenden Sie dabei die Parameterwerte, die in der nächsten Aufgabe behandelt werden.	DBA, DevOps Techniker
Aktivieren Sie GTID-bezogene Einstellungen in der DB-Parametergruppe.	Aktivieren Sie die folgenden Parameter in der DB-Parametergruppe von Amazon RDS für MySQL. Setzen Sie `enforce_gtid_consistency` auf onund `gtid-mode` auf on.	DBA
Starten Sie die Amazon RDS for MySQL-Instance neu.	Ein Neustart ist erforderlich, damit die Parameteränderungen wirksam werden.	DBA
Erstellen Sie einen Benutzer und erteilen Sie ihm Replikationsberechtigungen.	Verwenden Sie die folgenden Befehle, um MySQL zu installieren. `CREATE USER 'repl'@'%' IDENTIFIED BY 'xxxx'; GRANT REPLICATI ON slave ON *.* TO 'repl'@'%' ;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`FLUSH PRIVILEGES;`	

Installieren und Vorbereiten von MySQL auf der Amazon EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie MySQL auf Amazon Linux.	Verwenden Sie die folgenden Befehle, um MySQL zu installieren.
	`sudo yum update`
	`sudo wget https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum localinstall mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum install mysql-community-server`
	`sudo systemctl start mysqld`
		DBA

Melden Sie sich bei MySQL auf der EC2-Instance an und erstellen Sie die Datenbank.	Der Datenbankname sollte mit dem Datenbanknamen in Amazon RDS for MySQL übereinstimmen. Im folgenden Beispiel lautet der Datenbank name `replication` . `create database replication;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bearbeiten Sie die MySQL-Konfigurationsdatei und starten Sie die Datenbank neu.	Bearbeiten Sie die `my.conf` Datei, die sich in befindet, `/etc/` indem Sie die folgenden Parameter hinzufügen.
	`server-id=3`
	`gtid_mode=ON`
	`enforce_gtid_consistency=ON`
	`replicate-ignore-db=mysql`
	`binlog-format=ROW`
	`log_bin=mysql-bin`
	Starten Sie dann den `mysqld` Service neu.
	`systemctl mysqld restart`
		DBA

Einrichten der Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie den Datenabbild aus der Datenbank von Amazon RDS für MySQL.	Verwenden Sie den folgenden Befehl, um den Dump aus Amazon RDS for MySQL zu exportieren. `mysqldump --single-transaction -h mydb.xxxxxxx.amazonaws.com -uadmin -p --databases replication > replication-db.sql`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die SQL-Dump-Datei in der MySQL-Datenbank auf Amazon EC2 wieder her.	Verwenden Sie den folgenden Befehl, um den Dump in die MySQL-Datenbank auf Amazon EC2 zu importieren. `mysql -D replication -uroot -p < replication-db.sql`	DBA

Konfigurieren Sie die MySQL-Datenbank auf Amazon EC2 als Replikat.	Um die Replikation zu starten und den Replikationsstatus zu überprüfen, melden Sie sich bei der MySQL-Datenbank auf Amazon EC2 an und verwenden Sie den folgenden Befehl.
	`CHANGE MASTER TO MASTER_HOST="mydb.xxxxxxx.amazonaws.com", MASTER_USER="repl", MASTER_PASSWORD="rep123", MASTER_PORT=3306, MASTER_AUTO_POSITION = 1;`
	`START SLAVE;`
	`SHOW SLAVE STATUS\G`
		DBA

Zugehörige Ressourcen

- Amazon EC2-Benutzerhandbuch für Linux-Instances
- Installieren von MySQL unter Linux mit dem MySQL Yum Repository
- Replikation mit globalen Transaktionskennungen
- Verwenden der GTID-basierten Replikation für Amazon RDS for MySQL

Übergangsrollen für eine Oracle- PeopleSoft Anwendung in Amazon RDS Custom für Oracle

Erstellt von Sampath Kathirvel (AWS)

Umgebung: Produktion	Technologien: Datenbanken; Infrastruktur	Workload: Oracle
AWS-Services: Amazon RDS		

Übersicht

Um die Enterprise PeopleSoft Resource Planning (ERP)-Lösung von Oracle auf Amazon Web Services (AWS) auszuführen, können Sie Amazon Relational Database Service (Amazon RDS) oder Amazon RDS Custom für Oracle verwenden, das ältere, benutzerdefinierte und verpackte Anwendungen unterstützt, die Zugriff auf das zugrunde liegende Betriebssystem (OS) und die Datenbankumgebung benötigen. Wichtige Faktoren, die Sie bei der Planung einer Migration berücksichtigen sollten, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster konzentriert sich auf die Schritte zur Durchführung einer Oracle Data Guard-Umschaltung oder Rollenübergangs für eine PeopleSoft Anwendungsdatenbank, die auf Amazon RDS Custom als Primärdatenbank mit einer Lesereplikat-Datenbank ausgeführt wird. Das Muster enthält Schritte zum Konfigurieren des Fast-Start-Failovers (FSFO). Während dieses Prozesses funktionieren die Datenbanken in der Oracle Data Guard-Konfiguration weiterhin in ihren neuen Rollen. Typische Anwendungsfälle für Oracle Data Guard Switchover sind Notfallwiederherstellungs-Drosselungen (DR), geplante Wartungsaktivitäten für Datenbanken und fortlaufende Patches für Standby-First Patch Apply. Weitere Informationen finden Sie im Blogbeitrag Reduzierung der Ausfallzeit beim Datenbank-Patching in Amazon RDS Custom .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Abschluss von HA zu Oracle auf PeopleSoft Amazon RDS Custom hinzufügen mithilfe eines Lesereplikatmusters.

Einschränkungen

- Einschränkungen und nicht unterstützte Konfigurationen für RDS Custom für Oracle
- Einschränkungen im Zusammenhang mit Lesereplikaten von Amazon RDS Custom für Oracle

Produktversionen

- Informationen zu Oracle-Database-Versionen, die von Amazon RDS Custom unterstützt werden, finden Sie unter RDS Custom für Oracle.
- Informationen zu Oracle-Database-Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Unterstützung von DB-Instance-Klassen für RDS Custom für Oracle.

Architektur

Technologie-Stack

- Amazon RDS Custom für Oracle

Zielarchitektur

Das folgende Diagramm zeigt eine Amazon RDS Custom DB-Instance und ein Amazon RDS Custom Read Replica. Oracle Data Guard bietet einen Rollenwechsel während des Failovers für DR.

Eine repräsentative Architektur mit Oracle PeopleSoft in AWS finden Sie unter Einrichten einer hochverfügbaren PeopleSoft Architektur in AWS .

Tools

AWS-Services

- Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und gepackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen. In diesem Muster rufen Sie die Datenbankbenutzerpasswörter

von Secrets Manager für `RDS_DATAGUARD` mit dem Secret-Namen `abdo-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Andere -Services

- Oracle Data Guard unterstützt Sie beim Erstellen, Verwalten und Überwachen von Standby-Datenbanken. Dieses Muster verwendet die maximale Leistung von Oracle Data Guard für den Übergang von Rollen (Oracle Data Guard Switchover).

Bewährte Methoden

Für Ihre Produktionsbereitstellung empfehlen wir, die Watcher-Instance in einer dritten Availability Zone zu starten, getrennt von den Primär- und Lesereplikatknoten.

Polen

Rollenübergang initiieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pausieren Sie die Datenbank automatisierung sowohl für den primären als auch für das Replikat.	Obwohl das RDS Custom Automation Framework den Rollenübergangsprozess nicht beeinträchtigt, empfiehlt es sich, die Automatisierung während der Oracle Data Guard-Umstellung anzuhalten. Um die RDS Custom Database Automation anzuhalten und fortzusetzen, folgen Sie den Anweisungen unter Anhalten und Fortsetzen der RDS Custom Automation.	Cloud-Administrator, DBA
Überprüfen Sie den Oracle Data Guard-Status.	Um den Oracle Data Guard-Status zu überprüfen, melden Sie sich bei der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Primärdatenbank an. Dieses Muster enthält Code für die Verwendung einer Multi-Tenant-Container-Datenbank (CDB) oder einer Nicht-CDB-Instance.
	
	Nicht-CDB
	
	`-bash-4.2$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_A`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Mon Nov 28 20:55:50 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`
	`Connected to "ORCL_A"`
	`Connected as SYSDG.`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SUCCESS (status updated 59 seconds ago) DGMGRL> CDB CDB-bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:13:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_A" Connected as SYSDG. DGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 52 seconds ago)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DGMGRL>`	
Überprüfen Sie die Instance-Rolle.	Öffnen Sie die AWS-Management konsole und navigieren Sie zur Amazon RDS-Konsole. Überprüfen Sie im Abschnitt Replikation der Datenbank auf der Registerkarte Konnektivität und Sicherheit die Instance-Rolle für das Primär- und das Replikat. Die primäre Rolle sollte mit der Primärdatenbank von Oracle Data Guard übereinstimmen und die Replikatrolle sollte mit der physischen Standby-Datenbank von Oracle Data Guard übereinstimmen.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die Umstellung durch.	Um die Umstellung durchzuführen, stellen Sie vom Primärknoten DGMGRL aus eine Verbindung zu her.
	
	Nicht-CDB
	
	`DGMGRL> switchover to orcl_d;`
	`Performing switchover NOW, please wait...`
	`Operation requires a connection to database "orcl_d"`
	`Connecting ...`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`New primary database "orcl_d" is opening...`
	`Operation requires start up of instance "ORCL" on database "orcl_a"`
	`Starting instance "ORCL"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "ORCL_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "ORCL_A"`
	`Switchover succeeded, new primary is "orcl_d"`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> switchover to rdscdb_b`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Performing switchover NOW, please wait...`
	`New primary database "rdscdb_b" is opening...`
	`Operation requires start up of instance "RDSCDB" on database "rdscdb_a"`
	`Starting instance "RDSCDB"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "RDSCDB_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "RDSCDB_A"`
	`Switchover succeeded, new primary is "rdscdb_b"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Oracle Data Guard-Verbindung.	Überprüfen Sie nach der Umstellung die Oracle Data Guard-Verbindung vom Primärknoten zu `DGMGRL`.
	
	Nicht-CDB
	
	`DGMGRL> show configura tion;`
	`Configuration - rds_dg`
	`Protection Mode:`
	`MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	`database`
	`orcl_a - Physical`
	`standby database`
	`Fast-Start Failover:`
	`Disabled`
	`Configuration Status:`
	`SUCCESS (status updated`
	`60 seconds ago)`
	`DGMGRL>`
	
	`DGMGRL> show configura tion lag;`
	`Configuration - rds_dg`
	`Protection Mode:`
	`MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	`database`
	`orcl_a - Physical`
	`standby database`
	`Transport Lag: 0`
	`seconds (computed 0`
	`seconds ago)`
	`Apply Lag: 0 seconds`
	`(computed 0 seconds`
	`ago)`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS (status updated
 44 seconds ago)
DGMGRL>
```

CDB

```
DGMGRL> show configura
tion
DGMGRL> show configura
tion
Configuration - rds_dg
  Protection Mode:
 MaxAvailability
  Members:
  rdscdb_b - Primary
 database
    rdscdb_a - Physical
 standby database
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS   (status
 updated 52 seconds ago)
DGMGRL>

DGMGRL> show configura
tion lag
Configuration - rds_dg
  Protection Mode:
 MaxAvailability
  Members:
  rdscdb_b - Primary
 database
    rdscdb_a - Physical
 standby database
              Transport
 Lag:      0 seconds
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 53 seconds ago) DGMGRL>	
Überprüfen Sie die Instance-Rolle in der Amazon RDS-Konsole.	Nachdem Sie den Rollenwechsel durchgeführt haben, zeigt die Amazon RDS-Konsole die neuen Rollen im Abschnitt Replikation auf der Registerkarte Konnektivität und Sicherheit unter Datenbanken an. Es kann einige Minuten dauern, bis der Replikationsstatus von leer auf Replizieren aktualisiert wird.	DBA

Konfigurieren von FSFO

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Setzen Sie die Umstellung zurück.	Setzen Sie die Umstellung wieder auf den Primärknoten.	DBA
Installieren und starten Sie den Beobachter.	Ein Watcher-Prozess ist eine `DGMGRL` Client-Komponente, die normalerweise auf einem anderen Computer als die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Primär- und Standby-D atenbank ausgeführt wird. Bei der ORACLE-HoME-Instal lation für den Beobachter kann es sich um eine Oracle-Client-Administrator-Installa tion handeln, oder Sie können entweder Oracle Database Enterprise Edition oder Personal Edition installieren. Weitere Informationen zur Installation von Beobachte rn für Ihre Datenbankversion finden Sie unter Installieren und Starten von Beobachte rn. Um die hohe Verfügbarkeit für den Beobachterprozess zu konfigurieren, sollten Sie Folgendes tun: • Aktivieren Sie die automatis che Wiederherstellung der EC2-Instance für die EC2-Instance, auf der Ihr Beobachter ausgeführt wird. Sie müssen den Startvorg ang des Beobachters im Rahmen des Betriebss ystemstarts automatisieren. • Stellen Sie einen Beobachte r in der EC2-Instance bereit und konfigurieren Sie eine Amazon EC2-Auto Scaling-Gruppe mit der Größe 1 (1). Im Falle eines Ausfalls	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der EC2-Instance startet die Auto-Scaling-Gruppe automatisch eine weitere EC2-Instance. Für Oracle 12c Release 2 und höher können Sie bis zu drei Beobachter bereitstellen. Ein Beobachter ist der primäre Beobachter und der Rest sind Backup-Beobachter. Wenn der primäre Beobachter ausfällt, übernimmt einer der Backup-Beobachter die primäre Rolle.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie vom Beobachter-Host aus eine Verbindung zu CCPMGRL her.	Der Watcher-Host ist mit `tnsnames.ora` Einträgen für die primäre und Standby-Datenbankkonnektivität konfiguriert. Sie können FSFO mit dem maximalen Leistungs schutzmodus aktivieren, solange der Datenverlust innerhalb der FastStart FailoverLagLimit Konfigura tion liegt (Wert in Sekunden) . Sie müssen jedoch den maximalen Verfügbarkeitsschu tzmodus verwenden, um zu arbeiten, um keinen Datenverl ust zu erreichen (RPO=0). Nicht-CDB `DGMGRL> show configura tion; Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 58 seconds ago) DGMGRL> show configura tion lag Configuration - rds_dg`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 5 seconds ago) DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:55:09 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_A " Connected as SYSDG.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 18 seconds ago)
	DGMGRL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Standby-Datenbank als Failover-Ziel.	Stellen Sie entweder vom Primärknoten oder vom Beobachterknoten aus eine Verbindung zu einer Standby-Datenbank her. (Obwohl Ihre Onfiguration mehrere Standby-Datenbanken haben könnte, müssen Sie derzeit nur eine Verbindung zu einer herstellen.)
	
	Nicht-CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='orcl_d';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database orcl_d set property FastStartFailoverTarget='orcl_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database orcl_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_d'`
	`DGMGRL> show database orcl_d FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_a'`
	`DGMGRL>`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='rdscdb_b';`
	`Object "orcl_a" was not found`
	`DGMGRL> edit database rdscdb_a set property FastStartFailoverTarget='rdscdb_b';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database rdscdb_b set property FastStartFailoverTarget='rdscdb_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database rdscdb_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_b'`
	`DGMGRL> show database rdscdb_b FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_a'`
	`DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie FastStart FailoverThreshold für die Verbindung mit CCPRL.	Der Standardwert ist 30 Sekunden in Oracle 19c und der Mindestwert ist 6 Sekunden. Ein niedrigerer Wert kann möglicherweise das Recovery Time Objective (RTO) während des Failovers verkürzen. Ein höherer Wert trägt dazu bei, das Risiko unnötiger vorüberge hender Failover-Fehler in der Primärdatenbank zu verringer n. Das Automatisierungs-F ramework von RDS Custom für Oracle überwacht den Datenbankzustand und führt alle paar Sekunden Korrektur maßnahmen durch. Daher empfehlen wir, FastStart FailoverThreshold auf einen Wert über 10 Sekunden einzustellen. Im folgenden Beispiel wird der Schwellen wert auf 35 Sekunden konfiguriert. Nicht-CBD oder CDB `DGMGRL> edit configura tion set property  FastStartFailoverT hreshold=35;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Property "faststar tfailoverthreshold" updated DGMGRL> show configura tion FastStart FailoverThreshold; FastStartFailover Threshold = '35' DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktivieren Sie FSFO, indem Sie vom Primär- oder Beobachterknoten aus eine Verbindung zu CCPMGRL herstellen.	Wenn für die Datenbank keine Flashback-Datenbank aktiviert ist, `ORA-16827` wird die Warnmeldung angezeigt. Die optionale Flashback-Datenbank hilft dabei, ausgefallene Primärdatenbanken automatisch auf einen Zeitpunkt vor dem Failover wiederherzustellen, wenn die FastStartFailoverAutoReinstate Konfigurationseigenschaft auf gesetzt ist `TRUE` (was die Standardeinstellung ist).
	
	Nicht-CDB
	
	`DGMGRL> enable fast_start failover;`
	`Warning: ORA-16827: Flashback Database is disabled`
	`Enabled in Zero Data Loss Mode.`
	`DGMGRL>`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`Warning: ORA-16819: fast-start failover observer not started`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	orcl_d - (*) Physical
	 standby database
	Warning: ORA-16819:
	 fast-start failover
	 observer not started
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:
	WARNING (status updated
	 29 seconds ago)
	DGMGRL>
	
	CDB
	
	DGMGRL> enable fast_star
	t failover;
	Warning: ORA-16827:
	 Flashback Database is
	 disabled
	Enabled in Zero Data
	 Loss Mode.
	DGMGRL> show configura
	tion;
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  Warning: ORA-16819
	: fast-start failover
	 observer not started
	  rdscdb_b - (*)
	 Physical standby
	 database
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`WARNING (status updated 11 seconds ago)` `DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie den Beobachter für die FSFO-Überwachung und überprüfen Sie den Status.	Sie können den Beobachter vor oder nach der Aktivierung von FSFO starten. Wenn FSFO bereits aktiviert ist, beginnt der Beobachter sofort mit der Überwachung des Status und der Verbindungen zu den primären und Ziel-Standby-Datenbanken. Wenn FSFO nicht aktiviert ist, beginnt der Beobachter erst mit der Überwachung, nachdem FSFO aktiviert wurde.
	
	Wenn Sie den Beobachter starten, wird die primäre DB-Konfiguration ohne Fehlermeldungen angezeigt, wie durch den vorherigen `show configuration` Befehl belegt.
	
	Nicht-CDB
	
	`DGMGRL> start observer;`
	`[W000 2022-12-01T06:16:51.271+00:00] FSFO target standby is orcl_d`
	`Observer 'ip-10-0-1-89' started`
	`[W000 2022-12-01T06:16:51.352+00:00] Observer trace level is set to USER`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 56 seconds ago) DGMGRL> DGMGRL> show observer Configuration - rds_dg Primary: orcl_a Active Target: orcl_d Observer "ip-10-0- 1-89" - Master Host Name: ip-10-0-1 -89 Last Ping to Primary: 1 second ago Last Ping to Target: 1 second ago DGMGRL> CDB DGMGRL> start observer; Succeeded in opening the observer file "/home/oracle/fsfo _ip-10-0-1-56.dat". [W000 2023-01-1 8T07:31:32.589+00:00]	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	FSFO target standby is rdscdb_b Observer 'ip-10-0-1-56' started The observer log file is '/home/oracle/observer_ip-10-0-1-56.log'. DGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 12 seconds ago) DGMGRL> DGMGRL> show observer; Configuration - rds_dg Primary: rdscdb_a Active Target: rdscdb_b Observer "ip-10-0-1-56" - Master Host Name: ip-10-0-1-56 Last Ping to Primary: 1 second ago Last Ping to Target: 2 seconds ago	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das Failover.	In diesem Szenario kann ein Failover-Test durchgeführt werden, indem die primäre EC2-Instance manuell gestoppt wird. Bevor Sie die EC2-Instance anhalten, verwenden Sie den `tail` Befehl , um die Beobachte r-Protokolldatei basierend auf Ihrer Konfiguration zu überwachen. Verwenden Sie `DGMGRL`, um sich bei der Standby-Datenbank `orcl_d` mit dem Benutzer anzumelde n `RDS_DATAGUARD` und den Oracle Data Guard-Status zu überprüfen. Es sollte zeigen, dass die neue Primärdat enbank `orcl_d` ist. Hinweis: In diesem Failover-Testszenario `orcl_d` ist die Nicht-CDB-Datenbank. Vor dem Failover wurde die Flashback-Datenbank auf aktiviert`orcl_a`. Nachdem die frühere Primärdatenbank online zurückgekehrt ist und im -`MOUNT`Zustand beginnt, stellt der Beobachter sie wieder in eine neue Standby-Datenbank wieder her. Die wiederhergestellte Datenbank fungiert als FSFO-Ziel für	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die neue Primärdatenbank. Sie können die Details in Beobachterprotokollen überprüfen. `DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_d - Primary database Warning: ORA-16824 : multiple warnings, including fast-star t failover-related warnings, detected for the database orcl_a - (*) Physical standby database (disabled) ORA-16661: the standby database needs to be reinstated Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 25 seconds ago) DGMGRL>`  Das folgende Beispiel zeigt die Ausgabe in `observer.log` .  `$ tail -f /tmp/obse rver.log`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Unable to connect to database using rds_custom_orcl_a [W000 2023-01-1 8T07:50:32.589+00:00] Primary database cannot be reached. [W000 2023-01-1 8T07:50:32.589+00:00] Fast-Start Failover threshold has expired. [W000 2023-01-1 8T07:50:32.590+00:00] Try to connect to the standby. [W000 2023-01-1 8T07:50:32.590+00: 00] Making a last connection attempt to primary database before proceeding with Fast- Start Failover. [W000 2023-01-1 8T07:50:32.591+00:00] Check if the standby is ready for failover. [S002 2023-01-1 8T07:50:32.591+00:00] Fast-Start Failover started... 2023-01-18T07:50 :32.591+00:00 Initiating Fast-Star t Failover to database "orcl_d"... [S002 2023-01-1 8T07:50:32.592+00:00] Initiating Fast-start Failover. Performing failover NOW, please wait...	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Failover succeeded, new primary is "orcl_d" 2023-01-18T07:55:3 2.101+00:00 [S002 2023-01-1 8T07:55:32.591+00:00] Fast-Start Failover finished... [W000 2023-01-1 8T07:55:32.591+00:00] Failover succeeded. Restart pinging. [W000 2023-01-1 8T07:55:32.603+00:00] Primary database has changed to orcl_d. [W000 2023-01-1 8T07:55:33.618+00:00] Try to connect to the primary. [W000 2023-01-1 8T07:55:33.622+00: 00] Try to connect to the primary rds_custo m_orcl_d. [W000 2023-01-1 8T07:55:33.634+00: 00] The standby orcl_a needs to be reinstated [W000 2023-01-1 8T07:55:33.654+00:00] Try to connect to the new standby orcl_a. [W000 2023-01-1 8T07:55:33.654+00: 00] Connection to the primary restored! [W000 2023-01-1 8T07:55:35.654+00: 00] Disconnecting from database rds_custo m_orcl_d.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`[W000 2023-01-18T07:55:57.701+00:00] Try to connect to the new standby orcl_a. ORA-12170: TNS:Connect timeout occurred`	

Konfigurieren der Konnektivität zwischen der Oracle-Personsoft-Anwendung und der Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und starten Sie den Service in der Primärdatenbank.	Sie können Änderungen der Anwendungskonfiguration während eines Rollenwechsels vermeiden, indem Sie einen TNS-Eintrag verwenden, der sowohl die primären als auch die Standby-Datenbankendpunkte in der Konfiguration enthält. Sie können zwei rollenbasierte Datenbankservices definieren, um Lese-/Schreib-Workloads und schreibgeschützte Workloads zu unterstützen. Im folgenden Beispiel `orcl_rw` ist der Lese-Schreib-Service, der in der Primärdatenbank aktiv ist. `orcl_ro` ist der schreibgeschützte Service und ist in der Standby-Datenbank aktiv, die im schreibgeschützten Modus geöffnet wurde.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ---------- ORCL READ WRITE SQL> exec dbms_serv ice.create_service ('orcl_rw','orcl_r w'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.create_service ('orcl_ro','orcl_r o'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.start_service('orcl_rw'); PL/SQL procedure successfully completed . SQL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Service in der Standby-Datenbank.	Verwenden Sie den folgenden Code, um den Service in der schreibgeschützten Standby-Datenbank zu starten. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- ---------- ----------- ORCL READ ONLY WITH  APPLY SQL> exec dbms_serv ice.start_service( 'orcl_ro'); PL/SQL procedure  successfully completed . SQL>`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Automatisieren Sie den Start des Services, wenn die primäre DB neu gestartet wird.	Verwenden Sie den folgenden Code, um den Service in der Primärdatenbank automatisch zu starten, wenn er neu gestartet wird. `SQL> CREATE OR REPLACE TRIGGER TrgDgServices after startup on database DECLARE db_role VARCHAR(30); db_open_mode VARCHAR(30); BEGIN SELECT DATABASE_ROLE, OPEN_MODE INTO db_role, db_open_mode FROM V$DATABASE; IF db_role = 'PRIMARY' THEN DBMS_SERV 2 ICE.START_SERVICE('orcl_rw'); END IF; IF db_role = 'PHYSICAL STANDBY' AND db_open_mode LIKE 'READ ONLY%' THEN DBMS_SERVICE.START_SERVICE('orcl_ro'); END IF; END; / Trigger created. SQL>`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine Verbindung zwischen der Lese-/Schreibdatenbank und der schreibgeschützten Datenbank.	Sie können das folgende Anwendungskonfigurationsbeispiel für die Lese-/Schreib- und schreibgeschützte Verbindung verwenden. `ORCL_RW = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = orcl_rw))) ORCL_RO = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`.rds.amazonaws.com)(PORT=1521))(ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com)(PORT=1521))))(CONNECT_DATA=(SERVICE_NAME = orcl_ro))))`	

Zugehörige Ressourcen

- Hochverfügbarkeit mit Data Guard auf Amazon RDS Custom für Oracle aktivieren (technisches AWS-Handbuch)
- Konfigurieren von Amazon RDS als Oracle PeopleSoft -Datenbank (AWS-Whitepaper)
- Oracle Data Guard Broker-Handbuch (Oracle-Referenzdokumentation)
- Konzepte und Administration von Data Guard (Oracle-Referenzdokumentation)
- Oracle Data Guard Specific FAN- undF-Konfigurationsanforderungen (Oracle-Referenzdokumentation)

Datenbankmigrationsmuster nach Workload

Themen

IBM

- Migrieren einer Db2-Datenbank von Amazon EC2 zu Aurora MySQL – kompatibel mithilfe von AWS DMS
- Migrieren Sie Db2 für LUW zu Amazon EC2, indem Sie den Protokoll-Versand verwenden, um die Ausfallzeit zu reduzieren
- Migrieren Sie Db2 für LUW zu Amazon EC2 mit Notfallwiederherstellung für hohe Verfügbarkeit
- Migrieren von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL – kompatibel mit AWS DMS und AWS SCT
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Sichern und optimieren Sie den Benutzerzugriff in einer Db2-Verbunddatenbank in AWS mithilfe vertrauenswürdiger Kontexte

Microsoft

- Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS
- Zugriff auf lokale Microsoft SQL Server-Tabellen von Microsoft SQL Server auf Amazon EC2 über verknüpfte Server
- Bewerten der Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas in AWS
- Ändern von Python- und Perl-Anwendungen zur Unterstützung der Datenbankmigration von Microsoft SQL Server zu Amazon Aurora PostgreSQL – Kompatible Edition
- Konfigurieren von schreibgeschütztem Routing in einer AlwaysOn-Verfügbarkeitsgruppe in SQL Server auf AWS
- Erstellen von AWS- CloudFormation Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- Exportieren einer Microsoft SQL Server-Datenbank nach Amazon S3 mithilfe von AWS DMS
- Exportieren von Amazon RDS for SQL Server-Tabellen in einen S3-Bucket mithilfe von AWS DMS
- Aufnehmen und Migrieren von EC2-Windows-Instances in ein AWS Managed Services-Konto
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server mithilfe nativer Sicherungs- und Wiederherstellungsmethoden
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mit AWS DMS
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten
- ???

- Migrieren von Daten von Microsoft Azure Blob zu Amazon S3 mithilfe von Rclone
- Migrieren von SQL Server zu AWS mithilfe verteilter Verfügbarkeitsgruppen
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- ???
- Senden von Benachrichtigungen für eine Datenbank-Instance von Amazon RDS für SQL Server mithilfe eines On-Premises-SMTP-Servers und Database Mail
- Einrichten einer Multi-AZ-Infrastruktur für eine SQL Server Always On FCI mithilfe von Amazon FSx

–

- Erstellen eines Genehmigungsprozesses für Firewall-Anforderungen während einer Hostwechsel-Migration zu AWS
- Verschlüsseln einer vorhandenen DB-Instance von Amazon RDS für PostgreSQL
- Schätzen der Speicherkosten für eine Amazon-DynamoDB-Tabelle
- Implementieren Sie regionsübergreifende Notfallwiederherstellung mit AWS DMS und Amazon Aurora

Open-Source-Software

- ???
- Erstellen von Anwendungsbenutzern und -rollen in Aurora PostgreSQL – kompatibel
- Aktivieren verschlüsselter Verbindungen für PostgreSQL-DB-Instances in Amazon RDS
- ???
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Migrieren einer On-Premises-MySQL-Datenbank zu Amazon RDS für MySQL
- Migrieren einer On-Premises-MySQL-Datenbank zu Aurora MySQL
- Migrieren einer On-Premises-PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Migrieren von Oracle 8i oder 9i zu Amazon RDS für Oracle mit SharePlex und AWS DMS
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren von PostgreSQL auf Amazon EC2 zu Amazon RDS für PostgreSQL mit pglogical
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie On-Premises-MySQL-Datenbanken zu Aurora MySQL mit Percona XtraBackup, Amazon EFS und Amazon S3
- Migrieren externer Oracle-Tabellen zu Amazon Aurora PostgreSQL – kompatibel
- Migrieren von Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten zu PostgreSQL
- Migrieren von Redis-Workloads zu Redis Enterprise Cloud in AWS
- Überwachen von Amazon Aurora auf Instances ohne Verschlüsselung
- Starten Sie den AWS Replication Agent automatisch neu, ohne SELinux nach dem Neustart eines RHEL-Quellservers zu deaktivieren
- Planen von Aufträgen für Amazon RDS for PostgreSQL und Aurora PostgreSQL mithilfe von Lambda und Secrets Manager
- Einrichten der Datenreplikation zwischen Amazon RDS für MySQL und MySQL auf Amazon EC2 mithilfe von GTID
- Transportieren von PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport

Oracle

- Hinzufügen von HA zu Oracle PeopleSoft auf Amazon RDS Custom mithilfe eines Lesereplikats
- Konfigurieren von Links zwischen Oracle Database und Aurora PostgreSQL – kompatibel
- Konvertieren von JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL
- Konvertieren des Datentyps VARCHAR2(1) für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Emulieren von Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Emulieren von Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL
- Schätzen der Amazon RDS-Engine-Größe für eine Oracle-Datenbank mithilfe von AWR-Berichten
- Behandlung anonymer Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL
- Verarbeiten überlasteter Oracle-Funktionen in Aurora PostgreSQL – kompatibel
- Inkrementelle Migration von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL mit Oracle SQL Developer und AWS SCT
- ???
- Migrieren von DB-Instances von Amazon RDS für Oracle zu anderen Konten, die AMS verwenden
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und AWS DMS mithilfe von AWS CLI und AWS CloudFormation
- ???
- Migrieren einer DB-Instance von Amazon RDS für Oracle zu einer anderen VPC
- Migrieren einer lokalen Oracle-Datenbank zu Amazon EC2 mithilfe von Oracle Data Pump
- Migrieren einer lokalen Oracle-Datenbank zu Amazon OpenSearch Service mit Logstash
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren einer On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle mithilfe des direkten Oracle Data Pump Imports über einen Datenbanklink
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle Data Pump

- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe eines Oracle-Bystanders und AWS DMS
- Migrieren einer lokalen Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren einer Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB mithilfe von AWS DMS und AWS SCT
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren einer Oracle-Datenbank zu Amazon DynamoDB mit AWS DMS
- Migrieren einer Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle GoldenGate Flat File Adaptern
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mit AWS DMS und AWS SCT
- Migrieren einer Oracle JD Edwards- EnterpriseOne Datenbank zu AWS mithilfe von Oracle Data Pump und AWS DMS
- Migrieren einer partitionierten Oracle-Tabelle zu PostgreSQL mithilfe von AWS DMS
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren von Daten aus einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für MySQL
- Migrieren Sie von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mithilfe materialisierter Ansichten und AWS DMS
- Migrieren von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mit SharePlex und AWS DMS
- Migrieren von Oracle Database zu Amazon RDS for PostgreSQL mithilfe von Oracle GoldenGate
- ???
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Migrieren von funktionsbasierten Indizes von Oracle zu PostgreSQL
- Migrieren älterer Anwendungen von Oracle Pro*C zu ECPG
- Migrieren von Oracle CLOB-Werten zu einzelnen Zeilen in PostgreSQL in AWS
- Migrieren von Oracle-Database-Fehlercodes zu einer mit Amazon Aurora PostgreSQL kompatiblen Datenbank
- Migrieren der Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren von nativen Oracle-Funktionen zu PostgreSQL mithilfe von Erweiterungen

- Migrieren von Oracle-OUT-Bindungsvariablen in eine PostgreSQL-Datenbank
- Migrieren von Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren der Oracle ROWID-Funktionalität zu PostgreSQL in AWS
- Migrieren von Oracle SERIALLY_REUSABLE-Pragma-Paketen zu PostgreSQL
- Migrieren von virtuell generierten Spalten von Oracle zu PostgreSQL
- Überwachen von Oracle- GoldenGate Protokollen mithilfe von Amazon CloudWatch
- Plattformwechsel von Oracle Database Enterprise Edition auf Standard Edition 2 auf Amazon RDS für Oracle
- Einrichten einer HA/DR-Architektur für Oracle E-Business Suite in Amazon RDS Custom mit einer aktiven Standby-Datenbank
- Einrichten der Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL – kompatibel
- Übergangsrollen für eine Oracle- PeopleSoft Anwendung in Amazon RDS Custom für Oracle
- Validieren von Datenbankobjekten nach der Migration von Oracle zu Amazon Aurora PostgreSQL

SAP

- Automatisches Sichern von SAP HANA-Datenbanken mit Systems Manager und EventBridge
- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren von SAP ASE zu Amazon RDS for SQL Server mit AWS DMS
- Migrieren von SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL – kompatibel mit AWS SCT und AWS DMS
- ???
- Reduzieren Sie die homogene Cutover-Zeit für die SAP-Migration mithilfe von Application Migration Service
- Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten

Mehr Muster

- Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden
- Aggregieren von Daten in Amazon DynamoDB für ML-Prognosen in Athena
- EC2-Instances Schreibzugriff auf S3-Buckets in AMS-Konten gewähren
- Analysieren und visualisieren Sie verschachtelte JSON-Daten mit Amazon Athena und Amazon QuickSight
- Authentifizieren von Microsoft SQL Server auf Amazon EC2 mit AWS Directory Service
- Automatisieren von Backups für Amazon RDS for PostgreSQL-DB-Instances mithilfe von AWS Batch
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatisches Generieren eines PynamoDB-Modells und von CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung
- Automatische Behebung unverschlüsselter Amazon RDS-DB-Instances und -Cluster
- ???
- Erstellen Sie mithilfe von DevOps Praktiken und AWS Cloud9 eine lose gekoppelte Architektur mit Microservices
- Ändern von Python- und Perl-Anwendungen zur Unterstützung der Datenbankmigration von Microsoft SQL Server zu Amazon Aurora PostgreSQL – Kompatible Edition
- Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren
- Konfigurieren von Links zwischen Oracle Database und Aurora PostgreSQL – kompatibel
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL
- Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL
- Konvertieren des Datentyps VARCHAR2(1) für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Erstellen von Anwendungsbenutzern und -rollen in Aurora PostgreSQL – kompatibel
- Erstellen von AWS- CloudFormation Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- ???
- Bereitstellen eines Cassandra-Clusters auf Amazon EC2 mit privaten statischen IPs, um einen Neuausgleich zu vermeiden

- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct
- Emulieren von Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Aktivieren der transparenten Datenverschlüsselung in Amazon RDS für SQL Server
- Exportieren einer Microsoft SQL Server-Datenbank nach Amazon S3 mithilfe von AWS DMS
- Inkrementelle Migration von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL mit Oracle SQL Developer und AWS SCT
- ???
- Verwalten von Anmeldeinformationen mit AWS Secrets Manager
- Migrieren einer Db2-Datenbank von Amazon EC2 zu Aurora MySQL – kompatibel mithilfe von AWS DMS
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas in der AWS-Cloud
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und AWS DMS mithilfe von AWS CLI und AWS CloudFormation
- Migrieren einer Amazon RDS-DB-Instance zu einer anderen VPC oder einem anderen Konto
- ???
- Migrieren einer DB-Instance von Amazon RDS für Oracle zu einer anderen VPC
- Migrieren eines Amazon-Redshift-Clusters zu einer AWS-Region in China
- ???
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server

- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server mithilfe nativer Sicherungs- und Wiederherstellungsmethoden
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mit AWS DMS
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten
- ???
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Migrieren einer On-Premises-MySQL-Datenbank zu Amazon RDS für MySQL
- Migrieren einer On-Premises-MySQL-Datenbank zu Aurora MySQL
- Migrieren einer lokalen Oracle-Datenbank zu Amazon EC2 mithilfe von Oracle Data Pump
- Migrieren einer lokalen Oracle-Datenbank zu Amazon OpenSearch Service mit Logstash
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren einer On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle mithilfe des direkten Oracle Data Pump Imports über einen Datenbanklink
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle Data Pump
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe eines Oracle-Bystanders und AWS DMS
- Migrieren einer lokalen Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren einer On-Premises-PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren einer lokalen ThoughtSpot Falcon-Datenbank zu Amazon Redshift
- Migrieren Sie eine lokale Vertica-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren einer Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB mithilfe von AWS DMS und AWS SCT
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren einer Oracle-Datenbank zu Amazon DynamoDB mit AWS DMS

- Migrieren einer Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle GoldenGate Flat File Adaptern
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mit AWS DMS und AWS SCT
- Migrieren einer Oracle JD Edwards- EnterpriseOne Datenbank zu AWS mithilfe von Oracle Data Pump und AWS DMS
- Migrieren einer partitionierten Oracle-Tabelle zu PostgreSQL mithilfe von AWS DMS
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren von Daten aus einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren von Daten in die AWS Cloud mithilfe von Starburst
- Migrieren Sie Db2 für LUW zu Amazon EC2, indem Sie den Protokoll-Versand verwenden, um die Ausfallzeit zu reduzieren
- Migrieren Sie Db2 für LUW zu Amazon EC2 mit Notfallwiederherstellung für hohe Verfügbarkeit
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für MySQL
- ???
- Migrieren von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL – kompatibel mit AWS DMS und AWS SCT
- Migrieren Sie von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mithilfe materialisierter Ansichten und AWS DMS
- Migrieren von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mit SharePlex und AWS DMS
- Migrieren von Oracle Database zu Amazon RDS for PostgreSQL mithilfe von Oracle GoldenGate
- ???
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren von PostgreSQL auf Amazon EC2 zu Amazon RDS für PostgreSQL mit pglogical
- Migrieren von SAP ASE zu Amazon RDS for SQL Server mit AWS DMS
- Migrieren von funktionsbasierten Indizes von Oracle zu PostgreSQL
- Migrieren älterer Anwendungen von Oracle Pro*C zu ECPG
- Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS
- Migrieren Sie On-Premises-MySQL-Datenbanken zu Aurora MySQL mit Percona XtraBackup, Amazon EFS und Amazon S3
- Migrieren Sie Oracle Business Intelligence 12c von On-Premises-Servern zur AWS Cloud

- Migrieren von Oracle CLOB-Werten zu einzelnen Zeilen in PostgreSQL in AWS
- Migrieren von Oracle-Database-Fehlercodes zu einer mit Amazon Aurora PostgreSQL kompatiblen Datenbank
- Migrieren der Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren externer Oracle-Tabellen zu Amazon Aurora PostgreSQL – kompatibel
- Migrieren von nativen Oracle-Funktionen zu PostgreSQL mithilfe von Erweiterungen
- Migrieren von Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren der Oracle ROWID-Funktionalität zu PostgreSQL in AWS
- Migrieren von Oracle SERIALLY_REUSABLE-Pragma-Paketen zu PostgreSQL
- Migrieren von Redis-Workloads zu Redis Enterprise Cloud in AWS
- Migrieren von SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL – kompatibel mit AWS SCT und AWS DMS
- Migrieren von virtuell generierten Spalten von Oracle zu PostgreSQL
- Überwachen Sie ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand
- Überwachen von ElastiCache Clustern für Sicherheitsgruppen
- Reduzieren Sie die homogene Cutover-Zeit für die SAP-Migration mithilfe von Application Migration Service
- Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern
- Ausführen von nachrichtengesteuerten Workloads in großem Umfang mithilfe von AWS Fargate
- Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein
- ???
- Einrichten der Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL – kompatibel
- Übertragen Sie umfangreiche Db2-z/OS-Daten in CSV-Dateien an Amazon S3
- Transportieren von PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport
- Verwenden von CloudEndure für die Notfallwiederherstellung einer On-Premises-Datenbank
- Validieren von Datenbankobjekten nach der Migration von Oracle zu Amazon Aurora PostgreSQL
- Überprüfen, ob neue Amazon-Redshift-Cluster in einer VPC gestartet werden

DevOps

Themen

- Bereitstellen einer CI/CD-Pipeline für Java-Microservices auf Amazon ECS
- Verwenden von AWS CodeCommit und AWS CodePipeline zum Bereitstellen einer CI/CD-Pipeline in mehreren AWS-Konten
- Bereitstellen einer Firewall mit AWS Network Firewall und AWS Transit Gateway
- Bereitstellen eines AWS Glue-Auftrags mit einer AWS CodePipeline CI/CD-Pipeline
- Bereitstellen eines Amazon EKS-Clusters aus AWS Cloud9 mithilfe eines EC2-Instance-Profils
- Bereitstellen von Code in mehreren AWS-Regionen mithilfe von AWS CodePipeline, AWS CodeCommitund AWS CodeBuild
- Exportieren von AWS Backup-Berichten aus einer Organisation in AWS Organizations als CSV-Datei
- Exportieren von Tags für eine Liste von Amazon EC2-Instances in eine CSV-Datei
- Generieren einer AWS- CloudFormation Vorlage mit verwalteten AWS Config-Regeln mithilfe vonoSphere
- Gewähren Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Implementieren einer GitHub Flow-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten
- Implementieren einer Gitflow-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten
- Implementierung einer Trunk-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten
- Automatisches Erkennen von Änderungen und Initiieren verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit
- Integrieren eines Bitbucket-Repositorys mit AWS Amplify mithilfe von AWS CloudFormation
- Starten eines CodeBuild Projekts über AWS-Konten hinweg mithilfe von Step Functions und einer Lambda-Proxy-Funktion
- Verwalten Sie Blau/Grün-Bereitstellungen von Microservices für mehrere Konten und Regionen mithilfe von AWS-Codeservices und AWS KMS-Schlüsseln für mehrere Regionen
- Überwachen von Amazon ECR-Repositorys auf Platzhalterberechtigungen mit AWS CloudFormation und AWS Config
- Führen Sie benutzerdefinierte Aktionen aus CodeCommit AWS-Ereignissen durch
- Veröffentlichen von Amazon- CloudWatch Metriken in einer CSV-Datei

- Führen Sie Komponententests für Python-ETL-Jobs in AWS Glue mithilfe des Pytest-Frameworks aus
- Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein
- Richten Sie eine CI/CD-Pipeline mithilfe von AWS CodePipeline und AWS CDK ein
- Einrichten der end-to-end Verschlüsselung für Anwendungen in Amazon EKS mit cert-manager und Let's Encrypt
- Vereinfachen Sie die Bereitstellung von Amazon-EKS-Anwendungen mit mehreren Mandanten mithilfe von Flux
- Abonnieren mehrerer E-Mail-Endpunkte für ein SNS-Thema mithilfe einer benutzerdefinierten Ressource
- Verwenden von Serverspec für die testgesteuerte Entwicklung von Infrastrukturcode
- Verwenden Sie Git-Quell-Repositorys von Drittanbietern in AWS CodePipeline
- Erstellen einer CI/CD-Pipeline zur Validierung von Terraform-Konfigurationen mithilfe von AWS CodePipeline
- Mehr Muster

Automatisieren der AWS-Ressourcenbewertung

Erstellt von Naveen Suthar (AWS), Arun Bolal (AWS), Manish Garg (AWS) und Sandeep Gawande (AWS)

Code-Repository: infrastructure-assessment-iac-automation	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur; Management und Governance; Betrieb; Serverless
AWS-Services: Amazon Athena; AWS CloudTrail; AWS Lambda ;Amazon S3; Amazon QuickSight		

Übersicht

Dieses Muster beschreibt einen automatisierten Ansatz für die Einrichtung von Ressourcenbewertungsfunktionen mithilfe des AWS Cloud Development Kit (AWS CDK). Durch die Verwendung dieses Musters sammeln Betriebsteams automatisch Details zur Ressourcenüberwachung und zeigen die Details aller Ressourcen an, die in einem AWS-Konto auf einem einzigen Dashboard bereitgestellt werden. Dies ist in den folgenden Anwendungsfällen hilfreich:

- Identifizieren von Infrastructure as Code (IaC)-Tools und Isolieren von Ressourcen, die von verschiedenen IaC-Lösungen wie HashiCorp Terraform , AWS CloudFormation, AWS CDK und AWS Command Line Interface (AWS CLI) erstellt wurden
- Abrufen von Informationen zur Ressourcenüberprüfung

Diese Lösung hilft dem Führungsteam auch dabei, von einem einzigen Dashboard aus Einblicke in die Ressourcen und Aktivitäten in einem AWS-Konto zu erhalten.

Hinweis: Amazon QuickSight ist ein kostenpflichtiger Service. Bevor Sie es ausführen, um Daten zu analysieren und ein Dashboard zu erstellen, lesen Sie die Amazon- QuickSight Preisliste .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Identity and Access Management (IAM)-Rollen und -Berechtigungen mit Zugriff auf Bereitstellungsressourcen
- Ein Amazon- QuickSight Konto, das mit Zugriff auf Amazon Simple Storage Service (Amazon S3) und Amazon Athena erstellt wurde
- AWS-CDK-Version 2.55.1 oder höher installiert
- Python Version 3.9 oder höher installiert

Einschränkungen

- Diese Lösung wird in einem einzigen AWS-Konto bereitgestellt.
- Die Lösung verfolgt nicht die Ereignisse, die vor ihrer Bereitstellung aufgetreten sind, es sei denn, AWS CloudTrail war bereits eingerichtet und speichert Daten in einem S3-Bucket.

Produktversionen

- AWS-CDK-Version 2.55.1 oder höher
- Python Version 3.9 oder höher

Architektur

Zieltechnologie-Stack

- Amazon Athena
- AWS CloudTrail
- AWS Glue
- AWS Lambda
- Amazon QuickSight
- Amazon S3

Zielarchitektur

Der AWS-CDK-Code stellt alle Ressourcen bereit, die zum Einrichten von Ressourcenbewertungsfunktionen in einem AWS-Konto erforderlich sind. Das folgende Diagramm zeigt den Prozess des Sendens von CloudTrail Protokollen an AWS Glue , Amazon Athena und QuickSight.

1. CloudTrail sendet Protokolle zur Speicherung an einen S3-Bucket.
2. Eine Ereignisbenachrichtigung ruft eine Lambda-Funktion auf, die die Protokolle verarbeitet und gefilterte Daten generiert.
3. Die gefilterten Daten werden in einem anderen S3-Bucket gespeichert.
4. Ein AWS Glue-Crawler wird für die gefilterten Daten eingerichtet, die sich im S3-Bucket befinden, um ein Schema in der AWS Glue Data Catalog-Tabelle zu erstellen.
5. Die gefilterten Daten können von Amazon Athena abgefragt werden.
6. Auf die abgefragten Daten wird von QuickSight zur Visualisierung zugegriffen.

Automatisierung und Skalierung

- Diese Lösung kann von einem AWS-Konto auf mehrere AWS-Konten skaliert werden, wenn es einen organisationsweiten CloudTrail Trail in AWS Organizations gibt. Durch die Bereitstellung CloudTrail auf Organisationsebene können Sie diese Lösung auch verwenden, um Details zur Ressourcenüberprüfung für alle erforderlichen Ressourcen abzurufen.
- Dieses Muster verwendet AWS Serverless-Ressourcen, um die Lösung bereitzustellen.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen hinweg zu verwalten.

- AWS CloudTrail unterstützt Sie bei der Prüfung der Governance, Compliance und des Betriebsrisikos Ihres AWS-Kontos.
- AWS Glue ist ein vollständig verwalteter ETL-Service (Extract, Transform, Load). Es hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue-Crawler und eine AWS Glue Data Catalog-Tabelle.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon QuickSight ist ein Cloud-Scale Business Intelligence (BI)-Service, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im GitHub infrastructure-assessment-iac-automationRepository verfügbar.

Das Code-Repository enthält die folgenden Dateien und Ordner:

- `lib` Ordner – Das AWS-CDK-Konstrukt Python-Dateien, die zum Erstellen von AWS-Ressourcen verwendet werden
- `src/lambda_code` – Der Python-Code, der in der Lambda-Funktion ausgeführt wird
- `requirements.txt` – Die Liste aller Python-Abhängigkeiten, die installiert werden müssen
- `cdk.json` – Die Eingabedatei, um Werte bereitzustellen, die zum Hochfahren von Ressourcen erforderlich sind

Bewährte Methoden

Richten Sie die Überwachung und Warnung für die Lambda-Funktion ein. Weitere Informationen finden Sie unter Überwachung und Fehlerbehebung bei Lambda-Funktionen. Allgemeine bewährte Methoden für die Arbeit mit Lambda-Funktionen finden Sie in der AWS-Dokumentation.

Sekunden

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihrem lokalen Computer.	Führen Sie zum Klonen des Repositorys den Befehl `git clone https://github.com/aws-samples/infrastructure-assessment-iac-automation.git` aus.	AWS DevOps, DevOps Techniker

Richten Sie die virtuelle Python-Umgebung ein und installieren Sie die erforderlichen Abhängigkeiten.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd infrastructure-assessment-iac-automation`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Führen Sie den Befehl aus, um die erforderlichen Abhängigkeiten einzurichten`pip install -r requirements.txt .`
		AWS DevOps, DevOps Techniker

Richten Sie die AWS-CDK-Umgebung ein und synthetisieren Sie den AWS-CDK-Code.	1. Um die AWS-CDK-Umgebung in Ihrem AWS-Konto einzurichten, führen Sie den Befehl aus`cdk bootstrap aws://ACC`	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`OUNT-NUMBER/REGION`. 2. Um den Code in eine AWS-CloudFormation Stack-Konfiguration zu konvertieren, führen Sie den Befehl aus `cdk synth`.	

Einrichten von AWS-Anmeldeinformationen auf Ihrem lokalen Computer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die Region, in der der Stack bereitgestellt wird.	Um AWS-Anmeldeinformationen für AWS CDK mithilfe von Umgebungsvariablen bereitzustellen, führen Sie die folgenden Befehle aus.
	`export CDK_DEFAULT_ACCOUNT=<12 Digit AWS Account Number>`
	`export CDK_DEFAULT_REGION=<region>`
		AWS DevOps, DevOps Techniker

Richten Sie das AWS CLI-Profil ein.	Um das AWS CLI-Profil für das Konto einzurichten, folgen Sie den Anweisungen in der AWS-Dokumentation.	AWS DevOps, DevOps Techniker

Konfigurieren und Bereitstellen des Tools zur Ressourcenbewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe von AWS CDK bereitzustellen: 1. Geben Sie im Stammverz eichnis des geklonten Repositorys in der -`cdk.json`Datei Eingaben für die folgenden Parameter an: • `s3_context` • `ct_context` • `kms_context` • `lambda_context` • `glue_context` • `qs_context` Diese Werte definiere n Ressourcenkonfigur ationen und Nomenclat ure. Standardwerte werden festgelegt und können bei Bedarf geändert werden. Hinweis: Um einen Fehler zu vermeiden, der besagt, dass der S3-Bucket bereits vorhanden ist, stellen Sie sicher, dass Sie `s3_context` in den `output` Abschnitten `ct`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und eindeutige Namen für angeben. 2. Um Ressourcen bereitzustellen, führen Sie den Befehl aus `cdk deploy`. Der `cdk deploy` Befehl erstellt eine CloudTrail Ressource, um Ereignisse zu protokollieren und die Protokolldatei im S3-Eingabe-Bucket zu speichern. Die Protokolldateien des Trails werden von der Lambda-Funktion verarbeitet. Die gefilterten Ergebnisse werden im Ausgabe-S3-Bucket gespeichert und können von Amazon Athena und Amazon verwendet werden QuickSight.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue-Crawler aus und erstellen Sie die Data Catalog-Tabelle.	Ein AWS Glue-Crawler wird verwendet, um das Datenschema dynamisch zu halten. Die Lösung erstellt und aktualisiert Partitionen in der AWS Glue Data Catalog-Tabelle, indem der Crawler regelmäßig ausgeführt wird, wie vom AWS Glue-Crawler-Scheduler definiert. Nachdem die Daten im Ausgabe-S3-Bucket verfügbar sind, führen Sie die folgenden Schritte aus, um den AWS Glue-Crawler auszuführen und das Data Catalog-Tabellenschema zum Testen zu erstellen: 1. Melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zur AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Data Catalog die Option Crawler aus. 3. Wählen Sie den `iac-tool-qa-resource-iac-json-crawler` Crawler aus. 4. Führen Sie den Crawler aus. 5. Nachdem der Crawler erfolgreich ausgeführt	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wurde, wird eine AWS Glue Data Catalog-Tabelle erstellt. AWS QuickSight verwendet die Tabelle, um die Daten zu visualisieren. Hinweis: Der AWS-CDK-Code konfiguriert den AWS Glue-Crawler so, dass er zu einem bestimmten Zeitpunkt ausgeführt wird, aber Sie können ihn auch bei Bedarf ausführen.	
Stellen Sie das QuickSight Konstrukt bereit.	1. Um das QuickSight Konstrukt bereitzustellen, kommentieren Sie den Code zwischen `#QuickSight setup - start` und `#QuickSight setup – ends` in aus`resource_iac_tool_stack.py` . 2. Nachdem Sie die Kommentarerstellung aufgehoben haben, führen Sie den `cdk deploy` Befehl aus, um `QuickSight DataSource` und `QuickSight DataSet` im QuickSight Konto zu erstellen.	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das QuickSight Dashboard.	Gehen Sie wie folgt vor, um das Beispiel QuickSight - Dashboard und die Analyse zu erstellen: 1. Navigieren Sie zur QuickSight -Konsole und wählen Sie die AWS-Regio n aus, in der Ressourcen bereitgestellt werden. 2. Wählen Sie im Navigatio nsbereich Datensätze aus und überprüfen Sie, ob im Amazon- QuickSight Datensatz ein Datensatz mit dem Namen erstellt `ct-operations-iac-ds` wurde. Wenn Sie den Datensatz nicht sehen, stellen Sie das QuickSight Konstrukt erneut bereit. 3. Wählen Sie den `ct-operations-iac-ds` Datensatz aus und wählen Sie IN ANALYSE VERWENDEN aus. 4. Wählen Sie das Standardb latt aus. 5. Wählen Sie die entsprech enden Spalten aus der Feldliste auf der linken Seite aus.	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Nachdem Sie die erforderlichen Spalten ausgewählt haben, wählen Sie den entsprechenden Visualisierungstyp aus, um die Daten anzuzeigen. Weitere Informationen finden Sie unter Starten einer Analyse in Amazon QuickSight und Visualisierungstypen in Amazon QuickSight.	

Bereinigen aller AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	1. Um AWS-Ressourcen zu entfernen, die von der Lösung bereitgestellt werden, führen Sie den Befehl aus `cdk destroy`. 2. Löschen Sie alle Objekte aus den beiden S3-Buckets und entfernen Sie dann die Buckets. Weitere Informationen finden Sie unter Löschen eines Buckets.	AWS DevOps, DevOps Techniker

Einrichten zusätzlicher Funktionen zusätzlich zur Automatisierung des AWS-Tools zur Ressourcenbewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen und bereinige n Sie manuell erstellte Ressourcen.	(Optional) Wenn Ihre Organisation Compliance-Anforderungen zum Erstellen von Ressourcen mit IaC-Tools hat, können Sie Complianc e erreichen, indem Sie die Automatisierung des AWS-Tools zur Ressource nbewertung verwenden, um manuell bereitgestellte Ressourcen abzurufen. Sie können das Tool auch verwenden, um die Ressource n in ein IaC-Tool zu importier en oder neu zu erstellen. Führen Sie die folgenden allgemeinen Aufgaben aus, um manuell bereitgestellte Ressourcen zu überwachen: 1. Stellen Sie die Automatis ierung des AWS-Tools zur Ressourcenbewertung bereit. 2. Richten Sie eine Lambda-Funktion ein, um die Athena-Tabellen täglich abzufragen, die relevanten Daten zu manuell bereitges tellten Ressourcen zu finden und sie in eine CSV-Datei (durch Kommas	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	getrennte Werte) zu exportieren. 3. Nachdem die Lambda-Funktion ausgeführt wurde, kann eine Benachrichtigung mit den erforderlichen Daten an die jeweiligen Stakeholder gesendet werden. 4. Für eine längere Aufbewahrung kann die CSV-Datei im S3-Bucket gespeichert werden. 5. Löschen Sie auf der Grundlage der Informationen in der CSV-Datei die manuell erstellten Ressourcen oder importieren Sie sie in eine vorhandene IaC-Lösung.	

Fehlerbehebung

Problem	Lösung
AWS CDK gibt Fehler zurück.	Hilfe zu AWS-CDK-Problemen finden Sie unter Fehlerbehebung bei häufigen AWS-CDK-Problemen.

Zugehörige Ressourcen

- Erstellen von Lambda-Funktionen mit Python

- Erste Schritte mit AWS CDK
- Arbeiten mit AWS CDK in Python
- Erstellen eines CloudTrail Protokoll-Trails
- Erste Schritte mit Amazon QuickSight

Zusätzliche Informationen

Mehrere Konten

Verwenden Sie AWS-Profile, um die AWS CLI-Anmeldeinformationen für mehrere Konten einzurichten. Weitere Informationen finden Sie im Abschnitt Konfigurieren mehrerer Profile unter Einrichten der AWS CLI.

AWS-CDK-Befehle

Beachten Sie bei der Arbeit mit AWS CDK die folgenden nützlichen Befehle:

- Listet alle Stacks in der App auf

```
cdk ls
```

- Gibt die synthetisierte AWS- CloudFormation Vorlage aus

```
cdk synth
```

- Stellt den Stack für Ihr Standard-AWS-Konto und Ihre Region bereit

```
cdk deploy
```

- Vergleicht den bereitgestellten Stack mit dem aktuellen Status

```
cdk diff
```

- Öffnet die AWS-CDK-Dokumentation

```
cdk docs
```

Installieren Sie SAP-Systeme automatisch mithilfe von Open-Source-Tools

Erstellt von Guilherme Sheim (AWS)

Code-Repository: Haupt-Repository	Umgebung: Produktion	Technologien: DevOps
Workload: SAP	AWS-Services: Amazon EC2; Amazon S3	

Übersicht

Dieses Muster zeigt, wie Sie die Installation von SAP-Systemen mithilfe von Open-Source-Tools automatisieren, um die folgenden Ressourcen zu erstellen:

- Eine SAP S/4HANA 1909-Datenbank
- Eine SAP ABAP Central Services (ASCS)-Instance
- Eine SAP Primary Application Server (PAS)-Instance

HashiCorp Terraform erstellt die Infrastruktur des SAP-Systems und Ansible konfiguriert das Betriebssystem (OS) und installiert SAP-Anwendungen. Jenkins führt die Installation aus.

Diese Einrichtung macht die Installation von SAP-Systemen zu einem wiederholbaren Prozess, der dazu beitragen kann, die Effizienz und Qualität der Bereitstellung zu erhöhen.

Hinweis: Der in diesem Muster bereitgestellte Beispielcode funktioniert sowohl für Systeme mit hoher Verfügbarkeit (HA) als auch für Nicht-HA-Systeme.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket, der alle Ihre SAP-Mediendateien enthält

- Ein AWS Identity and Access Management (IAM)-Prinzipal mit einem Zugriffsschlüssel und einem geheimen Schlüssel , der über die folgenden Berechtigungen verfügt:
  - Schreibgeschützte Berechtigungen: Amazon Route 53, AWS Key Management Service (AWS KMS)
  - Lese- und Schreibberechtigungen: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB
- Eine privat gehostete Route 53-Zone https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html
- Ein Abonnement für Red Hat Enterprise Linux für SAP mit HA und Update Services 8.2 Amazon Machine Image (AMI) in Amazon Marketplace
- Kundenverwalteter AWS KMS-Schlüssel
- Ein Secure Shell (SSH)-Schlüsselpaar
- Eine Amazon EC2-Sicherheitsgruppe, die eine SSH-Verbindung auf Port 22 vom Hostnamen zulässt, auf dem Sie Jenkins installieren (der Hostname ist höchstwahrscheinlich localhost)
- Vagrant nach HashiCorp installiert und konfiguriert
- VirtualBox von Oracle installiert und konfiguriert
- Vertrautheit mit Git, Terraform, Ansible und Jenkins

Einschränkungen

- Nur SAP S/4HANA 1909 wurde vollständig für dieses spezifische Szenario getestet. Der Ansible-Beispielcode in diesem Muster erfordert Änderungen, wenn Sie eine andere Version von SAP HANA verwenden.
- Das Beispielverfahren in diesem Muster funktioniert für Mac OS- und Linux-Betriebssysteme. Einige der Befehle können nur in Unix-basierten Terminals ausgeführt werden. Sie können jedoch ein ähnliches Ergebnis erzielen, indem Sie verschiedene Befehle und ein Windows-Betriebssystem verwenden.

Produktversionen

- SAP S/4HANA 1909
- Red Hat Enterprise Linux (RHEL) 8.2 oder höhere Versionen

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow, der Open-Source-Tools verwendet, um die Installation von SAP-Systemen in einem AWS-Konto zu automatisieren:

Das Diagramm zeigt den folgenden Workflow:

1. Jenkins orchestriert die Ausführung der SAP-Systeminstallation durch die Ausführung von Terraform- und Ansible-Code.
2. Terraform-Code baut die Infrastruktur des SAP-Systems auf.
3. Ansibler Code konfiguriert das Betriebssystem und installiert SAP-Anwendungen.
4. Auf einer Amazon EC2-Instance werden eine SAP S/4HANA 1909-Datenbank, eine ASCS-Instance und eine PAS-Instance installiert, die alle definierten Voraussetzungen enthalten.

Hinweis: Die Beispieleinrichtung in diesem Muster erstellt automatisch einen Amazon S3-Bucket in Ihrem AWS-Konto, um die Terraform-Statusdatei zu speichern.

Technologie-Stack

- Terraform
- Ansible
- Jenkins
- Eine SAP S/4HANA 1909-Datenbank
- Eine SAP ASCS-Instance
- Eine SAP PAS-Instance
- Amazon EC2

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und sie schnell nach oben oder unten skalieren.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Key Management Service (AWS KMS) unterstützt Sie beim Erstellen und Steuern kryptografischer Schlüssel zum Schutz Ihrer Daten.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Andere Tools

- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.
- Ansible ist ein Open-Source-Tool zur Konfiguration als Code (CaC), das bei der Automatisierung von Anwendungen, Konfigurationen und IT-Infrastruktur hilft.
- Jenkins ist ein Open-Source-Automatisierungsserver, mit dem Entwickler ihre Software erstellen, testen und bereitstellen können.

Code

Der Code für dieses Muster ist im GitHub aws-install-sap-with-jenkins-ansible-Repository verfügbar.

Polen

Konfigurieren der Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Ihre SAP-Mediendateien zu einem Amazon S3-Bucket hinzu.	Erstellen Sie einen Amazon S3-Bucket, der alle Ihre SAP-Mediendateien enthält. Wichtig: Stellen Sie sicher, dass Sie die Ordnerhierarchie des AWS Launch Wizard für S/4HANA in der Dokumenta	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tion des Launch Wizard befolgen.	
Installieren Sie VirtualBox.	Installieren und konfigurieren Sie VirtualBox von Oracle.	DevOps Techniker
Installieren Sie Vagrant.	Installieren und konfigurieren Sie Vagrant von HashiCorp.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihr AWS-Konto.	1. Stellen Sie sicher, dass Sie über einen IAM-Prinzipal mit einem Zugriffsschlüssel und einem geheimen Schlüssel verfügen und über die folgenden Berechtigungen verfügen: • Schreibgeschützte Berechtigungen:Amazon Route 53, AWS Key Management Service (AWS KMS) • Lese- und Schreibbe rechtigungen:Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatc h, Amazon DynamoDB 2. Speichern Sie den Zugriffss chlüssel und den geheimen Schlüssel des IAM-Prinz ipals zur späteren Referenz. 3. Erstellen Sie eine privat gehostete Route 53-Zone, falls Sie noch keine haben. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html Speichern Sie den Zonennamen (z. B. sapteam.net) zur späteren Referenz.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Abonnieren Sie das Red Hat Enterprise Linux für SAP mit HA und Update Services 8.2 AMI in Amazon Marketplace. Speichern Sie die AMI-ID (z. B. ami-0000000) zur späteren Referenz. 5. Erstellen Sie einen vom Kunden verwalteten AWS KMS-Schlüssel. Speichern Sie den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels zur späteren Referenz. Hinweis: Im Folgenden finden Sie ein Beispiel für einen vom Kunden verwalteten AWS KMS-Schlüssel-ARN: arn:aws:kms:us-east-1:123412341234:key/uuid 6. Erstellen Sie ein SSH-Schlüsselpaar . Speichern Sie den Namen und die PEM-Datei des Schlüsselpaars zur späteren Referenz. 7. Erstellen Sie eine Amazon EC2-Sicherheitsgruppe, die eine SSH-Verbindung auf Port 22 über den Hostnamen zulässt, auf dem Sie Jenkins installie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ren. Speichern Sie die Sicherheitsgruppen-ID zur späteren Referenz. Hinweis: Der Hostname ist höchstwahrscheinlich localhost .	

Erstellen und Ausführen Ihrer SAP-Installation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repository aus GitHub.	Klonen Sie das aws-install-sap-with-jenkins-ansible Repository auf GitHub.	DevOps Techniker
Starten Sie den Jenkins-Service.	Öffnen Sie das Linux-Terminal. Navigieren Sie dann zum lokalen Ordner, der den geklonten Code-Repository-Ordner enthält, und führen Sie den folgenden Befehl aus: `sudo vagrant up` Hinweis: Der Start von Jenkins dauert etwa 20 Minuten. Der Befehl gibt eine Meldung zurück, dass der Service aktiv ist und ausgeführt wird, wenn er erfolgreich ist.	DevOps Techniker
Öffnen Sie Jenkins in einem Webbrowser und melden Sie sich an.	1. Geben Sie in einem Webbrowser http://lo	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	calhost:5555 ein. Jenkins wird geöffnet. 2. Melden Sie sich bei Jenkins an, indem Sie Admin für den Benutzernamen und my_secret_pass_fro m_vault für das Passwort verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihre SAP-Systeminstallationsparameter.	1. Wählen Sie in Jenkins die Option Jenkins verwalten aus. Wählen Sie dann Anmeldeinformation en verwalten aus. Eine Liste der Anmeldein formationsvariablen, die Sie konfigurieren können, wird angezeigt. 2. Konfigurieren Sie alle der folgenden Anmeldein formationsvariablen: • Geben Sie für AWS_ACCOUNT_CREDEN TIALS die Zugriffsschlüssel-ID Ihres IAM-Prinzipals und die ID des geheimen Zugriffsschlüssels ein. • Geben Sie für AMI_ID das Red Hat Enterprise Linux für SAP mit HA und die AMI-ID des Update Services 8.2 AMI ein. • Geben Sie für KMS_KEY_A RN den ARN Ihres kundenverwalteten AWS KMS-Schlüssels ein. • Geben Sie für SSH_KEYPA IR_NAME den Namen Ihres SSH-Schlüsselpaars ein, ohne den PEM-Dateityp einzugeben.	AWS-Systemadministrator, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Geben Sie für SSH_KEYPAIR_FILE den vollständigen Namen der PEM-Datei Ihres Schlüsselpaars ein (z. B. mykeypair.pem). Stellen Sie sicher, dass Sie auch die PEM-Datei der Schlüsselpaare in Jenkins hochladen. • Geben Sie für S3_ROOT_FOLDER_INSTALL_FILES den Namen des Amazon S3-Buckets – und ggf. den Ordner – (z. B. s3://my-media-bucket/S4H1909) ein, der Ihre SAP-Mediendateien enthält. • Geben Sie für PRIVATE_DNS_ZONE_NAME den Namen Ihrer privat gehosteten Route 53-Zone ein (z. B. myprivatecompanyurl.net). • Geben Sie für VPC_ID die VPC-ID (z. B. vpc-12345) der Amazon VPC ein, in der Sie die SAP-Ressourcen erstellen. • Geben Sie für SUBNET_IDS zwei öffentliche Subnetz-IDs ein, wenn Sie in einer Testumgebung arbeiten (für zukünftige HA-Funktionen). Wenn Sie in einer Produktionsumgebung arbeiten,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	empfiehlt es sich, zwei private Subnetze mit einem Bastion-Host zu verwenden. • Geben Sie für SECURITY_GROUP_ID die ID der Amazon EC2-Sicherheitsgruppe ein, die eine SSH-Verbindung auf Port 22 über den Hostnamen zulässt, auf dem Sie Jenkins installiert haben. Hinweis: Sie können die anderen nicht erforderlichen Parameter nach Bedarf konfigurieren, je nach Anwendungsfall. Sie können beispielsweise die SAP-System-ID (SID) der Instances, das Standardpasswort, die Namen und Tags für Ihr SAP-System ändern. Alle erforderlichen Variablen haben (erforderlich) am Anfang ihrer Namen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Ihre SAP-Systeminstallation aus.	1. Wählen Sie in Jenkins Jenkins Home aus. Wählen Sie dann SAP Hana+ASCS +PAS 3 Instances aus. 2. Wählen Sie Hochfahren und installieren Sie . Wählen Sie dann Haupt aus. 3. Wählen Sie Jetzt erstellen aus. Informationen zu den Pipeline-Schritten finden Sie im Abschnitt Grundlegendes zu den Pipeline-Schritten unter Automatisierung der SAP-Installation mit Open-Source-Tools im AWS-Blog. Hinweis: Wenn ein Fehler auftritt, verschieben Sie den Cursor über das rote Fehlerfeld, das angezeigt wird, und wählen Sie Protokolle aus. Die Protokolle für den fehlerhaften Pipeline-Schritt werden angezeigt. Die meisten Fehler treten aufgrund falscher Parametereinstellungen auf.	DevOps Techniker, AWS-Systemadministrator

Zugehörige Ressourcen

- DevOps für SAP – SAP-Installation: Von 2 Monaten bis 2 Stunden (DevOps Enterprise Summit Video Library)

Automatisieren der Portfolio- und Produktbereitstellung von AWS Service Catalog mithilfe von AWS CDK

Erstellt von Sandeep Gawande (AWS), RAJNEESH TYAGI (AWS) und Viyoma Sachdeva (AWS)

Code-Repository: aws-cdk-servicecatalog-automation	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur; Management und Governance
Workload: Open-Source	AWS-Services: AWS Service Catalog; AWS CDK	

Übersicht

AWS Service Catalog hilft Ihnen dabei, Kataloge von IT-Services oder Produkten, die für die Verwendung in der AWS-Umgebung Ihrer Organisation genehmigt sind, zentral zu verwalten. Eine Sammlung von Produkten wird als Portfolio bezeichnet, und ein Portfolio enthält auch Konfigurationsinformationen. Mit AWS Service Catalog können Sie ein benutzerdefiniertes Portfolio für jeden Benutzertyp in Ihrer Organisation erstellen und dann Zugriff auf das entsprechende Portfolio gewähren. Diese Benutzer können dann schnell jedes Produkt bereitstellen, das sie im Portfolio benötigen.

Wenn Sie über eine komplexe Netzwerkinfrastruktur verfügen, z. B. Architekturen mit mehreren Regionen und Konten, wird empfohlen, Service-Catalog-Portfolios in einem einzigen, zentralen Konto zu erstellen und zu verwalten. Dieses Muster beschreibt, wie Sie AWS Cloud Development Kit (AWS CDK) verwenden, um die Erstellung von Service-Catalog-Portfolios in einem zentralen Konto zu automatisieren, Endbenutzern Zugriff darauf zu gewähren und dann optional Produkte in einem oder mehreren AWS-Zielkonten bereitzustellen. Diese ready-to-use Lösung erstellt die Service-Catalog-Portfolios im Quellkonto. Optional stellt sie auch Produkte in Zielkonten mithilfe von AWS-CloudFormation Stacks bereit und hilft Ihnen bei der Konfiguration TagOptions für die Produkte:

- AWS CloudFormation StackSets – Sie können verwenden StackSets , um Service-Catalog-Produkte über mehrere AWS-Regionen und -Konten hinweg zu starten. Bei dieser Lösung haben Sie die Möglichkeit, bei der Bereitstellung dieser Lösung Produkte automatisch bereitzustellen. Weitere Informationen finden Sie unter Verwenden von AWS CloudFormation StackSets (Dokumentation zum Service Catalog) und StackSets Konzepten (CloudFormation Dokumentation).

- -TagOption Bibliothek – Sie können Tags für bereitgestellte Produkte mithilfe der - TagOption Bibliothek verwalten. Ein TagOption ist ein Schlüssel-Wert-Paar, das in AWS Service Catalog verwaltet wird. Es handelt sich nicht um ein AWS-Tag, sondern dient als Vorlage für die Erstellung eines AWS-Tags basierend auf dem TagOption. Weitere Informationen finden Sie in der -TagOption Bibliothek (Dokumentation zum Service Catalog).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto, das Sie als Quellkonto für die Verwaltung von Service-Catalog-Portfolios verwenden möchten.
- Wenn Sie diese Lösung verwenden, um Produkte in einem oder mehreren Zielkonten bereitzustellen, muss das Zielkonto bereits vorhanden und aktiv sein.
- AWS Identity and Access Management (IAM)-Berechtigungen für den Zugriff auf AWS Service Catalog CloudFormation , AWS und AWS IAM.

Produktversionen

- AWS-CDK-Version 2.27.0

Architektur

Zieltechnologie-Stack

- Service Catalog-Portfolios in einem zentralen AWS-Konto
- Service-Catalog-Produkte, die im Zielkonto bereitgestellt werden

Zielarchitektur

1. Im Portfolio (oder Quellkonto) aktualisieren Sie die Datei config.json mit dem AWS-Konto, der AWS-Region, der IAM-Rolle, dem Portfolio und den Produktinformationen für Ihren Anwendungsfall.
2. Sie stellen die AWS-CDK-Anwendung bereit.

3. Die AWS-CDK-Anwendung übernimmt die Bereitstellungs-IAM-Rolle und erstellt die Service Catalog-Portfolios und -Produkte, die in der Datei config.json definiert sind.

   Wenn Sie für StackSets die Bereitstellung von Produkten in einem Zielkonto konfiguriert haben, wird der Prozess fortgesetzt. Wenn Sie nicht StackSets für die Bereitstellung von Produkten konfiguriert haben, ist der Vorgang abgeschlossen.
4. Die AWS-CDK-Anwendung übernimmt die StackSet Administratorrolle und stellt das AWS-CloudFormation Stack-Set bereit, das Sie in der Datei config.json definiert haben.
5. StackSets Übernimmt im Zielkonto die StackSet Ausführungsrolle und stellt die Produkte bereit.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS Cloud-Infrastruktur im Code unterstützt.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, das Sie bei der Interaktion mit Ihrer AWS-CDK-App unterstützt.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Service Catalog hilft Ihnen dabei, Kataloge von IT-Services, die für AWS genehmigt sind, zentral zu verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Code-Repository

Der Code für dieses Muster ist auf GitHubim aws-cdk-servicecatalog-automationRepository verfügbar. Das Code-Repository enthält die folgenden Dateien und Ordner:

- cdk-sevicecatalog-app – Dieser Ordner enthält die AWS-CDK-Anwendung für diese Lösung.
- config – Dieser Ordner enthält die Datei config.json und die CloudFormation Vorlage für die Bereitstellung der Produkte im Service-Catalog-Portfolio.

- config/config.json – Diese Datei enthält alle Konfigurationsinformationen. Sie aktualisieren diese Datei, um diese Lösung an Ihren Anwendungsfall anzupassen.
- config/templates – Dieser Ordner enthält die CloudFormation Vorlagen für die Service Center-Produkte.
- setup.sh – Dieses Skript stellt die Lösung bereit.
- uninstall.sh – Dieses Skript löscht den Stack und alle AWS-Ressourcen, die bei der Bereitstellung dieser Lösung erstellt wurden.

Um den Beispiel-Code zu verwenden, folgen Sie den Anweisungen im Abschnitt „Epics“.

Bewährte Methoden

- IAM-Rollen, die zur Bereitstellung dieser Lösung verwendet werden, sollten dem Prinzip der geringsten Berechtigung entsprechen (IAM-Dokumentation).
- Halten Sie sich an die Bewährten Methoden für die Entwicklung von Cloud-Anwendungen mit AWS CDK (AWS-Blogbeitrag).
- Halten Sie sich an die CloudFormation bewährten Methoden von AWS (CloudFormation Dokumentation).

Polen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS CDK Toolkit.	Stellen Sie sicher, dass Sie AWS CDK Toolkit installiert haben. Geben Sie den folgenden Befehl ein, um zu bestätigen, ob er installiert ist, und überprüfen Sie die Version. `cdk --version`	AWS DevOps, DevOps Engineering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Wenn AWS CDK Toolkit nicht installiert ist, geben Sie den folgenden Befehl ein, um es zu installieren.
	`npm install -g aws-cdk@2.27.0`
	Wenn die AWS-CDK-Toolkit-Version älter als 2.27.0 ist, geben Sie den folgenden Befehl ein, um sie auf Version 2.27.0 zu aktualisieren.
	`npm install -g aws-cdk@2.27.0 --force`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	Geben Sie den folgenden Befehl ein. Unter Repository klonen im Abschnitt Zusätzliche Informationen können Sie den vollständigen Befehl kopieren, der die URL für das Repository enthält. Dadurch wird das aws-cdk-servicecatalog-automationRepository von geklont GitHub.
	`git clone <repository-URL>.git`
	Dadurch wird ein `cd aws-cdk-servicecatalog-automation` Ordner im Zielverzeichnis erstellt. Geben Sie den folgenden Befehl ein, um zu diesem Ordner zu navigieren.
	`cd aws-cdk-servicecatalog-automation`
		AWS DevOps, DevOps Engineering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie AWS-Anmeldeinformationen ein.	Geben Sie die folgenden Befehle ein. Diese exportieren die folgenden Variablen, die das AWS-Konto und die Region definieren, in der Sie den Stack bereitstellen.
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<AWS Region>`
	AWS-Anmeldeinformationen für AWS CDK werden über Umgebungsvariablen bereitgestellt.
		AWS DevOps, DevOps Engineering

Konfigurieren Sie Berechtigungen für Endbenutzer-IAM-Rollen.	Wenn Sie IAM-Rollen verwenden, um Zugriff auf das Portfolio und die darin enthaltenen Produkte zu gewähren, müssen die Rollen über Berechtigungen verfügen, die vom servicecatalog.amazonaws.com-Serviceprinzipal übernommen werden können. Anweisungen zum Erteilen dieser Berechtigungen finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs mit Service Catalog (Dokumentation zu AWS Organizations).	AWS DevOps, DevOps Engineering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die für erforderlichen IAM-Rollen StackSets.	Wenn Sie verwenden, StackSets um Produkte automatisch in Zielkonten bereitzustellen, müssen Sie die IAM-Rollen konfigurieren, die das Stack-Set verwalten und ausführen. 1. Überprüfen Sie im Quellkonto, ob `AWSCloudFormationStackSetAdministrationRole` bereits vorhanden ist. Überprüfen Sie in den Zielkonten, ob `AWSCloudFormationStackSetExecutionRole` bereits vorhanden ist. Wenn diese Rollen bereits vorhanden sind, können Sie mit dem nächsten Epos fortfahren. 2. Folgen Sie den Anweisungen unter Selbstverwaltete Berechtigungen gewähren (IAM-Dokumentation), um die Stack-Set-Verwaltungsrolle im Portfoliokonto zu erstellen und die Ausführungsrolle in jedem Zielkonto zu erstellen.	AWS DevOps, DevOps Engineering

Anpassen und Bereitstellen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CloudFormation Vorlagen.	Erstellen Sie im `config/templates` Ordner CloudFormation Vorlagen für alle Produkte, die Sie in Ihre Portfolios aufnehmen möchten. Weitere Informationen finden Sie unter Arbeiten mit AWS- CloudFormation Vorlagen (CloudFormation Dokumentation).	App-Entwickler, AWS DevOps, DevOps Techniker

Passen Sie die Konfigurationsdatei an.	Öffnen Sie im `config` Ordner die Datei config.json und definieren Sie die Parameter entsprechend Ihrem Anwendungsfall. Die folgenden Parameter sind erforderlich, sofern nicht anders angegeben:
	• Definieren Sie im `portfolios` Abschnitt die folgenden Parameter, um ein oder mehrere Service-Catalog-Portfolios zu erstellen:
	  • `portfolioName` – Der Name des Portfolios.
	  • `providerName` – Der Name der Person, des Teams oder der Organisation, die das Portfolio verwaltet.
		App-Entwickler, DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `description` – Eine kurze Beschreibung des Portfolios. • `roles` – (Optional) Namen aller IAM-Rolle n, die Zugriff auf dieses Portfolio haben sollen. Benutzer mit dieser Rolle können auf die Produkte in diesem Portfolio zugreifen. • `users` – (Optional) Namen aller IAM-Benut zer, die Zugriff auf dieses Portfolio und seine Produkte haben sollen. • `groups` – (Optional) Namen aller IAM-Benut zergruppen, die Zugriff auf dieses Portfolio und seine Produkte haben sollen. Warnung: IAM-Benutzer verfügen über langfrist ige Anmeldeinformation en, was ein Sicherhei tsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, dass Sie diesen Benutzern nur die Berechtigungen gewähren, die sie zur Ausführung der Aufgabe benötigen, und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	dass Sie diese Benutzer entfernen, wenn sie nicht mehr benötigt werden.
	
	Wichtig: `roles`, `users`und `groups` sind alle optionale n Parameter. Wenn Sie jedoch keinen dieser Parameter definieren, kann niemand die Portfolio produkte in der Service-C atalog-Konsole anzeigen. Definieren Sie mindesten s einen dieser Parameter . Weitere Informationen finden Sie unter Erteilen von Berechtigungen für Service-Catalog-Endbenutzer (Dokumentation zu Service Catalog).
	• (Optional) Definieren Sie im `tagOption` Abschnitt TagOptions für die Produkte:
	  • `key` – Name des TagOption Schlüssels
	  • `value` – Zulässige Zeichenfolgenwerte für die TagOption
	
	Weitere Informationen finden Sie in der -TagOption Bibliothek (Dokumentation zum Service Catalog).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Definieren Sie im `products` Abschnitt die folgenden Parameter für die Produkte:
	  • `portfolioName` – Der Name des Portfolios, zu dem Sie das Produkt hinzufügen möchten. Sie können nur ein Portfolio angeben.
	  • `productName` – Der Name des Produkts.
	  • `owner` – Der Besitzer des Produkts.
	  • `productVersionName` – Der Name der Produktversion im Zeichenfolgenwert, z. B. `v1`.
	  • `templatePath` – Der Dateipfad für die CloudFormation Vorlage für das Produkt.
	  • `deployWithStackSets` – (Optional) Geben Sie ein oder mehrere Konten und Regionen an, mit denen Sie Produkte StackSets automatisch in den Portfolios bereitstellen möchten. Wenn Sie diese Bereitstellungsoption verwenden, sind alle folgenden Parameter in	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	diesem Abschnitt erforderlich: • `accounts` – Die Zielkonten. • `regions` – Die Zielregionen. • `stackSetAdministrationRoleName` – Der Name der IAM-Rolle, die zur Verwaltung der StackSets Konfiguration verwendet wird. Ändern Sie diesen Wert nicht. Diese Rolle muss genau diesen Namen haben. • `stackSetExecutionRoleName` – Der Name der IAM-Rolle im Zielkonto, das die Stack-Instances bereitstellt. Ändern Sie diesen Wert nicht. Diese Rolle muss genau diesen Namen haben. Ein Beispiel für eine abgeschlossene Konfigurationsdatei finden Sie unter Beispielk	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onfigurationsdatei im Abschnitt Zusätzliche Informationen.	
Stellen Sie die Lösung bereit.	Geben Sie den folgenden Befehl ein. Dadurch wird die AWS-CDK-App bereitgestellt und die Service Catalog-P ortfolios und -Produkte werden wie in der Datei config.json angegeben bereitgestellt. `sh +x setup.sh`	App-Entwickler, DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitstellung.	Überprüfen Sie die erfolgreiche Bereitstellung, indem Sie wie folgt vorgehen: 1. Melden Sie sich bei der AWS-Managementkonsole mit Anmeldeinformationen an, die auf eines oder mehrere der Portfolios zugreifen können, die Sie in der Konfigurationsdatei definiert haben. 2. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/. 3. Wählen Sie im Navigationsbereich unter Bereitstellung die Option Produkte aus. Stellen Sie sicher, dass eine Liste der Produkte angezeigt wird, die Sie für das Portfolio angegeben haben. 4. Folgen Sie den Anweisungen unter Starten eines Produkts (Dokumentation zum Service Catalog), um eines der verfügbaren Produkte zu starten. Vergewissern Sie sich, dass die verfügbaren Produktversionen und Tags mit den Werten übereinstimmen,	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Sie in der Konfigura tionsdatei angegeben haben. 5. Wenn Sie sich für die automatische Bereitstellung von Produkten in einem oder mehreren Zielkonte n mithilfe von entschieden haben StackSets, gehen Sie wie folgt vor: a. Melden Sie sich mit Anmeldeinformationen an, mit denen Sie die bereitgestellten Produkte in einem der Zielkonten anzeigen können. b. Wählen Sie in der Service-Catalog-Konsole im Navigationsbereich unter Bereitstellung die Option Bereitgestellte Produkte aus. c. Vergewissern Sie sich, dass die erwarteten Produkte in der Liste erscheinen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Aktualisieren Sie die Portfolios und Produkte.	Wenn Sie diese Lösung verwenden möchten, um die Portfolios oder Produkte zu aktualisieren oder neue Produkte bereitzustellen: 1. Nehmen Sie die erforderlichen Änderungen in der Datei config.json vor. 2. Fügen Sie CloudFormation Vorlagen nach Bedarf im `config/template` Ordner hinzu oder ändern Sie sie. 3. Stellen Sie die Lösung erneut bereit. Sie können beispielsweise zusätzliche Portfolios hinzufügen oder mehr Ressourcen bereitstellen. Die AWS-CDK-App implementiert nur die Änderungen. Wenn es keine Änderungen an zuvor bereitgestellten Portfolios oder Produkten gibt, wirkt sich die erneute Bereitstellung nicht auf sie aus.	App-Entwickler, DevOps Techniker, Allgemeines AWS

Bereinigen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Entfernen Sie AWS-Ressourcen, die von dieser Lösung bereitgestellt werden.	Wenn Sie ein bereitgestelltes Produkt löschen möchten, folgen Sie den Anweisungen unter Löschen bereitgestellter Produkte (Dokumentation zum Service Catalog). Wenn Sie alle von dieser Lösung erstellten Ressourcen löschen möchten, geben Sie den folgenden Befehl ein. `sh uninstall.sh`	AWS DevOps, DevOps Techniker, App-Entwickler

Zugehörige Ressourcen

- AWS Service Catalog Construct Library (AWS-API-Referenz)
- StackSets Konzepte (CloudFormation Dokumentation)
- AWS Service Catalog (AWS-Marketing)
- Verwenden von Service Catalog mit dem AWS CDK (AWS-Workshop)

Zusätzliche Informationen

Zusätzliche Informationen

Klonen des Repositorys

Geben Sie den folgenden Befehl ein, um das Repository von zu klonen GitHub.

```
git clone https://github.com/aws-samples/aws-cdk-servicecatalog-automation.git
```

Beispielkonfigurationsdatei

Im Folgenden finden Sie ein Beispiel für eine config.json-Datei mit Beispielwerten.

```
{
    "portfolios": [
        {
            "displayName": "EC2 Product Portfolio",
            "providerName": "User1",
            "description": "Test1",
            "roles": [
                "<Names of IAM roles that can access the products>"
            ],
            "users": [
                "<Names of IAM users who can access the products>"
            ],
            "groups": [
                "<Names of IAM user groups that can access the products>"
            ]
        },
        {
            "displayName": "Autoscaling Product Portfolio",
            "providerName": "User2",
            "description": "Test2",
            "roles": [
                "<Name of IAM role>"
            ]
        }
    ],
    "tagOption": [
        {
            "key": "Group",
            "value": [
                "finance",
                "engineering",
                "marketing",
                "research"
            ]
        },
        {
            "key": "CostCenter",
            "value": [
                "01",
                "02",
                "03",
                "04"
```

```
            ]
        },
        {
            "key": "Environment",
            "value": [
                "dev",
                "prod",
                "stage"
            ]
        }
    ],
    "products": [
        {
            "portfolioName": "EC2 Product Profile",
            "productName": "Ec2",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template1.json"
        },
        {
            "portfolioName": "Autoscaling Product Profile",
            "productName": "autoscaling",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template2.json",
            "deployWithStackSets": {
                "accounts": [
                    "012345678901",
                ],
                "regions": [
                    "us-west-2"
                ],
                "stackSetAdministrationRoleName":
 "AWSCloudFormationStackSetAdministrationRole",
                "stackSetExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
            }
        }
    ]
}
```

Automatisieren von ereignisgesteuerten Backups von CodeCommit zu Amazon S3 mithilfe von CodeBuild und - CloudWatch Ereignissen

Erstellt von Kirankumar Chandrashekar (AWS)

Umgebung: Produktion	Technologien: DevOps; Speicher und Backup	Workload: Alle anderen Workloads
AWS-Services: Amazon S3; Amazon CloudWatch; AWS CodeBuild; AWS CodeCommit		

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie AWS verwenden, CodeCommit um sichere Git-basierte Repositorys zu hosten. CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice. Wenn ein CodeCommit Repository jedoch versehentlich gelöscht wird, wird sein Inhalt ebenfalls gelöscht und kann nicht wiederhergestellt werden.

Dieses Muster beschreibt, wie ein CodeCommit Repository automatisch in einem Amazon Simple Storage Service (Amazon S3)-Bucket gesichert wird, nachdem eine Änderung am Repository vorgenommen wurde. Wenn das CodeCommit Repository später gelöscht wird, bietet Ihnen diese Backup-Strategie eine point-in-time Wiederherstellungsoption.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandenes CodeCommit Repository, in dem der Benutzerzugriff entsprechend Ihren Anforderungen konfiguriert ist. Weitere Informationen finden Sie unter Einrichten von für AWS CodeCommit in der - CodeCommit Dokumentation.
- Ein S3-Bucket zum Hochladen der CodeCommit Backups.

Einschränkungen

- Dieses Muster sichert automatisch alle Ihre CodeCommit Repositorys. Wenn Sie einzelne CodeCommit Repositorys sichern möchten, müssen Sie die Amazon CloudWatch Events-Regel ändern.

Architektur

Das folgende Diagramm veranschaulicht den Workflow für dieses Muster.

Der Workflow besteht aus folgenden Schritten:

1. Code wird in ein CodeCommit Repository übertragen.
2. Das CodeCommit Repository benachrichtigt CloudWatch Ereignisse über eine Repository-Änderung (z. B. einen `-git push`Befehl).
3. CloudWatch Events ruft AWS auf CodeBuild und sendet ihm die CodeCommit Repository-Informationen.
4. CodeBuild klont das gesamte CodeCommit Repository und verpackt es in eine ZIP-Datei.
5. CodeBuild lädt die ZIP-Datei in einen S3-Bucket hoch.

Technologie-Stack

- CloudWatch Ereignisse
- CodeBuild
- CodeCommit
- Amazon S3

Tools

- Amazon CloudWatch Events – CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.

- AWS CodeBuild – CodeBuild ist ein vollständig verwalteter Service für die kontinuierliche Integration, der Quellcode kompiliert, Tests ausführt und Softwarepakete erstellt, die bereitgestellt werden können.

- AWS CodeCommit – CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet.
- AWS Identity and Access Management (IAM) – IAM ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.

Polen

Erstellen eines CodeBuild Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CodeBuild Servicerolle.	Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole. Wählen Sie Rollen und dann Rolle erstellen aus. Erstellen Sie eine Servicerolle für , CodeBuild um das CodeCommit Repository zu klonen, Dateien in den S3-Bucket hochzuladen und Protokolle an Amazon zu senden CloudWatch. Weitere Informationen finden Sie unter Erstellen einer CodeBuild Servicerolle in der - CodeBuild Dokumentation.	Cloud-Administrator
Erstellen Sie ein CodeBuild Projekt.	Wählen Sie in der CodeBuild -Konsole CodeBuild Projekt erstellen aus. Erstellen Sie ein	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeBuild Projekt mithilfe der `buildspec.yml` Vorlage aus dem Abschnitt Zusätzliche Informationen. Hilfe zu dieser Geschichte finden Sie unter Erstellen eines Build-Projekts in der - CodeBuild Dokumentation.	

Erstellen und Konfigurieren der CloudWatch Ereignisregel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für CloudWatch Ereignisse.	Wählen Sie in der IAM-Konsole Rollen und erstellen Sie eine IAM-Rolle für CloudWatch Ereignisse. Weitere Informationen dazu finden Sie unter CloudWatch Events IAM role in der IAM-Dokumentation. Wichtig: Sie müssen der IAM-Rolle für CloudWatch Ereignisse `codebuild:StartBuild` Berechtigungen hinzufügen.	Cloud-Administrator
Erstellen Sie eine CloudWatch Ereignisregel.	1. Wählen Sie in der - CloudWatch Konsole Ereignisse und dann Regeln aus. Wählen Sie Regel erstellen und verwenden Sie die Regel CloudWatch Ereignisse im Abschnitt Zusätzliche	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen. Dadurch wird eine Regel erstellt, die auf Ereignisänderungen (z. B. - `git push` oder -`git commit`Befehle) in Ihren CodeCommit Repositorys wartet. Weitere Informationen finden Sie unter Erstellen einer CloudWatch Ereignisregel für eine CodeCommit Quelle in der AWS- CodePipeline Dokumentation. 2. Wählen Sie Ziele, Themen und dann Eingabe konfigurieren aus. Wählen Sie Eingabe-Transformator und verwenden Sie den Eingabepfad und die Eingabevorlage aus dem Abschnitt Zusätzliche Informationen. Dadurch wird sichergestellt, dass Ihre CodeCommit Repository-Details analysiert und als Umgebungsvariablen an das CodeBuild Projekt gesendet werden. Weitere Informationen finden Sie im Tutorial zum Eingabe-Transformator in der -CloudWatch Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Details konfigurieren und geben Sie einen Namen und eine Beschreibung für die Regel ein. Wählen Sie Regel erstellen aus. Wichtig: Diese CloudWatch Ereignisregel beschreibt Änderungen in allen Ihren CodeCommit Repositorys. Sie müssen die CloudWatch Ereignisregel ändern, wenn Sie einzelne CodeCommit Repositorys sichern oder separate S3-Buckets für verschiedene Repository-Backups verwenden möchten.	

Zugehörige Ressourcen

Erstellen eines CodeBuild Projekts

- Erstellen einer CodeBuild Servicerolle
- Erstellen eines CodeBuild Projekts
- Erforderliche Berechtigungen für Git-Client-Befehle

Erstellen und Konfigurieren einer CloudWatch Ereignisregel

- Erstellen einer CloudWatch Ereignisregel für eine CodeCommit Quelle
- Verwenden Sie den Eingabe-Transformator, um anzupassen, was an das Ereignisziel übergeben wird
- Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird

- Erstellen einer CloudWatch Ereignis-IAM-Rolle

Zusätzliche Informationen

CodeBuild buildspec.yml-Vorlage

```
version: 0.2
phases:
  install:
    commands:
      - pip install git-remote-codecommit
  build:
    commands:
       - env
       - git clone -b $REFERENCE_NAME codecommit::$REPO_REGION://$REPOSITORY_NAME
       - dt=$(date '+%d-%m-%Y-%H:%M:%S');
       - echo "$dt"
       - zip -yr $dt-$REPOSITORY_NAME-backup.zip ./
       - aws s3 cp $dt-$REPOSITORY_NAME-backup.zip s3:// #substitute a valid S3 Bucket
 Name here
```

CloudWatch Ereignisregel

```
{
  "source": [
    "aws.codecommit"
  ],
  "detail-type": [
    "CodeCommit Repository State Change"
  ],
  "detail": {
    "event": [
      "referenceCreated",
      "referenceUpdated"
    ]
  }
}
```

Beispiel-Eingabe-Transformator für das CloudWatch Ereignisregelziel

Eingabepfad:

```
{"referenceType":"$.detail.referenceType","region":"$.region","repositoryName":"$.detail.reposi
```

Eingabevorlage (Ausdruck füllt die Werte nach Bedarf aus):

```
{
    "environmentVariablesOverride": [
        {
            "name": "REFERENCE_NAME",
            "value": ""
        },
        {
            "name": "REFERENCE_TYPE",
            "value": ""
        },
        {
            "name": "REPOSITORY_NAME",
            "value": ""
        },
        {
            "name": "REPO_REGION",
            "value": ""
        },
        {
            "name": "ACCOUNT_ID",
            "value": ""
        }
    ]
}
```

Automatisieren der Stack-Set-Bereitstellung mithilfe von AWS CodePipeline und AWS CodeBuild

Erstellt von Bolyagar Boln Mani (AWS), Mihir Borkar (AWS) und Raghu Gowda (AWS)

Code-Repository: automated-code-pipeline-stackset-Bereitstellung	Umgebung: Produktion	Technologien: DevOps; Softwareentwicklung und -tests
AWS-Services: AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; AWS Organizations ; AWS CloudFormation		

Übersicht

In Ihren CI/CD-Prozessen (Continuous Integration and Continuous Delivery) möchten Sie Anwendungen möglicherweise automatisch in all Ihren vorhandenen AWS-Konten und in neuen Konten bereitstellen, die Sie Ihrer Organisation in AWS Organizations hinzufügen. Wenn Sie eine CI/CD-Lösung für diese Anforderung entwerfen, CloudFormation ist die delegierte Stack-Set-Administratorfunktion von AWS nützlich, da sie eine Sicherheitsebene ermöglicht, indem der Zugriff auf das Verwaltungskonto eingeschränkt wird. AWS CodePipeline verwendet jedoch das serviceverwaltete Berechtigungsmodell, um Anwendungen in mehreren Konten und Regionen bereitzustellen. Sie müssen das AWS Organizations-Verwaltungskonto verwenden, um mit Stack-Sets bereitzustellen, da AWS die delegierte Stack-Set-Administratorfunktion CodePipeline nicht unterstützt.

Dieses Muster beschreibt, wie Sie diese Einschränkung umgehen können. Das Muster verwendet AWS CodeBuild und ein benutzerdefiniertes Skript, um die Bereitstellung von Stack-Sets mit AWS zu automatisieren CodePipeline. Es automatisiert diese Aktivitäten zur Anwendungsbereitstellung:

- Bereitstellen einer Anwendung als Stack-Sets in vorhandenen Organisationseinheiten (OUs)
- Erweitern der Bereitstellung einer Anwendung auf zusätzliche OUs und Regionen
- Entfernen einer bereitgestellten Anwendung aus allen oder bestimmten OUs oder Regionen

Voraussetzungen und Einschränkungen

Voraussetzungen

Bevor Sie die Schritte in diesem Muster ausführen:

- Erstellen Sie Organisationen in Ihrem AWS Organizations-Verwaltungskonto. Anweisungen finden Sie in der AWS Organizations-Dokumentation.
- Aktivieren Sie den vertrauenswürdigen Zugriff zwischen AWS Organizations und CloudFormation , um serviceverwaltete Berechtigungen zu verwenden. Anweisungen finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs mit AWS Organizations in der - CloudFormation Dokumentation.

Einschränkungen

Der Code, der mit diesem Muster geliefert wird, hat die folgenden Einschränkungen:

- Sie können nur eine einzelne CloudFormation Vorlage für eine Anwendung bereitstellen; die Bereitstellung mehrerer Vorlagen wird derzeit nicht unterstützt.
- Die Anpassung der aktuellen Implementierung erfordert DevOps Fachwissen.
- Dieses Muster verwendet keine AWS Key Management System (AWS KMS)-Schlüssel. Sie können diese Funktionalität jedoch aktivieren, indem Sie die in diesem Muster enthaltene CloudFormation Vorlage neu konfigurieren.

Architektur

Diese Architektur für die CI/CD-Bereitstellungspipeline verarbeitet Folgendes:

- Schränkt den direkten Zugriff auf das Verwaltungskonto ein, indem die Verantwortung für die Bereitstellung von Stack-Sets an ein dediziertes CI/CD-Konto als Stack-Set-Administrator für Anwendungsbereitstellungen delegiert wird.
- Verwendet das serviceverwaltete Berechtigungsmodell, um die Anwendung automatisch bereitzustellen, wenn ein neues Konto erstellt und einer Organisationseinheit zugeordnet wird.
- Stellt die Konsistenz der Anwendungsversion für alle Konten auf Umgebungsebene sicher.
- Verwendet mehrere Genehmigungsphasen auf Repository- und Pipeline-Ebene, um zusätzliche Sicherheits- und Governance-Ebenen für die bereitgestellte Anwendung bereitzustellen.

- Überwindet die aktuelle Einschränkung von , CodePipeline indem ein benutzerdefiniertes Bereitstellungsskript in verwendet wird CodeBuild , um Stack-Sets und Stack-Instances automatisch bereitzustellen oder zu entfernen. Eine Veranschaulichung der Flusssteuerung und Hierarchie der API-Aufrufe, die durch das benutzerdefinierte Skript implementiert werden, finden Sie im Abschnitt Zusätzliche Informationen.
- Erstellt einzelne Stack-Sets für die Entwicklungs-, Test- und Produktionsumgebungen. Darüber hinaus können Sie Stack-Sets erstellen, die mehrere OUs und Regionen in jeder Phase kombinieren. Sie können beispielsweise Sandbox und Entwicklungs-OUs innerhalb einer Entwicklungsbereitstellungsphase kombinieren.
- Unterstützt die Anwendungsbereitstellung in oder den Ausschluss von einer Teilmenge von Konten oder einer Liste von OUs.

Automatisierung und Skalierung

Sie können den Code verwenden, der mit diesem Muster bereitgestellt wird, um ein AWS-CodeCommit Repository und eine Code-Pipeline für Ihre Anwendung zu erstellen. Sie können diese dann als Stack-Sets in mehreren Konten auf Organisationseinheitsebene bereitstellen. Der Code automatisiert auch Komponenten wie Amazon Simple Notification Service (Amazon SNS)-Themen, um Genehmiger, die erforderlichen AWS Identity and Access Management (IAM)-Rollen und die Service-Kontrollrichtlinie (SCP) zu benachrichtigen, die im Verwaltungskonto angewendet werden sollen.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen in Amazon Elastic Compute Cloud (Amazon EC2) oder On-Premises-Instances, AWS Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS)-Services.

- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.

Code-Repository

Der Code für dieses Muster ist im GitHub automated-code-pipeline-stackset-Bereitstellungs-Repository verfügbar. Die Ordnerstruktur und andere Details finden Sie in der Readme-Datei für das Repository.

Bewährte Methoden

Dieses Muster schränkt den direkten Zugriff auf das Verwaltungskonto ein, während die Anwendung auf Organisationseinheitsebene bereitgestellt wird. Das Hinzufügen mehrerer Genehmigungsphasen zum Pipeline- und Repository-Prozess trägt dazu bei, zusätzliche Sicherheit und Governance für die Anwendungen und Komponenten zu bieten, die Sie mithilfe dieses Ansatzes bereitstellen.

Sekunden

Konten in AWS Organizations konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie alle Funktionen im Verwaltungskonto.	Aktivieren Sie alle Funktionen im Verwaltungskonto für Ihre Organisation, indem Sie den Anweisungen in der Dokumentation zu AWS Organizations folgen.	AWS-Administrator, Plattformadministrator
Erstellen Sie ein CI/CD-Konto.	Erstellen Sie in AWS Organizations in Ihrer	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Organisation ein dediziertes CI/CD-Konto und weisen Sie ein Team zu, das den Zugriff auf das Konto besitzt und kontrolliert.	
Fügen Sie einen delegierten Administrator hinzu.	Registrieren Sie im Verwaltungskonto das CI/CD-Konto, das Sie im vorherigen Schritt erstellt haben, als delegierten Stack-Set-Administrator. Anweisungen finden Sie in der AWS- CloudFormation Dokumentation.	AWS-Administrator, Plattformadministrator

Erstellen eines Anwendungs-Repositorys und einer CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repository.	1. Klonen Sie das Code-Repository, das mit diesem Muster bereitgestellt wird, auf Ihren Computer: `git clone https://github.com/aws-samples/automated-code-pipeline-stackset-deployment.git` 2. Überprüfen Sie die Readme-Datei, um die Verzeichnisstruktur und andere Details zu verstehen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie SNS-Themen.	Sie können die im GitHub Repository bereitgestellte `sns-template.yaml` Vorlage verwenden, um SNS-Themen zu erstellen und Abonnements für Genehmigungsanforderungen zu konfigurieren. 1. Melden Sie sich in der AWS-Konsole beim CI/CD-Konto an. 2. Öffnen Sie die - CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation. 3. Erstellen Sie einen neuen Stack mit neuen Ressourcen (Standardoption). 4. Wählen Sie für Vorlage angeben die Option Vorlagendatei hochladen, Datei auswählen und wählen Sie dann die `sns-template.yaml` Datei aus dem `templates` Ordner des geklonten GitHub Repositorys aus. Wählen Sie Weiter aus. 5. Geben Sie einen aussagekräftigen Namen für den Anwendungs-Stack an. 6. Geben Sie ein Präfix für - Ressourcen an.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie Weiter , Weiter und Übermitteln aus. 8. Wenn der Stack erfolgreich erstellt wurde, wählen Sie die Registerkarte Outputs und notieren Sie sich die Amazon-Ressourcennamen (ARNs) der SNS-Theme n für Pull-Anforderungen , die Testumgebung und die Produktionsumgebun g. Sie verwenden diese Informationen in nachfolge nden Schritten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie IAM-Rollen für CI/CD-Komponenten.	Sie können die `cicd-role-template.yaml` Vorlage verwenden, die im GitHub Repository bereitgestellt wird, um IAM-Rollen und -Richtlinien zu erstellen, die für CI/CD-Komponenten erforderlich sind. 1. Melden Sie sich in der AWS-Konsole beim CI/CD-Konto an. 2. Öffnen Sie die - CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation. 3. Erstellen Sie einen neuen Stack mit neuen Ressourcen (Standardoption). 4. Wählen Sie für Vorlage angeben die Option Vorlagendatei hochladen, Datei auswählen und wählen Sie dann die `cicd-role-template.yaml` Datei aus dem `templates` Ordner des geklonten GitHub Repositorys aus. Wählen Sie Weiter aus. 5. Geben Sie einen aussagekräftigen Namen für den Anwendungs-Stack an. 6. Geben Sie Werte für die folgenden Parameter ein:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Der ARN für die Berechtigungsgrenz enrichtlinie. Sie können diesen ARN im Abschnitt Richtliniendetails Ihrer Berechtigungsgrenz enrichtlinie in der IAM-Konsole abrufen. • Der ARN für das SNS-Produktionsgen ehmigungsthema, das Sie zuvor notiert haben. • Der ARN für das SNS-Testgenehmigun gsthema, das Sie zuvor notiert haben. • Ein Präfix für Ressource n, die von der Vorlage erstellt wurden. 7. Wählen Sie Weiter , Weiter und Übermitteln aus. 8. Wenn der Stack erfolgreich erstellt wurde, wählen Sie die Registerkarte Outputs und notieren Sie sich die ARNs der erstellten IAM-Rollen. Sie verwenden diese Informationen in nachfolgenden Schritten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository und eine Code-Pipeline für Ihre Anwendung.	Sie können die im GitHub Repository bereitgestellte `cicd-pipeline-template.yaml` Vorlage verwenden, um ein CodeCommit Repository und eine Code-Pipeline für Ihre Anwendung zu erstellen. 1. Melden Sie sich in der AWS-Konsole beim CI/CD-Konto an. 2. Öffnen Sie die - CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation. 3. Erstellen Sie einen neuen Stack mit neuen Ressourcen (Standardoption). 4. Wählen Sie für Vorlage angeben die Option Vorlagendatei hochladen, Datei auswählen und wählen Sie dann die `cicd-pipeline-template.yaml` Datei aus dem `templates` Ordner des geklonten GitHub Repositorys aus. Wählen Sie Weiter aus. 5. Geben Sie einen aussagekräftigen Namen für den Anwendungs-Stack an.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie Werte für die folgenden Parameter ein: • AppRepositoryName – Der Name des CodeCommit Repositorys, das für die Anwendung erstellt wird. • AppRepositoryDescription – Eine kurze Beschreibung des CodeCommit Repositorys, das für die Anwendung erstellt wird. • ApplicationName – Der Name Ihrer Anwendung. Diese Zeichenfolge wird als Name des CodeCommit Repositorys und als Präfix der CI/CD-Pipeline verwendet. • CloudWatchEventRoleARN – Der ARN der CloudWatch Ereignisrolle aus der vorherigen Aufgabe. • CodeBuildProjectRoleARN – Der ARN der CodeBuild Projektrolle aus der vorherigen Aufgabe. • CodePipelineRoleARN – Der ARN der CodePipeline Rolle aus der vorherigen Aufgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• DeploymentConfigBucket – Der Amazon Simple Storage Service (Amazon S3)-Bucket-Name, in dem die Bereitstellungskonfigurationsdateien und die ZIP-Skriptdatei gespeichert werden. • DeploymentConfigKey – Der Pfad und der ZIP-Dateiname (Amazon S3-Schlüssel). • PRApprovalSNSARN – Der ARN für das SNS-Thema für Pull-Anforderungsbenachrichtigungen. • ProdApprovalSNSpeedN – Der ARN für das SNS-Thema für Produktionsgenehmigungen. • TESTApprovalSNSARN – Der ARN für das SNS-Thema für Testgenehmigungen. • TemplateBucket – Der Name des S3-Buckets im CI/CD-Konto, in dem die CI/CD-Pipeline-Erstellungsvorlage gespeichert wird. 7. Wählen Sie Weiter , Weiter und Übermitteln aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wenn der Stack erfolgreich abgeschlossen wurde, wird ein CodeCommit Repository mit dem angegebenen Namen und einer Standardverzeichnisstruktur, Bereitstellungskonfigurationsdateien, Skripts und einer CodePipeline für das Repository erstellt.	

Bereitstellen eines Stack-Sets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Anwendungs-Repository.	Die CI/CD-Pipeline-Vorlage, die Sie zuvor verwendet haben, erstellt ein Beispielanwendungs-Repository und eine Code-Pipeline. So klonen und überprüfen Sie das Repository: 1. Melden Sie sich beim CI/CD-Konto an. 2. Suchen Sie das Anwendungs-Repository und die CI/CD-Pipeline, die Sie im vorherigen Epi erstellt haben. 3. Kopieren Sie die URL für das Repository und verwenden Sie den git-Klonbefehl, um das	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Repository auf Ihrem lokalen Computer zu klonen.
	4. Stellen Sie sicher, dass die Verzeichnisstruktur und die Dateien mit den folgenden übereinstimmen:
	`root`
	` |- deploy_configs`
	` |  |- deployment_config.json`
	` |- parameters`
	` |  |- template-parameter-dev.json`
	` |  |- template-parameter-test.json`
	` |  |- template-parameter-prod.json`
	` |- templates`
	` |  |- template.yml`
	` |- buildspec.yml`
	wobei der `deploy_configs` Ordner die Bereitstellungskonfigurationsdatei enthält und die `parameters` Ordner `templates` und Standarddateien enthalten, die Sie durch Ihre eigenen CloudFormation Vorlagen- und Parameterdateien ersetzen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Passen Sie die Ordnerstruktur nicht an. 5. Erstellen Sie einen Feature-Zweig.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Anwendung sartefakte hinzu.	Aktualisieren Sie das Anwendungs-Repository mithilfe einer CloudFormation Vorlage. Hinweis: Diese Lösung unterstützt die Bereitstellung nur einer einzigen CloudFormation Vorlage. 1. Erstellen Sie Ihre CloudFormation Vorlage für die Bereitstellung Ihrer Anwendungscodeände rungen und benennen Sie sie `<application-name>.yaml` . 2. Ersetzen Sie die `template.yml` Datei im `templates` Ordner des Anwendungs-Repositorys durch die CloudFormation Vorlage, die Sie in Schritt 1 erstellt haben. 3. Bereiten Sie Parameter dateien für jede Umgebung vor (Entwicklung, Test und Produktion). 4. Benennen Sie die Parameterdateien im Format `<cloudformation-template-name>-parameter-<env`	App-Entwickler, Dateninge nieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ironment-name>.jso n` . 5. Ersetzen Sie die Standardp arameterdateien im `parameters` Ordner durch Ihre Dateien aus Schritt 4.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Bereitstellungskonfigurationsdatei.	Aktualisieren Sie die `deployment_config.json` Datei: 1. Navigieren Sie im Anwendungs-Repository zum `deploy_configs` Ordner . 2. Öffnen Sie die Datei `deployment_config.json` : `{ "deployment_action": "<deploy/delete>", "stack_set_name": "<stack set name>", "stack_set_desciption": "<stack set description>", "deployment_targets": { "dev": { "org_units": ["list of OUs"], "regions": ["list of regions"], "filter_accounts": ["list of accounts"],`	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"test": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],
	"filter_accounts": ["list of accounts"],
	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"prod": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"filter_accounts": ["list of accounts"], "filter_type": "<DIFFERENCE/INTERSECTION/UNION>" } }, "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"], "auto_deployement": "<True/False>", "retain_stacks_on_account_removal": "<True/False>", "region_deployment_concurrency": "<SEQUENTIAL/PARALLEL>" }</pre> 3. Aktualisieren Sie die Werte für die Bereitstellungsaktion, den Namen des Stack-Sets, die Beschreibung des Stack-Sets und die Bereitstellungsziele. Sie können beispielsweise `deployment_action` auf setzen, `delete` um	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das gesamte Stack-Set und die zugehörigen Stack-Instances zu löschen. Verwenden Sie `deploy`, um ein neues Stack-Set zu erstellen, ein vorhandenes Stack-Set zu aktualisieren oder Stack-Instances für zusätzliche OUs oder Regionen hinzuzufügen oder zu entfernen. Weitere Beispiele finden Sie im Abschnitt Zusätzliche Informationen. Dieses Muster erstellt individuelle Stack-Sets für jede Umgebung, indem der Umgebungsname dem Stack-Set-Namen hinzugefügt wird, den Sie in der Bereitstellungskonfigurationsdatei angeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übernehmen Sie Änderungen und stellen Sie das Stack-Set bereit.	Übernehmen Sie die Änderungen, die Sie in Ihrer Anwendungsvorlage angegeben haben, und führen Sie das Stack-Set schrittweise in mehreren Umgebungen zusammen und stellen Sie es bereit: 1. Speichern Sie alle Ihre Dateien und übernehmen Sie Änderungen am Feature-Zweig Ihres lokalen Anwendungs-Repositorys. 2. Verschieben Sie den Feature-Zweig in das Remote-Repository. 3. Erstellen Sie eine Pull-Anforderung, um die Änderungen mit dem Hauptzweig zusammenzuführen. Wenn die Pull-Anforderung genehmigt und Änderungen am Hauptzweig zusammengeführt wurden, wird die CI/CD-Pipeline initiiert. 4. Wenn die Bereitstellungsphase erfolgreich abgeschlossen wurde, überprüfen Sie die CloudFormation Konsole,	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	StackSets, die Registerk arte Serviceverwaltet. Sie sehen ein neues Stack-Set mit dem Suffix `dev`. 5. Überprüfen Sie die CodeBuild Protokolle für die Bereitstellungsphase der Entwicklung auf Probleme. 6. Stellen Sie das Stack-Set in den Test- und Produktionsumgebungen bereit, indem Sie Ihre Genehmiger auffordern, die Bereitstellungen für diese Phasen zu genehmigen und die Schritte 5 und 6 zu wiederholen. Die Stack-Sets für die Test- und Produktionsumgebungen haben die Suffixe `test` und `prod`.	

Fehlerbehebung

Problem	Lösung
Die Bereitstellung schlägt mit der Ausnahme fehl: Ändern Sie den Namen der Vorlagenp arameterdatei in <application name>-par ameter-<evn>.json mit . Standardnamen sind nicht zulässig.	Die CloudFormation Vorlagenparameterdateien müssen der angegebenen Namenskonvention entsprechen. Aktualisieren Sie die Parameter dateinamen und versuchen Sie es erneut.

Problem	Lösung
Die Bereitstellung schlägt mit der Ausnahme fehl: Ändern Sie den Namen der CloudFormation Vorlage als <Anwendungsname>.yml, Standard template.yml oder template.yaml sind nicht zulässig	Der CloudFormation Vorlagenname muss der angegebenen Namenskonvention entsprech en. Aktualisieren Sie den Dateinamen und versuchen Sie es erneut.
Die Bereitstellung schlägt mit der Ausnahme fehl: Keine gültige CloudFormation Vorlage und ihre Parameterdatei für die Umgebung {environment name} gefunden	Überprüfen Sie die Namenskonventionen für die CloudFormation Vorlage und ihre Parameterdatei für die angegebene Umgebung.
Die Bereitstellung schlägt mit der Ausnahme fehl: Ungültige Bereitstellungsaktion in der Bereitste llungskonfigurationsdatei angegeben. Gültige Optionen sind „Bereitstellung“ und „Löschen“.	Sie haben einen ungültigen Wert für den `deployment_action` Parameter in der Bereitstellungskonfigurationsdatei angegeben. Der Parameter hat zwei gültige Werte: `deploy` und `delete`. Verwenden Sie `deploy`, um die Stack-Sets und die zugehörigen Stack-Instances zu erstellen und zu aktualisieren. Verwenden Sie `delete` nur, wenn Sie das gesamte Stack-Set und die zugehörigen Stack-Instances entfernen möchten.

Zugehörige Ressourcen

- GitHub automated-code-pipeline-stackset-Bereitstellungs-Repository
- Aktivieren aller Funktionen in Ihrer Organisation (Dokumentation zu AWS Organizations)
- Registrieren eines delegierten Administrators (AWS- CloudFormation Dokumentation)
- Ziele auf Kontoebene für serviceverwaltete Stack-Sets (AWS- CloudFormation Dokumentation)

Zusätzliche Informationen

Flussdiagramm

Das folgende Flussdiagramm zeigt die Flusssteuerung und Hierarchie der API-Aufrufe, die vom benutzerdefinierten Skript implementiert werden, um die Bereitstellung von Stack-Sets zu automatisieren.

Beispielkonfigurationsdateien für die Bereitstellung

Erstellen eines neuen Stack-Sets

Die folgende Bereitstellungskonfigurationsdatei erstellt ein neues Stack-Set mit dem Namen `sample-stack-set` in der AWS-Region `us-east-1` in drei OUs.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
```

```
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Bereitstellen eines vorhandenen Stack-Sets in einer anderen Organisationseinheit

Wenn Sie die im vorherigen Beispiel gezeigte Konfiguration bereitstellen und das Stack-Set für eine zusätzliche Organisationseinheit namens `dev-org-unit-2` in der Entwicklungsumgebung bereitstellen möchten, könnte die Bereitstellungskonfigurationsdatei wie folgt aussehen.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Bereitstellen eines vorhandenen Stack-Sets in einer anderen AWS-Region

Wenn Sie die im vorherigen Beispiel gezeigte Konfiguration bereitstellen und das Stack-Set in einer zusätzlichen AWS-Region (`us-east-2`) in der Entwicklungsumgebung für zwei OUs (`dev-org-unit-1` und) bereitstellen möchten`dev-org-unit-2`, könnte die Bereitstellungskonfigurationsdatei wie folgt aussehen.

Hinweis: Die Ressourcen in der CloudFormation Vorlage müssen gültig und regionsspezifisch sein.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                              "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                              "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                              "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                            },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Entfernen einer Stack-Instance aus einer Organisationseinheit oder AWS-Region

Angenommen, die im vorherigen Beispiel gezeigte Bereitstellungskonfiguration wurde bereitgestellt. Die folgende Konfigurationsdatei entfernt die Stack-Instances aus beiden Regionen der Organisationseinheit `dev-org-unit-2`.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Die folgende Konfigurationsdatei entfernt die Stack-Instance aus der AWS-Region `us-east-1` für beide OUs in der Entwicklungsumgebung.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
```

```
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Löschen des gesamten Stack-Sets

Die folgende Bereitstellungskonfigurationsdatei löscht das gesamte Stack-Set und alle zugehörigen Stack-Instances.

```
{
     "deployment_action": “delete”,
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
```

```
                                },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                }
                        },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Ausschließen eines Kontos von der Bereitstellung

Die folgende Bereitstellungskonfigurationsdatei schließt das Konto `111122223333`, das Teil der Organisationseinheit ist`dev-org-unit-1`, von der Bereitstellung aus.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": ["111122223333"],
                                        "filter_type": "DIFFERENCE"
                                },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                },
                            "prod": {
```

```
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Bereitstellen der Anwendung für eine Teilmenge von Konten in einer Organisationseinheit

Die folgende Bereitstellungskonfigurationsdatei stellt die Anwendung nur für drei Konten (111122223333, 444455556666und 777788889999) in der Organisationseinheit bereit`dev-org-unit-1`.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                    "org_units": ["dev-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": ["111122223333",
"444455556666", "777788889999"],
                                    "filter_type": "INTERSECTION"
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                        },
```

```
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Automatisches Anfügen einer von AWS verwalteten Richtlinie für Systems Manager an EC2-Instance-Profile mithilfe von Cloud Custodian und AWS CDK

Erstellt von Ali Asf4 (AWS) und Aaron Lennon (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Softwareentwicklung und -tests; Management und Governance; Sicherheit, Identität, Compliance; Infrastruktur	Workload: Open-Source
AWS-Services: Amazon SNS ; Amazon SQS ; AWS CodeBuild; AWS CodePipeline; AWS Systems Manager ; AWS CodeCommit		

Übersicht

Sie können Amazon Elastic Compute Cloud (Amazon EC2)-Instances in AWS Systems Manager integrieren, um betriebliche Aufgaben zu automatisieren und mehr Transparenz und Kontrolle zu bieten. Um in Systems Manager zu integrieren, müssen EC2-Instances über eine installierte AWS Systems Manager Agent (SSM Agent) und eine `AmazonSSMManagedInstanceCore` AWS Identity and Access Management (IAM)-Richtlinie verfügen, die ihren Instance-Profilen zugeordnet ist.

Wenn Sie jedoch sicherstellen möchten, dass allen EC2-Instance-Profilen die `AmazonSSMManagedInstanceCore` Richtlinie angefügt ist, können Probleme beim Aktualisieren neuer EC2-Instances auftreten, die keine Instance-Profile oder EC2-Instances haben, die ein Instance-Profil, aber nicht die `AmazonSSMManagedInstanceCore` Richtlinie haben. Es kann auch schwierig sein, diese Richtlinie über mehrere Amazon Web Services (AWS)-Konten und AWS-Regionen hinweg hinzuzufügen.

Dieses Muster hilft bei der Lösung dieser Herausforderungen, indem es drei Cloud-Custom-Richtlinien in Ihren AWS-Konten bereitstellt:

- Die erste Richtlinie von Cloud Custodian prüft auf vorhandene EC2-Instances, die über ein Instance-Profil, aber nicht über die `AmazonSSMManagedInstanceCore` Richtlinie verfügen. Die `AmazonSSMManagedInstanceCore` Richtlinie wird dann angehängt.
- Die zweite Richtlinie von Cloud Custodian sucht nach vorhandenen EC2-Instances ohne Instance-Profil und fügt ein Standard-Instance-Profil hinzu, dem die `AmazonSSMManagedInstanceCore` Richtlinie angefügt ist.
- Die dritte Cloud-Custom-Richtlinie erstellt AWS Lambda-Funktionen in Ihren Konten, um die Erstellung von EC2-Instances und Instance-Profilen zu überwachen. Dadurch wird sichergestellt, dass die `AmazonSSMManagedInstanceCore` Richtlinie automatisch angehängt wird, wenn eine EC2-Instance erstellt wird.

Dieses Muster verwendet AWS DevOps-Tools, um eine kontinuierliche, skalierbare Bereitstellung der Cloud-Custodiaan-Richtlinien in einer Umgebung mit mehreren Konten zu erreichen, ohne eine separate Datenverarbeitungsumgebung bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei oder mehr aktive AWS-Konten. Ein Konto ist das Sicherheitskonto und die anderen sind Mitgliedskonten.
- Berechtigungen zur Bereitstellung von AWS-Ressourcen im Sicherheitskonto. Dieses Muster verwendet Administratorberechtigungen, aber Sie sollten Berechtigungen gemäß den Anforderungen und Richtlinien Ihrer Organisation erteilen.
- Möglichkeit, eine IAM-Rolle vom Sicherheitskonto zu Mitgliedskonten zu übernehmen und die erforderlichen IAM-Rollen zu erstellen. Weitere Informationen dazu finden Sie unter Delegieren des Zugriffs in allen AWS-Konten mithilfe von IAM-Rollen in der IAM-Dokumentation.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Zu Testzwecken können Sie AWS CLI mithilfe des `aws configure` Befehls oder der Einstellung von Umgebungsvariablen konfigurieren. Wichtig: Dies wird nicht für Produktionsumgebungen empfohlen und wir empfehlen, dass diesem Konto nur der Zugriff mit den geringsten Rechten gewährt wird. Weitere Informationen dazu finden Sie unter Gewähren der geringsten Berechtigung in der IAM-Dokumentation.

- Die `devops-cdk-cloudcustodian.zip` Datei (angefügt), die auf Ihren lokalen Computer heruntergeladen wurde.
- Vertrautheit mit Python.
- Die erforderlichen Tools (Node.js, AWS Cloud Development Kit (AWS CDK) und Git), installiert und konfiguriert. Sie können die `-install-prerequisites.sh`Datei in der `-devops-cdk-cloudcustodian.zip`Datei verwenden, um diese Tools zu installieren. Stellen Sie sicher, dass Sie diese Datei mit Root-Berechtigungen ausführen.

Einschränkungen

- Obwohl dieses Muster in einer Produktionsumgebung verwendet werden kann, stellen Sie sicher, dass alle IAM-Rollen und -Richtlinien den Anforderungen und Richtlinien Ihrer Organisation entsprechen.

Paketversionen

- Cloud Custodian Version 0.9 oder höher
- TypeScript Version 3.9.7 oder höher
- Node.js Version 14.15.4 oder höher
- `npm` Version 7.6.1 oder höher
- AWS-CDK-Version 1.96.0 oder höher

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Cloud Custodian-Richtlinien werden in ein AWS- CodeCommit Repository im Sicherheitskonto übertragen. Eine Amazon CloudWatch Events-Regel initiiert die AWS- CodePipeline Pipeline automatisch.
2. Die Pipeline ruft den neuesten Code von ab CodeCommit und sendet ihn an den kontinuierlichen Integrationsbaustein der Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD), die von AWS verarbeitet wird CodeBuild.

3. CodeBuild führt die vollständigen DevSecOps Aktionen durch, einschließlich der Richtliniensyntaxvalidierung für die Cloud-Custom-Richtlinien, und führt diese Richtlinien im `--dryrun`Modus aus, um zu überprüfen, welche Ressourcen identifiziert werden.
4. Wenn es keine Fehler gibt, warnt die nächste Aufgabe einen Administrator, die Änderungen zu überprüfen und die Bereitstellung in den Mitgliedskonten zu genehmigen.

Technologie-Stack

- AWS-CDK
- CodeBuild
- CodeCommit
- CodePipeline
- IAM
- Cloud Custodian

Automatisierung und Skalierung

Das AWS-CDK-Pipelines-Modul stellt eine CI/CD-Pipeline bereit, die verwendet, CodePipeline um das Erstellen und Testen von Quellcode mit zu orchestrieren CodeBuild, zusätzlich zur Bereitstellung von AWS-Ressourcen mit AWS- CloudFormation Stacks. Sie können dieses Muster für alle Mitgliedskonten und Regionen in Ihrer Organisation verwenden. Sie können den `Roles creation`Stack auch erweitern, um andere IAM-Rollen in Ihren Mitgliedskonten bereitzustellen.

Tools

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework für die Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS CloudFormation.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Komponenten privat speichern und verwalten können.
- AWS CodePipeline ist ein kontinuierlicher Bereitstellungsservice, mit dem Sie die Schritte modellieren, visualisieren und automatisieren können, die für die Veröffentlichung Ihrer Software erforderlich sind.

- AWS Identity and Access Management ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können.
- Cloud Custodian ist ein Tool, das Dutzende von Tools und Skripts vereinheitlicht, die die meisten Organisationen zur Verwaltung ihrer öffentlichen Cloud-Konten in einem Open-Source-Tool verwenden.
- Node.js ist eine JavaScript Laufzeit, die auf der V8 JavaScript -Engine von Google Chrome basiert.

Code

Eine detaillierte Liste der Module, Kontofunktionen, Dateien und Bereitstellungsbefehle, die in diesem Muster verwendet werden, finden Sie in der `README` Datei in der -`devops-cdk-cloudcustodian.zip`Datei (angefügt).

Polen

Einrichten der Pipeline mit AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das CodeCommit Repository ein.	1. Entpacken Sie die `devops-cdk-cloudcustodian.zip` Datei (angefügt) im Arbeitsverzeichnis auf Ihrem lokalen Computer. 2. Melden Sie sich bei der AWS-Managementkonsole für Ihr Sicherheitskonto an, öffnen Sie die CodeCommit Konsole und erstellen Sie dann ein neues `devops-cdk-cloudcustodian` Repository. 3. Wechseln Sie in das Projektverzeichnis und richten Sie das CodeCommi	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	t Repository als Ursprung ein, übernehmen Sie die Änderungen und übertrage n Sie sie dann in den Ursprungszweig, indem Sie die folgenden Befehle ausführen: • `cd devops-cdk-cloudcustodian` • `git init --initial-branch=main` • `git add . git commit -m 'initial commit'` • `git remote add origin https://git-codecommit.us-east-1.amazonaws.com/v1/devops-cdk-cloudcustodian` • `git push origin main` Weitere Informationen dazu finden Sie unter Erstellen eines CodeCommit Repositorys in der AWS- CodeCommit Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die erforderlichen Tools.	Verwenden Sie die `-install-prerequisites.sh` Datei, um alle erforderlichen Tools auf Amazon Linux zu installieren. Dies beinhaltet nicht die AWS CLI, da sie vorinstalliert ist. Weitere Informationen dazu finden Sie im Abschnitt Voraussetzungen unter Erste Schritte mit dem AWS-CDK in der AWS-CDK-Dokumentation.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die erforderlichen AWS-CDK-Pakete.	1. Richten Sie Ihre virtuelle Umgebung ein, indem Sie den folgenden Befehl in AWS CLI ausführen: `$ python3 -m venv .env` 2. Aktivieren Sie Ihre virtuelle Umgebung, indem Sie den folgenden Befehl ausführen: `$ source .env/bin/activate` 3. Nachdem die virtuelle Umgebung aktiviert wurde, installieren Sie die erforderlichen Abhängigkeiten, indem Sie den folgenden Befehl ausführen: `$ pip install -r requirements.txt` 4. Um zusätzliche Abhängigkeiten hinzuzufügen (z. B. andere AWS-CDK-Bibliotheken), fügen Sie sie der `requirements.txt` Datei hinzu und führen Sie dann den folgenden Befehl aus: `pip install -r requirements.txt` Die folgenden Pakete werden von AWS CDK benötigt und sind in der `requirements.txt` Datei enthalten:	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `aws-cdk.aws-cloudwatch` • `aws-cdk.aws-codebuild` • `aws-cdk.aws-codecommit` • `aws-cdk.aws-codedeploy` • `aws-cdk.aws-codepipeline` • `aws-cdk.aws-codepipeline-actions` • `aws-cdk.aws-events` • `aws-cdk.aws-events-targets` • `aws-cdk.aws-iam` • `aws-cdk.aws-logs` • `aws-cdk.aws-s3` • `aws-cdk.aws-sns` • `aws-cdk.aws-sns-subscriptions` • `aws-cdk.aws-sqs` • `aws-cdk.core`	

Konfigurieren Ihrer Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die erforderlichen Variablen.	Öffnen Sie die `vars.py` Datei im Stammordner Ihres CodeCommit Repositorys und	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aktualisieren Sie die folgenden Variablen: • Aktualisieren Sie `var_deploy_region = ‘us-east-1’` mit der AWS-Region, in der die Pipeline bereitgestellt werden soll. • Aktualisieren Sie `var_codecommit_repo_name = “cdk-cloudcustodian”` mit dem Namen Ihres CodeCommit Repositorys. • Aktualisieren Sie `var_codecommit_branch_name = “main”` mit dem Namen der CodeCommit Verzweigung. • Aktualisieren Sie `var_adminEmail=notifyadmin@email.com’` mit der E-Mail-Adresse des Administrators, der Änderungen genehmigt. • Aktualisieren Sie `var_slackWebHookUrl = https://hooks.slack.com/services/T000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX '` mit dem Slack-Webhook, der zum Senden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von Cloud-Kustodia-Ben achrichtigungen verwendet wird, wenn Änderungen vorgenommen werden. • Aktualisieren Sie `var_orgId = 'o-yyyyyyyyyy'` mit Ihrer Organisations-ID. • Aktualisieren Sie `security_account = '123456789011'` mit der AWS-Konto-ID für das Konto, in dem die Pipeline bereitgestellt wird. • Aktualisieren Sie `member_accounts = ['111111111111','111111111112','111111111113']` mit den Mitgliedskonten, in denen Sie den AWS-CDK-Stack booten und die erforderlichen IAM-Rollen bereitstellen möchten. • Setzen Sie den Wert `cdk_bootstrap_member_accounts = True` auf `True`, wenn die Pipeline den AWS-CDK automatisch mit Ihren Mitgliedskonten booten soll. Wenn `True` diese Option auf gesetzt ist, ist auch der Name einer vorhandenen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Rolle in den Mitglieds konten erforderlich, die vom Sicherheitskonto übernommen werden kann. Diese IAM-Rolle muss auch über die erforderl ichen Berechtigungen zum Bootstrappen des AWS-CDK verfügen. • Aktualisieren Sie `cdk_bootstrap_role = ‘AWSControlTowerEx ecution’` mit der vorhandenen IAM-Rolle in den Mitgliedskonten, die vom Sicherheitskonto übernommen werden kann. Diese Rolle muss auch über die Berechtig ung zum Bootstrappen des AWS-CDK verfügen. Hinweis: Dies gilt nur, wenn auf gesetzt `cdk_boots trap_member_accoun ts` ist`True`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die Datei account.yml mit den Mitglieds kontoinformationen.	Um das c7n-org Cloud Custodian-Tool für mehrere Konten auszuführen, müssen Sie die Konfigurationsdate i im Stammverzeichnis des `accounts.yml` Repositorys ablegen. Im Folgenden finden Sie ein Beispiel für eine Cloud Custodian-Konfigurationsdatei für AWS:
	`accounts:`
	`- account_id: '12312312 3123'`
	`name: account-1`
	`regions:`
	`- us-east-1`
	`- us-west-2`
	`role: arn:aws:i am::123123123123:r ole/CloudCustodian`
	`vars:`
	`charge_code: xyz`
	`tags:`
	`- type:prod`
	`- division:some division`
	`- partition:us`
	`- scope:pci`
		Developer

Bootstrap der AWS-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Steigern Sie das Sicherhei tskonto.	Bootstrappen Sie die `deploy_account` mit der	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cloudcustodian_stack` Anwendung, indem Sie den folgenden Befehl ausführen: `cdk bootstrap -a 'python3 cloudcustodian/cloudcustodian_stack.py'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 – Automatisches Bootstrapping der Mitglieds konten.	Wenn die `cdk_bootstrap_member_accounts` Variable `True` in der `vars.py` Datei auf gesetzt ist, werden die in der `member_accounts` Variable angegeben en Konten automatisch von der Pipeline gebootet. Bei Bedarf können Sie `*cdk_bootstrap_role*` mit einer IAM-Rolle aktualisi eren, die Sie vom Sicherhei tskonto übernehmen können und die über die erforderl ichen Berechtigungen zum Bootstrappen des AWS-CDK verfügt. Neue Konten, die der `member_accounts` Variablen hinzugefü gt werden, werden automatis ch von der Pipeline gebootet, sodass die erforderlichen Rollen bereitgestellt werden können.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2 – Bootstrap der Mitgliedskonten manuell.	Obwohl wir nicht empfehlen, diesen Ansatz zu verwenden , können Sie den Wert von `cdk_bootstrap_member_accounts` auf setzen `False` und diesen Schritt manuell ausführen, indem Sie den folgenden Befehl ausführen: `$ cdk bootstrap -a 'python3 cloudcustodian/member_account_roles_stack.py' \ --trust {security_account_id} \ --context assume-role-credentials:writeIamRoleName={role_name} \ --context assume-role-credentials:readIamRoleName={role_name} \ --mode=ForWriting \ --context bootstrap=true \ --cloudformation-execution-policies arn:aws:iam::aws:policy/AdministratorAccess`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Stellen Sie sicher, dass Sie die `{role_name}` Werte `{security_account_id}` und mit dem Namen einer IAM-Rolle aktualisieren, die Sie vom Sicherheitskonto übernehmen können und die über die erforderlichen Berechtigungen zum Bootstrappen des AWS-CDK verfügt. Sie können auch andere Ansätze verwenden, um die Mitgliedskonten zu bootstrappen, z. B. mit AWS CloudFormation. Weitere Informationen dazu finden Sie unter Bootstrapping in der AWS-CDK-Dokumentation.	

Bereitstellen der AWS-CDK-Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rollen in den Mitgliedskonten.	Führen Sie den folgenden Befehl aus, um den `member_account_roles_stack` Stack bereitzustellen und die IAM-Rollen in den Mitgliedskonten zu erstellen: `cdk deploy --all -a 'python3 cloudcust`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`odian/member_accou nt_roles_stack.py' -- require-approval never`	
Stellen Sie den Cloud-Cus tom-Pipeline-Stack bereit.	Führen Sie den folgenden Befehl aus, um die Cloud-Custodiaan-`cloudcust odian_stack.py` Pipeline zu erstellen, die im Sicherhei tskonto bereitgestellt wird: `cdk deploy -a 'python3 cloudcustodian/clo udcustodian_stack.py'`	Developer

Zugehörige Ressourcen

- Erste Schritte mit dem AWS-CDK

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mit AWS CDK

Erstellt von Varsha Raju (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Container und Microservices; Modernisierung; Infrastruktur	AWS-Services: AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; Amazon ECS; AWS-CDK

Übersicht

Dieses Muster beschreibt, wie Sie die Pipelines für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) und die zugrunde liegende Infrastruktur für die Erstellung und Bereitstellung von Microservices auf Amazon Elastic Container Service (Amazon ECS) automatisch erstellen. Sie können diesen Ansatz verwenden, wenn Sie proof-of-concept CI/CD-Pipelines einrichten möchten, um Ihrer Organisation die Vorteile von CI/CD, Microservices und zu zeigen DevOps. Sie können diesen Ansatz auch verwenden, um erste CI/CD-Pipelines zu erstellen, die Sie dann an die Anforderungen Ihrer Organisation anpassen oder ändern können.

Der Ansatz des Musters erstellt eine Produktionsumgebung und eine Nicht-Produktionsumgebung, die jeweils über eine Virtual Private Cloud (VPC) und einen Amazon-ECS-Cluster verfügen, der für die Ausführung in zwei Availability Zones konfiguriert ist. Diese Umgebungen werden von allen Ihren Microservices gemeinsam genutzt und Sie erstellen dann eine CI/CD-Pipeline für jeden Microservice. Diese CI/CD-Pipelines rufen Änderungen aus einem Quell-Repository in AWS ab CodeCommit, erstellen die Änderungen automatisch und stellen sie dann in Ihren Produktions- und Nicht-Produktionsumgebungen bereit. Wenn eine Pipeline alle Phasen erfolgreich abgeschlossen hat, können Sie URLs verwenden, um auf den Microservice in den Produktions- und Nicht-Produktionsumgebungen zuzugreifen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto.

- Ein vorhandener Amazon Simple Storage Service (Amazon S3)-Bucket, der die `starter-code.zip` Datei enthält (angefügt).
- AWS Cloud Development Kit (AWS CDK), installiert und konfiguriert in Ihrem Konto. Weitere Informationen dazu finden Sie unter Erste Schritte mit dem AWS-CDK in der AWS-CDK-Dokumentation.
- Python 3 und `pip`, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Python-Dokumentation.
- Vertrautheit mit AWS CDK, AWS CodePipeline, AWS CodeBuild, CodeCommitAmazon Elastic Container Registry (Amazon ECR), Amazon ECS und AWS Fargate.
- Vertrautheit mit Docker.
- Ein Verständnis von CI/CD und DevOps.

Einschränkungen

- Es gelten allgemeine AWS-Kontolimits. Weitere Informationen dazu finden Sie unter AWS-Servicekontingente in der AWS General Reference-Dokumentation.

Produktversionen

- Der Code wurde mit Node.js Version 16.13.0 und AWS CDK Version 1.132.0 getestet.

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Ein Anwendungsentwickler überträgt Code an ein CodeCommit Repository.
2. Eine Pipeline wird initiiert.
3. CodeBuild erstellt das Docker-Image und überträgt es in ein Amazon ECR-Repository
4. CodePipeline stellt ein neues Image für einen vorhandenen Fargate-Service in einem Amazon-ECS-Cluster bereit, der nicht zur Produktion gehört.
5. Amazon ECS ruft das Image aus dem Amazon-ECR-Repository in einen Fargate-Dienst ab, der nicht zur Produktion gehört.
6. Tests werden unter Verwendung einer Nicht-Produktions-URL durchgeführt.

7. Der Release Manager genehmigt die Produktionsbereitstellung.
8. CodePipeline stellt das neue Image für einen vorhandenen Fargate-Service in einem Amazon-ECS-Produktionscluster bereit
9. Amazon ECS ruft das Image aus dem Amazon-ECR-Repository in den Fargate-Produktionsservice ab.
10. Produktionsbenutzer greifen über eine Produktions-URL auf Ihre Funktion zu.

Technologie-Stack

- AWS-CDK
- CodeBuild
- CodeCommit
- CodePipeline
- Amazon ECR
- Amazon ECS
- Amazon VPC

Automatisierung und Skalierung

Sie können den Ansatz dieses Musters verwenden, um Pipelines für Microservices zu erstellen, die in einem freigegebenen AWS- CloudFormation Stack bereitgestellt werden. Die Automatisierung kann mehr als einen Amazon-ECS-Cluster in jeder VPC erstellen und auch Pipelines für Microservices erstellen, die in einem gemeinsam genutzten Amazon-ECS-Cluster bereitgestellt werden. Dies erfordert jedoch, dass Sie neue Ressourceninformationen als Eingaben für den Pipeline-Stack bereitstellen.

Tools

- AWS CDK – AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework für die Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS CloudFormation.
- AWS CodeBuild – AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Einheitentests durch und erzeugt Artefakte, die bereitgestellt werden können.
- AWS CodeCommit – AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys in der AWS Cloud privat speichern und verwalten können. CodeCommit Sie müssen

kein eigenes Quellcodeverwaltungssystem verwalten oder sich Gedanken über die Skalierung seiner Infrastruktur machen.

- AWS CodePipeline – AWS CodePipeline ist ein kontinuierlicher Bereitstellungsservice, mit dem Sie die Schritte zur Veröffentlichung Ihrer Software modellieren, visualisieren und automatisieren können. Sie können die verschiedenen Phasen eines Software-Release-Prozesses schnell modellieren und konfigurieren. CodePipeline automatisiert die Schritte, die erforderlich sind, um Ihre Softwareänderungen kontinuierlich freizugeben.
- Amazon ECS – Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster verwendet wird. Sie können Ihre Aufgaben und Services auf einer Serverless-Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Alternativ können Sie für mehr Kontrolle über Ihre Infrastruktur Ihre Aufgaben und Services auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2)-Instances ausführen, die Sie verwalten.
- Docker – Docker hilft Entwicklern dabei, jede Anwendung als leichter, portabler und selbstzureichender Container zu packen, zu versenden und auszuführen.

Code

Der Code für dieses Muster ist in den `starter-code.zip` Dateien `cicdstarter.zip` und (angefügt) verfügbar.

Polen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Arbeitsverzeichnis für AWS CDK ein.	1. Erstellen Sie ein Verzeichnis mit dem Namen `cicdproject` auf Ihrem lokalen Computer. 2. Laden Sie die `cicdstarter.zip` Datei (angefügt) in das `cicdproject` Verzeichnis herunter und entpacken Sie sie. Dadurch wird ein Ordner mit dem	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen erstelltcicdstarter . 3. Führen Sie den Befehl cd <user-home>/cicdproject/cicdstarter aus. 4. Richten Sie die virtuelle Python-Umgebung ein, indem Sie den python3 -m venv .venv Befehl ausführen. 5. Führen Sie den Befehl source ./.venv/bin/activate aus. 6. Konfigurieren Sie Ihre AWS-Umgebung, indem Sie den aws configure Befehl ausführen oder die folgenden Umgebungsvariablen verwenden: • AWS_ACCESS_KEY_ID • AWS_SECRET_ACCESS_KEY • AWS_DEFAULT_REGION	

Erstellen der freigegebenen Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die gemeinsam genutzte Infrastruktur.	1. Führen Sie in Ihrem Arbeitsverzeichnis den cd cicdvpcecs Befehl aus.	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Führen Sie den `pip3 install -r requirements.txt` Befehl aus, um alle erforderlichen Python-Abhängigkeiten zu installieren 3. Führen Sie aus`cdk bootstrap command`, um die AWS-Umgebung für das AWS-CDK festzulegen. 4. Führen Sie den Befehl `cdk synth --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` aus. 5. Führen Sie den Befehl `cdk deploy --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` aus. 6. Der AWS- CloudFormation Stack erstellt die folgende Infrastruktur: • Eine Nicht-Produktions-VPC mit dem Namen `cicd-vpc-ecs/cicd-vpc-nonprod` • Eine Produktions-VPC mit dem Namen `cicd-vpc-ecs/cicd-vpc-prod`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Ein Amazon-ECS-Cluster mit dem Namen , der nicht zur Produktion gehört `cicd-ecs-nonprod` • Ein Amazon-ECS-Produktionscluster mit dem Namen `cicd-ecs-prod`	
Überwachen Sie den AWS-CloudFormation Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS-CloudFormation Konsole und wählen Sie dann den `cicd-vpc-ecs` Stack aus der Liste aus. 2. Wählen Sie im Bereich Stack-Details die Registerkarte Ereignisse aus und überwachen Sie den Fortschritt Ihrer Stack-Erstellung.	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den AWS-CloudFormation Stack.	1. Nachdem der `cicd-vpc-ecs` AWS- CloudFormation Stack erstellt wurde, stellen Sie sicher, dass die `cicd-vpc-ecs/cicd-vpc-prod` VPCs `cicd-vpc-ecs/cicd-vpc-nonprod` und erstellt werden. 2. Stellen Sie sicher, dass die `cicd-ecs-prod` Amazon-ECS-Cluster `cicd-ecs-nonprod` und erstellt werden. Wichtig: Stellen Sie sicher, dass Sie die IDs für die beiden VPCs und die Sicherheitsgruppen-IDs für die Standardsicherheitsgruppen in beiden VPCs aufzeichnen.	AWS DevOps, Cloud-Infrastruktur

Erstellen einer CI/CD-Pipeline für einen Microservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Infrastruktur für den Microservice.	1. Benennen Sie Ihren Microservice. Dieses Muster verwendet beispielsweise `myservice1` als Namen des Microservice. 2. Führen Sie in Ihrem Arbeitsverzeichnis den `cd`	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<working-directory>/cdkpipeline` Befehl aus. 3. Führen Sie den Befehl `pip3 install -r requirements.txt` aus. 4. Führen Sie den vollständigen `cdk synth` Befehl aus, der im Abschnitt Zusätzliche Informationen dieses Musters verfügbar ist. 5. Führen Sie den vollständigen `cdk deploy` Befehl aus, der im Abschnitt Zusätzliche Informationen dieses Musters verfügbar ist. Hinweis: Sie können die Werte für beide Befehle auch mithilfe der `cdk.json` Datei im Verzeichnis angeben.	
Überwachen Sie den AWS-CloudFormation Stack.	Öffnen Sie die AWS-CloudFormation Konsole und überwachen Sie den Fortschritt des `myservice1-cicd-stack` Stacks. Schließlich ändert sich der Status in `CREATE_COMPLETE` .	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den AWS-CloudFormation Stack.	1. Überprüfen Sie in der AWS-CodeCommit Konsole, ob ein Repository mit dem Namen `myservice1` vorhanden ist und den Startercode enthält. 2. Überprüfen Sie in der AWS-CodeBuild Konsole, ob ein Build-Projekt mit dem Namen `myservice1` vorhanden ist. 3. Überprüfen Sie in der Amazon-ECR-Konsole , ob ein Amazon-ECR-Repository mit dem Namen `myservice1` vorhanden ist. 4. Stellen Sie in der Amazon-ECS-Konsole sicher, dass sich ein Fargate-Service mit dem Namen sowohl in einem Amazon-ECS-Cluster `myservice1` befindet, der nicht zur Produktion gehört, als auch in der Produktion. 5. Überprüfen Sie in der Amazon Elastic Compute Cloud (Amazon EC2)-Konsole, ob die Application Load Balancer erstellt wurden, die nicht in der Produktion und Produktion ausgeführ	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	t werden. Notieren Sie sich die DNS-Namen der ALBs. 6. Überprüfen Sie in der AWS-CodePipeline Konsole, ob eine Pipeline mit dem Namen `myservice1` vorhanden ist. Es muss die `Deploy-Prod` Stufen `Source`, `BuildDeploy-NonProd` , und haben. Die Pipeline sollte auch den `in progress` Status haben. 7. Überwachen Sie die Pipeline, bis alle Phasen abgeschlossen sind. 8. Genehmigen Sie es manuell für die Produktion. 9. Geben Sie in einem Browserfenster die DNS-Namen der ALBs ein. 10. Die Anwendung sollte in den Nicht-Produktions- und Produktions-URLs angezeigt`Hello World` werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Pipeline.	1. Öffnen Sie das CodeCommit Repository, das Sie zuvor erstellt haben, und öffnen Sie die `index.js` Datei . 2. Ersetzen Sie `Hello World` durch `Hello CI/CD`. 3. Speichern Sie die Änderungen und führen Sie ein Commit für den Hauptzweig aus. 4. Stellen Sie sicher, dass die Pipeline initiiert wird und dass die Änderung die `Deploy-Prod` Phasen `BuildDeploy-NonProd` , und durchläuft. 5. Genehmigen Sie die Produktion manuell. 6. Sowohl Produktions- als auch Nicht-Produktions-URLs sollten jetzt anzeigen`Hello CICD`.	AWS DevOps, Cloud-Infrastruktur
Wiederholen Sie dieses Epic für jeden Microservice.	Wiederholen Sie die Aufgaben in diesem Epic, um eine CI/CD-Pipeline für jeden Ihrer Microservices zu erstellen.	AWS DevOps, Cloud-Infrastruktur

Zugehörige Ressourcen

- Verwenden von Python mit AWS CDK
- AWS-CDK-Python-Referenz

- Erstellen eines AWS Fargate-Services mit dem AWS-CDK

Zusätzliche Informationen

cdk synth -Befehl

```
cdk synth --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production
 VPC> --context vpc_prod_id=<id_of_production_VPC> --context
 ecssg_nonprod_id=< default_security_group_id_of_non-production_VPC>
 --context ecssg_prod_id=<default_security_group_id_of_production_VPC>
 --context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

cdk deploy command

```
cdk deploy --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production_VPC>
 --context vpc_prod_id=<id_of_production_VPC> --context ecssg_nonprod_id=<
 default_security_group_id_of_non-production_VPC> --context
 ecssg_prod_id=<default_security_group_id_of_production_VPC> --
context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie mithilfe von DevOps Praktiken und AWS Cloud9 eine lose gekoppelte Architektur mit Microservices

Erstellt von Alexandre Nardi (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Serverlos; Web- und mobile Apps; Datenbanken	AWS-Dienste: AWS Cloud9; AWS; AWS CloudFormation CodePipeline; Amazon DynamoDB; AWS CodeCommit

Übersicht

Dieses Muster zeigt, wie eine typische Webanwendung in einer serverlosen Architektur für Entwickler und Entwicklungsleiter entwickelt wird, die damit beginnen, DevOps Praktiken auf Amazon Web Services (AWS) zu testen. Es erstellt eine Beispielanwendung, die eine Storefront und ein Backend für das Durchsuchen und Kaufen von Büchern erstellt und einen Microservice bereitstellt, der unabhängig entwickelt werden kann. Das Muster verwendet AWS Cloud9 als Entwicklungsumgebung, eine Amazon DynamoDB DynamoDB-Datenbank als Datenspeicher und AWS-Services wie AWS und AWS CodeBuild für Continuous Integration CodePipeline and Continuous Deployment (CI/CD) -Funktionalität.

Das Muster führt Sie durch die folgenden Entwicklungsaktivitäten:

- Erstellen einer standardmäßigen AWS Cloud9 Cloud9-Entwicklungsumgebung
- Verwenden von CloudFormation AWS-Vorlagen zur Erstellung einer Webanwendung und eines Microservices für Bücher
- Verwenden von AWS Cloud9, um das Front-End zu modifizieren, Änderungen zu übernehmen und Änderungen zu testen
- Erstellen und Testen einer CI/CD-Pipeline zum Microservice
- Automatisierung von Komponententests

Der Code für dieses Muster befindet sich in GitHub, im DevOps AWS-End-Workshop-Repository.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Dateien aus dem DevOps AWS-End-Workshop wurden auf Ihren Computer heruntergeladen

Wichtig: Wenn Sie diese Demo-Anwendung in Ihrem AWS-Konto erstellen, werden AWS-Ressourcen erstellt und verbraucht. Sie sind für die Kosten der AWS-Services und Ressourcen verantwortlich, die für die Erstellung und Ausführung der Anwendung verwendet werden. Stellen Sie sicher, dass Sie nach Abschluss Ihrer Arbeit alle Ressourcen entfernen, um laufende Gebühren zu vermeiden. Anweisungen zur Bereinigung finden Sie im Abschnitt Epics.

Einschränkungen

Diese exemplarische Vorgehensweise dient nur zu Demonstrations- und Entwicklungszwecken. Informationen zur Verwendung in einer Produktionsumgebung finden Sie unter Bewährte Sicherheitsmethoden in der Dokumentation zu AWS Identity and Access Management (IAM) und nehmen Sie die erforderlichen Änderungen an den IAM-Rollen, Amazon DynamoDB und anderen verwendeten Services vor. Die Webanwendung ist von der AWS Bookstore Demo App abgeleitet. Weitere Überlegungen finden Sie im Abschnitt Bekannte Einschränkungen der README-Datei.

Architektur

Die Architektur der Bookstore-Anwendung wird im Abschnitt Architektur der README-Datei für die AWS-Bookstore-Demo-App veranschaulicht.

Aus Sicht der Bereitstellung verwendet die Bookstore-Demo-App eine einzige CloudFormation Vorlage, um alle Dienste und Objekte in einem Stack bereitzustellen. Dieses Muster enthält einige Änderungen, um zu demonstrieren, wie ein bestimmter Entwickler oder ein bestimmtes Team an einem bestimmten Produkt (Bücher) arbeiten und es unabhängig vom Rest der Anwendung aktualisieren könnte. Aus diesem Grund teilt der Code für dieses Muster die AWS Lambda Lambda-Funktionen und zugehörigen Objekte für den Microservice Books in eine zweite CloudFormation Vorlage auf, die einen Books-Stack erstellt. Auf diese Weise können Sie sehen, wie der Microservice mithilfe von CI/CD-Praktiken aktualisiert wird. In der folgenden Abbildung kennzeichnet der gestrichelte Rand den Microservice Books.

Tools

Tools

- Jest-Framework zum Testen JavaScript
- Python 3.9

Code

Der Quellcode und die Vorlagen für dieses Muster sind im DevOps AWS-End-Workshop-Repository verfügbar. GitHub Bevor Sie die Schritte im Abschnitt Epics ausführen, laden Sie alle Dateien aus dem Repository auf Ihren Computer herunter.

Hinweis: Der Abschnitt Epics enthält die allgemeinen Schritte für diese exemplarische Vorgehensweise, um Ihnen allgemeine Informationen über den Prozess zu geben. Um jeden Schritt abzuschließen, finden Sie in der README-Datei im DevOps AWS-End-Workshop-Repository detaillierte Anweisungen.

Das DevOps AWS-End-to-End-Workshop-Repository erweitert das AWS Bookstore Demo App-Repository und verwendet eine modifizierte Version des AWS Cloud9-Bootstrapping-Codes, um die AWS Cloud9 Cloud9-IDE zu erstellen.

Bewährte Methoden

Die Verwendung der Bookstore-Anwendung ist unkompliziert. Im Folgenden finden Sie einige empfohlene bewährte Methoden:

- Bei der Installation der Anwendung können Sie einen Projektnamen Ihrer Wahl oder der Einfachheit halber den Standardnamen (`demobookstore`) verwenden.
- Nachdem Sie die Anwendung betriebsbereit haben, empfiehlt es sich, die Amazon Neptune Neptune-Datenbank herunterzufahren, wenn Sie den Test für einen weiteren Tag fortsetzen möchten, da die Datenbank-Instance zusätzliche Kosten verursachen kann. Beachten Sie jedoch, dass die Datenbank nach sieben Tagen automatisch gestartet wird.
- Einzelheiten zum Code finden Sie in der Dokumentation zum AWS Bookstore Demo App-Repository. Sie beschreibt jeden Microservice und jede Tabelle.
- Weitere bewährte Methoden finden Sie unter Einige Herausforderungen, wenn Sie Zeit haben... Abschnitt der README-Datei im DevOps AWS-End-Workshop-Repository. Wir empfehlen Ihnen,

die Informationen zu lesen, um sich eingehend mit zusätzlichen Sicherheitsfunktionen vertraut zu machen und Entkopplungsservices zu üben.

Epen

Laden Sie den Quellcode herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode von herunter GitHub.	Der Quellcode und die Vorlagen für dieses Muster sind im GitHub DevOps AWS-End-Workshop-Repository verfügbar. Bevor Sie die nächsten Schritte im Abschnitt Epics ausführen, laden Sie alle Dateien aus dem Repository auf Ihren Computer herunter. Hinweis: Der Abschnitt Epics enthält die allgemeinen Schritte für diese exemplarische Vorgehensweise, um Ihnen allgemeine Informationen über den Vorgang zu geben. Um jeden Schritt abzuschließen, finden Sie in der README-Datei im DevOps AWS-End-Workshop-Repository detaillierte Anweisungen. Das DevOps AWS-End-to-End-Workshop-Repository erweitert das AWS Bookstore Demo App-Repository und	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwendet eine modifizierte Version des AWS Cloud9-Bootstrapping-Codes, um die AWS Cloud9 Cloud9-IDE zu erstellen.	

Erstellen Sie die Bookstore-Webanwendung und den Books-Microservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Front-End- und Lambda-Funktionen für die Bookstore-App.	1. Melden Sie sich bei der CloudFormation Konsole an und stellen Sie die `DemoBookstoreMainTemplate.yml` Vorlage bereit, um den Stack zu erstellen. DemoBookStoreStack Dadurch werden die Front-End- und Lambda-Funktionen erstellt, die sich außerhalb des Microservices Books befinden. 2. Notieren Sie sich auf der Registerkarte Ausgaben des Stacks die URL der Website unter dem Label. WebApplication	Developer
Erstellen Sie den Microservice Books.	Stellen Sie auf der CloudFormation Konsole die `DemoBookstoreBooksServiceTemplate.yml` Vorlage bereit, um den DemoBooks	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ServiceStack Stack zu erstellen.	
Testen Sie Ihre Anwendung.	Verwenden Sie die Website-URL aus dem DemoBookStoreStack Stack, um auf die Bookstore-Anwendung zuzugreifen.	Developer

Verwenden Sie die Cloud9-Umgebung, um Ihre Anwendung zu verwalten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Cloud9 Cloud9-IDE.	Stellen Sie auf der CloudFormation Konsole die `C9EnvironmentTemplate.yml` Vorlage bereit, um eine AWS Cloud9 Cloud9-Umgebung zu erstellen.	Entwickler, Leiter des Entwicklers
Erstellen Sie CodeCommit Repositorys.	1. Melden Sie sich bei der CodeCommit AWS-Konsole an und vergewissern Sie sich, dass Sie über ein `demobookstore-WebAssets` Repository verfügen, das den Code für die Front-End-Anwendung enthält. 2. Erstellen Sie ein Repository für den Microservice Books namens. `demobookstore-BooksService`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Klonen Sie die beiden Repositorys in AWS Cloud9 (`demobookstore-WebAssets` und `demobookstore-BooksService`) mithilfe des `git clone` Befehls.	
Ändern Sie den Code im Frontend und überprüfen Sie die Pipeline.	1. Verwenden Sie AWS Cloud9, um einige Codeänderungen auf einer Webseite vorzunehmen. Dadurch wird das `demobookstore-WebAssets` Repository aktualisiert. 2. Stellen Sie auf der CodePipeline AWS-Konsole sicher, dass DemoBookStore-Assets-Pipeline läuft. 3. Testen Sie Ihre Webanwendung, indem Sie sie über den Browser aktualisieren (Strg+F5 in Firefox).	Developer

Implementieren Sie eine CI/CD-Pipeline für den Microservice Books

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die YAML-Dateien für das Build- und Service-Update hinzu.	1. Laden Sie in AWS Cloud9 die `DemoBookstoreBooksServiceUpdateTemplate.yml`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dateien `buildspec.yml` und hoch. • `buildspec.yml` enthält Bauanweisungen und enthält auch Testanwei sungen für automatisierte Tests. Sie werden an dieser Stelle kommentie rt und werden später verwendet. • `DemoBookstoreBooks ServiceUp dateTempl ate.yml` ist eine aktualisierte Version von`DemoBooks toreBooks ServiceTe mplate.yml` , die in der Bereitstellungsphase der Pipeline verwendet werden soll. 2. Übergeben Sie die Dateien und übertragen Sie sie.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für die Build-Pipeline.	Um einen S3-Bucket zu erstellen, folgen Sie den Anweisungen in der Amazon S3 S3-Dokumentation. • Der Bucket-Name muss global eindeutig sein, zum Beispiel `demobookstore-books-service-pipeline-bucket-<YYYYMMDDHHMM>` . • Deaktivieren Sie das Kontrollkästchen Allen öffentlichen Zugriff blockieren und aktivieren Sie das Kontrollkästchen Ich bestätige...	Developer
Verwenden Sie IAM, um eine Rolle für die CloudFormation Bereitstellung zu erstellen.	Erstellen Sie eine `demobookstore-CloudFormation-role` Rolle und hängen Sie die `AdministratorAccess` Richtlinie an. Im nächsten Epic kannst du diese Rolle für Mindestberechtigungen neu konfigurieren.	Developer
Erstellen Sie eine neue Pipeline, um die Erstellung und Bereitstellung des Microservices Books zu automatisieren.	Erstellen Sie eine Pipeline (z. B. demobookstore- BooksService -Pipeline) mit den Phasen Commit, Build und Deploy, wie in der README-Datei beschrieben.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihren Microservice in AWS Cloud9.	Nehmen Sie eine Änderung an der ListBooksFunktion vor und sehen Sie, wie die Pipeline funktioniert.	Developer
Automatisieren Sie den Komponententest für die ListBooks Lambda-Funktion.	Aktivieren Sie in der AWS Cloud9 Cloud9-IDE den Build, um Komponententests auszuführen, und überprüfe n Sie die Testergebnisse. Anweisungen finden Sie in der README-Datei.	Developer

(Optional) Implementieren Sie zusätzliche Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Machen Sie Ihre Lösung sicher.	Stellen Sie `demobooks tore-CloudFormatio n-role` die Konfiguration so ein, dass Sie über Mindestbe rechtigungen verfügen, und überprüfen Sie auch andere verwendete Rollen.	Developer
Beseitigen Sie Abhängigk eiten in den CloudFormation Vorlagen.	Die Methode für den Informati onsaustausch zwischen der `DemoBookstoreMainT emplate.yml` Vorlage und der `DemoBookstoreBooks ServiceTemplate.yml` Vorlage basiert auf Ausgaben und Importen. Durch die Übergabe von Werten	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zwischen diesen beiden Vorlagen werden Abhängigkeiten hinzugefügt. Um die Abhängigkeiten zu beseitigen, sollten Sie die Verwendung von AWS Systems Manager Parameter Store in Betracht ziehen.	
Erstellen Sie einen Cart-Microservice.	Verwenden Sie den Microservice Books als Beispiel, um Funktionen im Zusammenhang mit Einkaufswagen aus der `DemoBookstoreMainTemplate.yml` Vorlage zu übernehmen und einen Warenkorb-Microservice zu erstellen.	Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die S3-Buckets.	Löschen Sie auf der Amazon S3 S3-Konsole die folgenden Buckets, die mit der Beispiel-Webanwendung verknüpft sind: • Zwei Buckets, die für die AWS Bookstore Demo App erstellt wurden. Die Buckets-Namen beginnen mit dem Stack-Namen, den Sie für AWS angegeben	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	haben CloudFormation , als Sie das Frontend erstellt haben; zum Beispiel. DemoBookStoreStack • <YYYYMMDDHHMM>Ein Bucket für die Build-Pipeline, zum Beispiel demobookstore-books-service-pipeline-bucket -.	
Lösche die Stapel.	Löschen Sie auf der CloudFormation Konsole die Stacks, die der Beispiel-Webanwendung zugeordnet sind: • DemoBooksServiceStack • DemoBookStoreStack Das Entfernen kann mehr als 90 Minuten dauern. Wenn das Entfernen fehlschlägt, löschen Sie sie erneut und löschen Sie auch alle manuellen Ressourcen (z. B. die VPC oder Netzwerkschnittstellen), die auf Benachrichtigungen basieren.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die IAM-Rollen.	Löschen Sie auf der IAM-Konsole die folgenden Rollen: • `demobookstore-Cloudformation-role` • `demobookstore-BooksService-BuildProject-service-role` step-by-step Anweisungen finden Sie in der IAM-Dokumentation.	Developer

Zugehörige Ressourcen

- AWS-Bookstore-Demo-App
- Beispiel für AWS Cloud9-Bootstrapping
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)

Zusätzliche Informationen

Eine ausführliche step-by-step Anleitung finden Sie in der README-Datei im DevOps GitHub AWS-End-Workshop-Repository.

Über das Update vom Mai 2023: Dieses Muster wurde aktualisiert, um neuere Versionen von Node und Python zu verwenden. Wir haben viele Pakete im Quellcode aktualisiert und Glyphicon entfernt, da es nicht mehr kostenlos ist. Wir haben auch alle Abhängigkeiten vom AWS Bookstore Demo App-Repository entfernt, sodass sich die beiden Repositorys nun unabhängig voneinander weiterentwickeln können.

Erstellen und pushen Sie Docker-Images mithilfe von GitHub Aktionen und Terraform auf Amazon ECR

Erstellt von Ruchika Modi (AWS)

Code-Repository: docker-ecr-actions-workflow	Umgebung: Produktion	Technologien: DevOps; Container und Microservices; Infrastruktur
Workload: Alle anderen Workloads	AWS-Services: Amazon ECR	

Übersicht

Dieses Muster erklärt, wie Sie wiederverwendbare GitHub Workflows erstellen können, um Ihre Dockerfile zu erstellen und das resultierende Image an Amazon Elastic Container Registry (Amazon ECR) zu übertragen. Das Muster automatisiert den Erstellungsprozess Ihrer Dockerfiles mithilfe von Terraform und GitHub Aktionen. Dies minimiert die Möglichkeit menschlicher Fehler und reduziert die Bereitstellungszeit erheblich.

Eine GitHub Push-Aktion an den Hauptzweig Ihres GitHub Repositorys initiiert die Bereitstellung von Ressourcen. Der Workflow erstellt ein eindeutiges Amazon ECR-Repository basierend auf der Kombination aus GitHub Organisation und Repository-Name. Anschließend wird das Dockerfile-Image in das Amazon ECR-Repository übertragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein aktives GitHub Konto.
- Ein GitHub Repository .
- Terraform Version 1 oder höher installiert und konfiguriert.
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket für das Terraform-Backend .

- Eine Amazon-DynamoDB-Tabelle für Terraform-Statussperren und Konsistenz. Die Tabelle muss einen Partitionsschlüssel mit dem Namen `LockID` und dem Typ haben`String`. Wenn dies nicht konfiguriert ist, wird die Statussperre deaktiviert.
- Eine AWS Identity and Access Management (IAM)-Rolle, die über Berechtigungen zum Einrichten des Amazon S3-Backends für Terraform verfügt. Eine Konfigurationsanleitung finden Sie in der Terraform-Dokumentation.

Einschränkungen

Dieser wiederverwendbare Code wurde nur mit GitHub Aktionen getestet.

Architektur

Zieltechnologie-Stack

- Amazon-ECR-Repository
- GitHub Aktionen
- Terraform

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Ein Benutzer fügt dem GitHub Repository Dockerfile- und Terraform-Vorlagen hinzu.

2. Diese Ergänzungen lösen einen GitHub Aktions-Workflow aus.

3. Der Workflow prüft, ob ein Amazon-ECR-Repository vorhanden ist. Ist dies nicht der Fall, wird das Repository basierend auf der GitHub Organisation und dem Repository-Namen erstellt.

4. Der Workflow erstellt das Dockerfile und überträgt das Image an das Amazon-ECR-Repository.

Tools

Amazon-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Registry-Service, der sicher, skalierbar und zuverlässig ist.

Andere Tools

- GitHub Aktionen sind in die GitHub Plattform integriert, damit Sie Workflows in Ihren GitHub Repositorys erstellen, freigeben und ausführen können. Sie können GitHub Aktionen verwenden, um Aufgaben wie das Erstellen, Testen und Bereitstellen Ihres Codes zu automatisieren.
- Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit HashiCorp dem Sie Cloud- und On-Premises-Infrastruktur erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub Workflow-Repository Docker ECR Actions verfügbar.

- Wenn Sie GitHub Aktionen erstellen, werden Docker-Workflow-Dateien im `/.github/workflows/` Ordner dieses Repositorys gespeichert. Der Workflow für diese Lösung befindet sich in der Datei workflow.yaml.
- Der `e2e-test` Ordner enthält ein Beispiel-Dockerfile für Referenz- und Testzwecke.

Bewährte Methoden

- Bewährte Methoden zum Schreiben von Dockerfiles finden Sie in der Docker-Dokumentation.
- Verwenden Sie einen VPC-Endpunkt für Amazon ECR . VPC-Endpunkte werden von AWS unterstützt PrivateLink, einer Technologie, mit der Sie über private IP-Adressen privat auf Amazon ECR-APIs zugreifen können. Bei Amazon-ECS-Aufgaben, die den Starttyp Fargate verwenden, ermöglicht der VPC-Endpunkt der Aufgabe, private Images von Amazon ECR abzurufen, ohne der Aufgabe eine öffentliche IP-Adresse zuzuweisen.

Sekunden

Einrichten des OIDC-Anbieters und des GitHub Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie OpenID Connect.	Erstellen Sie einen OpenID Connect (OIDC)-Anbieter. Sie verwenden den Anbieter in der Vertrauensrichtlinie für die	AWS-Administrator, AWS DevOps, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Rolle, die in dieser Aktion verwendet wird. Anweisungen finden Sie unter Konfigurieren von OpenID Connect in Amazon Web Services in der -GitHub Dokumentation.	
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub Docker ECR Actions Workflow-Repository in Ihren lokalen Ordner: `$git clone https://github.com/aws-samples/docker-ecr-actions-workflow`	DevOps Techniker

Anpassen des GitHub wiederverwendbaren Workflows und Bereitstellen des Docker-Images

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Ereignis an, das den Docker-Workflow initiiert.	Der Workflow für diese Lösung befindet sich in workflow.yaml. Dieses Skript ist derzeit so konfiguriert, dass Ressourcen bereitgestellt werden, wenn es das `workflow_dispatch` Ereignis empfängt. Sie können diese Konfiguration anpassen, indem Sie das Ereignis in ändern `workflow_call` und den Workflow von einem anderen übergeordneten Workflow aufrufen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie den Workflow an.	Die Datei workflow.yaml ist so konfiguriert, dass sie einen dynamischen, wiederverwendbaren GitHub Workflow erstellt. Sie können diese Datei bearbeiten, um die Standardkonfiguration anzupassen, oder Sie können die Eingabewerte aus der GitHub Aktionskonsole übergeben, wenn Sie das `workflow_dispatch` Ereignis verwenden, um die Bereitstellung manuell zu initiieren. • Stellen Sie sicher, dass Sie die richtige AWS-Konto-ID und Zielregion angeben. • Erstellen Sie eine Amazon-ECR-Lebenszyklusrichtlinie (siehe Beispielrichtlinie) und aktualisieren Sie den Standardpfad (`e2e-test/policy.json`) entsprechend. • Die Workflow-Datei erfordert zwei IAM-Rollen als Eingabe: • Eine IAM-Rolle, die über Berechtigungen zum Einrichten des Amazon S3-Backends für Terraform verfügt (siehe	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abschnitt Voraussetzungen). Sie können den Standardrollennamen `workload-assumable-role` in der Datei `yaml` entsprechend aktualisieren. • Eine IAM-Rolle, die über Berechtigungen für den Zugriff auf verfügt GitHub. Diese Rolle wird auch in der Amazon-ECR-Richtlinie verwendet, um Amazon-ECR-Operationen einzuschränken. Weitere Informationen finden Sie in der Datei data.tf.	
Stellen Sie die Terraform-Vorlagen bereit.	Der Workflow stellt automatisch die Terraform-Vorlagen bereit, die das Amazon ECR-Repository erstellen, basierend auf dem von Ihnen konfigurierten GitHub Ereignis. Diese Vorlagen sind als `.tf` Dateien im Stammverzeichnis des Github-Repositorys verfügbar.	AWS DevOps, DevOps Techniker

Fehlerbehebung

Problem	Lösung
Probleme oder Fehler bei der Konfiguration von Amazon S3 und DynamoDB als Terraform-Remote-Backend.	Folgen Sie den Anweisungen in der Terraform-Dokumentation, um die erforderlichen Berechtigungen für die Amazon S3- und DynamoDB-Ressourcen für die Remote-Backend-Konfiguration einzurichten.
Workflow kann nicht mit dem `workflow_dispatch` Ereignis ausgeführt oder gestartet werden.	Der Workflow, der für die Bereitstellung über das `workflow_dispatch` Ereignis konfiguriert ist, funktioniert nur, wenn der Workflow auch auf dem Hauptzweig konfiguriert ist.

Zugehörige Ressourcen

- Wiederverwenden von Workflows (GitHub Dokumentation)
- Auslösen eines Workflows (GitHub Dokumentation)

Erstellen und testen Sie iOS-Apps mit AWS CodeCommit CodePipeline, AWS und AWS Device Farm

Erstellt von Abdullahi Olaoye (AWS)

R-Typ: N/A	Quelle: Lokale Prozesse DevOps	Ziel: CI/CD-Pipeline für die Entwicklung von iOS-Apps auf AWS
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Web- und mobile Apps; DevOps
AWS-Dienste: AWS CodeCommit; AWS CodePipeline; AWS-Gerätefarm		

Übersicht

Dieses Muster beschreibt die Schritte zur Erstellung einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery), die AWS verwendet, CodePipeline um iOS-Anwendungen auf echten Geräten auf AWS zu erstellen und zu testen. Das Muster verwendet AWS CodeCommit zum Speichern des Anwendungscodes, das Jenkins-Open-Source-Tool zum Erstellen der iOS-Anwendung und AWS Device Farm, um die erstellte Anwendung auf realen Geräten zu testen. Diese drei Phasen werden mithilfe von AWS CodePipeline zusammen in einer Pipeline orchestriert.

Dieses Muster basiert auf dem Beitrag Erstellen und Testen von iOS- und iPadOS-Apps mit AWS DevOps und mobilen Diensten im DevOps AWS-Blog. Eine ausführliche Anleitung finden Sie im Blogbeitrag.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Apple-Entwicklerkonto
- Server erstellen (macOS)

- Xcode Version 11.3 (auf dem Build-Server installiert und eingerichtet)
- Auf der Workstation installierte und konfigurierte AWS-Befehlszeilenschnittstelle (AWS CLI)
- Grundkenntnisse in Git

Einschränkungen

- Auf dem Anwendungs-Build-Server muss macOS ausgeführt werden.
- Der Build-Server muss über eine öffentliche IP-Adresse verfügen, sodass er sich remote mit ihm verbinden CodePipeline kann, um Builds zu initiieren.

Architektur

Quelltechnologie-Stack

- Ein Prozess zur Erstellung von iOS-Anwendungen vor Ort, der die Verwendung eines Simulators oder einen manuellen Test auf physischen Geräten beinhaltet

Zieltechnologie-Stack

- Ein CodeCommit AWS-Repository zum Speichern von Anwendungsquellcode
- Ein Jenkins-Server für Anwendungsbuilds mit Xcode
- Ein AWS Device Farm Farm-Gerätepool zum Testen von Anwendungen auf realen Geräten

Zielarchitektur

Wenn ein Benutzer Änderungen am Quell-Repository festschreibt, ruft die Pipeline (AWS CodePipeline) den Code aus dem Quell-Repository ab, initiiert einen Jenkins-Build und übergibt den Anwendungscode an Jenkins. Nach dem Build ruft die Pipeline das Build-Artefakt ab und startet einen AWS Device Farm Farm-Job, um die Anwendung anhand eines Gerätepools zu testen.

Tools

- AWS CodePipeline ist ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs-

und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses bei jeder Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells.

- AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet. Es erleichtert Teams die Zusammenarbeit an Code in einem sicheren und hoch skalierbaren Ökosystem. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen.
- AWS Device Farm ist ein Service zum Testen von Anwendungen, mit dem Sie die Qualität Ihrer Web- und mobilen Apps verbessern können, indem Sie sie mit einer Vielzahl von Desktop-Browsern und echten Mobilgeräten testen, ohne eine Testinfrastruktur bereitstellen und verwalten zu müssen.
- Jenkins ist ein Open-Source-Automatisierungsserver, der es Entwicklern ermöglicht, ihre Software zu erstellen, zu testen und bereitzustellen.

Epen

Richten Sie die Build-Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Jenkins auf dem Build-Server, auf dem macOS ausgeführt wird.	Jenkins wird für die Erstellung der Anwendung verwendet, daher müssen Sie sie zuerst auf dem Build-Server installieren. Detaillierte Anweisungen für diese und nachfolgende Aufgaben finden Sie im AWS-Blogbeitrag Erstellen und Testen von iOS- und iPadOS-Apps mit AWS DevOps und mobilen Services und anderen Ressourcen im Abschnitt Verwandte Ressourcen am Ende dieses Musters.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Jenkins.	Folgen Sie den Anweisungen auf dem Bildschirm, um Jenkins zu konfigurieren.	DevOps
Installieren Sie das CodePipeline AWS-Plugin für Jenkins.	Dieses Plugin muss auf dem Jenkins-Server installiert sein, damit Jenkins mit dem AWS-Service interagieren kann. CodePipeline	DevOps
Erstellen Sie ein Jenkins-Freestyle-Projekt.	Erstellen Sie in Jenkins ein Freestyle-Projekt. Konfigurieren Sie das Projekt, um Trigger und andere Build-Konfigurationsoptionen anzugeben.	DevOps

AWS-Gerätefarm konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Device Farm Farm-Projekt.	Öffnen Sie die AWS Device Farm Farm-Konsole. Erstellen Sie ein Projekt und einen Gerätepool zum Testen. Anweisungen finden Sie im Blogbeitrag.	Developer

Konfigurieren Sie das Quell-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Erstellen Sie ein Repository, in dem der Quellcode gespeicherte wird.	DevOps
Übergeben Sie Ihren Anwendungscode in das Repository.	Connect zu dem CodeCommit Repository her, das Sie erstellt haben. Übertragen Sie den Code von Ihrem lokalen Computer in das Repository.	DevOps

Konfigurieren Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline in AWS CodePipeline.	Öffnen Sie die CodePipeline AWS-Konsole und erstellen Sie eine Pipeline. Die Pipeline orchestriert alle Phasen des CI/CD-Prozesses. Anweisungen finden Sie im AWS-Blogbeitrag Erstellen und Testen von iOS- und iPadOS-Apps mit AWS DevOps und mobilen Services.	DevOps
Fügen Sie der Pipeline eine Testphase hinzu.	Um eine Testphase hinzuzufügen und sie in AWS Device Farm zu integrieren, bearbeiten Sie die Pipeline.	DevOps
Initiieren Sie die Pipeline.	Um die Pipeline und den CI/CD-Prozess zu starten, wählen Sie Release change.	DevOps

Testergebnisse der Anwendung anzeigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Testergebnisse.	Wählen Sie in der AWS Device Farm Farm-Konsole das von Ihnen erstellte Projekt aus und überprüfen Sie die Ergebnisse der Tests. In der Konsole werden die Details der einzelnen Tests angezeigt.	Developer

Zugehörige Ressourcen

tep-by-step S-Anweisungen für dieses Muster

- iOS- und iPadOS-Apps mit AWS und mobilen Services erstellen DevOps und testen (DevOps AWS-Blogbeitrag)

AWS-Gerätefarm konfigurieren

- AWS Device Farm Farm-Konsole

Konfigurieren Sie das Quell-Repository

- Ein CodeCommit AWS-Repository erstellen
- Stellen Sie eine Connect zu einem CodeCommit AWS-Repository her

Konfigurieren Sie die Pipeline

- CodePipeline AWS-Konsole

Weitere Ressourcen

- CodePipeline AWS-Dokumentation
- CodeCommit AWS-Dokumentation

- Dokumentation zu AWS Device Farm
- Jenkins-Dokumentation
- Jenkins-Installation auf macOS
- CodePipeline AWS-Plugin für Jenkins
- Xcode-Installation
- Installation und Konfiguration von AWS CLI
- Git-Dokumentation

Überprüfen Sie AWS-CDK-Anwendungen oder - CloudFormation Vorlagen auf bewährte Methoden mithilfe von cdk-nag-Regelpaketen

Erstellt von Arun Donti

Umgebung: Produktion	Technologien: DevOps; Sicherheit, Identität, Compliance	Workload: Open-Source
AWS-Services: AWS CDK		

Übersicht

Dieses Muster erklärt, wie Sie das Hilfsprogramm cdk-nag verwenden können, um AWS Cloud Development Kit (AWS CDK)-Anwendungen auf bewährte Methoden zu überprüfen, indem Sie eine Kombination von Regelpaketen verwenden. cdk-nag ist ein Open-Source-Projekt, das von cfn_nag unterstützt wurde. Es implementiert Regeln in Bewertungspaketen wie AWS Solutions Library, Health Insurance Portability and Accountability Act (HIPAA) und National Institute of Standards and Technology (NIST) 800-53 unter Verwendung von AWS CDK Aspects . Sie können Ihre AWS-CDK-Anwendungen auf bewährte Methoden überprüfen, indem Sie die Regeln in diesen Paketen verwenden, Code basierend auf bewährten Methoden erkennen und korrigieren und die Regeln unterdrücken, die Sie nicht in Ihren Bewertungen verwenden möchten.

Sie können cdk-nag auch verwenden, um Ihre AWS- CloudFormation Vorlagen mithilfe des cloudformation-include-Moduls zu überprüfen.

Informationen zu allen verfügbaren Paketen finden Sie im Abschnitt Regeln des cdk-nag-Repositorys. Auswertungspakete sind verfügbar für:

- AWS-Lösungsbibliothek
- HIPAA-Sicherheit
- NIST 800-53, Version 4
- NIST 800-53, Version 5
- Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Anwendung, die das AWS-CDK verwendet

Tools

- AWS CDK – Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework für die Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS CloudFormation.
- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und Sie können sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.

Polen

Integrieren Sie cdk-nag in Ihre AWS-CDK-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfahren Sie mehr über cdk-nag.	Navigieren Sie zum Repository cdk-nag GitHub und lesen Sie die Dokumentation.	App-Developer
Installieren Sie das Paket cdk-nag in Ihrer AWS-CDK-Anwendung.	Um cdk-nag in Ihrer AWS-CDK-Anwendung zu verwenden, müssen Sie es zuerst installieren. cdk-nag kann von PyPI , npm NuGetund Apache Maven heruntergeladen werden. Die neuesten Informationen zu verfügbaren Versionen	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Download-Speicherorten finden Sie in der Readme-Datei im Repository.	
Wählen Sie Ihre aus NagPacks.	cdk-nag hat verschiedene Regelpakete namens NagPacks. Jedes NagPack enthält Regeln, die einem bestimmten Standard entsprechen. Die AWS-Lösungen NagPack enthalten beispielsweise allgemeine bewährte Methoden, und NIST 800-53 rev 5 NagPack kann bei der Compliance helfen. Sie können mehrere NagPacks auf Ihre Anwendung anwenden und bei Bedarf Pakete hinzufügen und entfernen. Eine Liste der verfügbaren Pakete finden Sie in der Readme-Datei im GitHub Repository. Informationen zu den einzelnen Regeln in jedem Paket finden Sie im Abschnitt Regeln des GitHub Repositorys.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Integrieren Sie cdk-nag in Ihre AWS-CDK-Anwendung.	Sie können cdk-nag auf anwendungsweiter Ebene in Ihre Anwendung integrieren oder in einzelne Phasen oder Stacks in Ihrer Anwendung integrieren. Um beispielsweise die AWS-Lösungen und HIPAA-Sicherheit NagPacks in eine AWS CDK v2- TypeScript Anwendung auf Anwendungsebene zu integrieren, können Sie den folgenden Code verwenden:
	`import { App, Aspects } from 'aws-cdk-lib';`
	`import { CdkTestStack } from '../lib/cdk-test-stack';`
	`import { AwsSolutionsChecks, HIPAASecurityChecks } from 'cdk-nag';`
	
	`const app = new App();`
	`new CdkTestStack(app, 'CdkNagDemo');`
	`// Simple rule informational messages`
	`Aspects.of(app).add(new AwsSolutionsChecks());`
	`// Additional explanations on the purpose of triggered rules`
	`Aspects.of(app).add(new HIPAASecurityChecks({ verbose: true }));`
		App-Developer

Zugehörige Ressourcen

- Code-Repository cdk-nag
- cdk-nag im Construct Hub

Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren

Erstellt von Shashi Dalmia (AWS) und Jay Enjamoori (AWS)

Umgebung: Produktion	Technologien: DevOps; Datenbanken; Sicherheit, Identität, Compliance	AWS-Services: Amazon DynamoDB ;AWS Identity and Access Management ;AWS Lambda

Übersicht

Dieses Muster erklärt die Schritte zur Konfiguration des kontoübergreifenden Zugriffs auf Amazon DynamoDB . Amazon Web Services (AWS)-Services können auf DynamoDB-Tabellen zugreifen, die sich im selben AWS-Konto befinden, wenn der Service über die entsprechenden AWS Identity and Access Management (IAM)-Berechtigungen verfügt, die in der Datenbank eingerichtet sind. Für den Zugriff von einem anderen AWS-Konto müssen jedoch IAM-Berechtigungen eingerichtet und eine Vertrauensstellung zwischen den beiden Konten eingerichtet werden.

Dieses Muster enthält Schritte und Beispielcode, um zu demonstrieren, wie Sie AWS Lambda-Funktionen in einem Konto so konfigurieren können, dass sie eine DynamoDB-Tabelle in einem anderen Konto lesen und in diese schreiben.

Voraussetzungen und Einschränkungen

- Zwei aktive AWS-Konten. Dieses Muster bezieht sich auf diese Konten als Konto A und Konto B .
- AWS Command Line Interface (AWS CLI) installiert und für den Zugriff auf Konto A konfiguriert, um die DynamoDB-Datenbank zu erstellen. Die anderen Schritte in diesem Muster enthalten Anweisungen zur Verwendung der IAM-, DynamoDB- und Lambda-Konsolen. Wenn Sie stattdessen AWS CLI verwenden möchten, konfigurieren Sie es für den Zugriff auf beide Konten.

Architektur

Im folgenden Diagramm befinden sich AWS Lambda , Amazon EC2 und DynamoDB alle im selben Konto. In diesem Szenario können Lambda-Funktionen und Amazon Elastic Compute Cloud (Amazon EC2)-Instances auf DynamoDB zugreifen.

Wenn Ressourcen in einem anderen AWS-Konto versuchen, auf DynamoDB zuzugreifen, müssen sie einen kontoübergreifenden Zugriff und eine Vertrauensstellung einrichten. Um beispielsweise im folgenden Diagramm den Zugriff zwischen DynamoDB in Konto A und der Lambda-Funktion in Konto B zu ermöglichen, müssen Sie eine Vertrauensstellung zwischen den Konten erstellen und den Benutzern des Lambda-Service und des entsprechenden Zugriffs gewähren, wie im Abschnitt „Epics“ beschrieben.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.

Code

Dieses Muster enthält Beispielcode im Abschnitt Zusätzliche Informationen, um zu veranschaulichen, wie Sie eine Lambda-Funktion in Konto B so konfigurieren können, dass sie aus der DynamoDB-Tabelle in Konto A schreibt und liest. Der Code wird nur zu Veranschaulichungs- und Testzwecken bereitgestellt. Wenn Sie dieses Muster in einer Produktionsumgebung implementieren, verwenden Sie den Code als Referenz und passen Sie ihn für Ihre eigene Umgebung an.

Dieses Muster veranschaulicht den kontoübergreifenden Zugriff mit Lambda und DynamoDB . Sie können dieselben Schritte auch für andere AWS-Services verwenden, müssen jedoch sicherstellen, dass Sie die entsprechenden Berechtigungen in beiden Konten erteilen und konfigurieren. Wenn Sie beispielsweise Zugriff auf eine Amazon Relational Database Service (Amazon RDS)-Datenbank in Konto A gewähren möchten, erstellen Sie eine Rolle für diese Datenbank und binden Sie sie an eine Vertrauensstellung an. Wenn Sie in Konto B Amazon EC2 anstelle von AWS Lambda verwenden möchten, erstellen Sie die entsprechende IAM-Richtlinie und -Rolle und fügen Sie sie dann an die EC2-Instance an.

Polen

Erstellen einer DynamoDB-Tabelle in Konto A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine DynamoDB-Tabelle in Konto A.	Nachdem Sie AWS CLI für Konto A konfiguriert haben, verwenden Sie den folgenden AWS CLI-Befehl, um eine DynamoDB-Tabelle zu erstellen:
	`aws dynamodb create-table \`
	`--table-name Table-Acccount-A \`
	`--attribute-definitions \`
	`Attribute Name=category,AttributeType=S \`
	`Attribute Name=item,AttributeType=S \`
	`--key-schema \`
	`Attribute Name=category,KeyType=HASH \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Attribute Name=item,KeyType=RANGE \ --provisioned-throughput \ ReadCapacityUnits=5,WriteCapacityUnits=5` Weitere Informationen zum Erstellen von Tabellen finden Sie in der DynamoDB-Dokumentation.	

Erstellen einer Rolle in Konto A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle in Konto A.	Diese Rolle wird von Konto B verwendet, um Berechtigungen für den Zugriff auf Konto A zu erhalten. So erstellen Sie die Rolle: 1. Melden Sie sich bei Konto A unter an`https://<account-ID-for-Account-A>.signin.aws.amazon.com/console` . 2. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/. 3. Wählen Sie im Navigationsbereich der Konsole	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Rollen und dann Rolle erstellen aus. 4. Wählen Sie für Vertrauen swürdige Entität auswählen die Option AWS-Konto und im Abschnitt Ein AWS-Konto die Option Ein anderes AWS-Konto aus. 5. Geben Sie für Konto-ID die ID für Konto B ein. 6. Wählen Sie Weiter: Berechtigungen aus. 7. Geben Sie im Feld Richtlini en filtern DynamoDB ein. 8. Wählen Sie in der Liste der DynamoDB-Richtlini en AmazonDynamoDB ausFullAccess. Hinweis: Diese Richtlini e erlaubt alle Aktionen in DynamoDB . Als bewährte Sicherheitsmethode sollten Sie immer nur die erforderl ichen Berechtigungen erteilen. Eine Liste anderer Richtlinien, die Sie stattdess en auswählen können, finden Sie unter Beispielr ichtlinien in der IAM-Dokum entation. 9. Wählen Sie Weiter: Name, Überprüfung und Erstellung von .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Geben Sie für Rollenname einen eindeutigen Namen für Ihre Rolle ein (z. B. DynamoDB -FullAcce ss-For-Account-B) und fügen Sie eine optionale Rollenbeschreibung hinzu. 11. Überprüfen Sie alle Abschnitte und fügen Sie der Rolle (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. 12. Wählen Sie Rolle erstellen aus. Weitere Informationen zum Erstellen von Rollen finden Sie in der IAM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich den ARN für die Rolle in Konto A.	1. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen aus. 2. Geben Sie im Suchfeld DynamoDB -FullAccess-For-Account-B (oder den Rollennamen, den Sie in der vorherigen Geschichte erstellt haben) ein und wählen Sie die Rolle aus. 3. Kopieren Sie auf der Übersichtsseite für die Rolle den Amazon-Ressourcennamen (ARN). Sie verwenden den ARN, wenn Sie den Lambda-Code in Konto B einrichten.	AWS DevOps

Konfigurieren des Zugriffs auf Konto A von Konto B aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Richtlinie für den Zugriff auf Konto A.	1. Melden Sie sich bei Konto B unter an`https://<account-ID-for-Account-B>.signin.aws.amazon.com/console` . 2. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/. 3. Wählen Sie im Navigationsbereich der Konsole	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Richtlinien und dann Richtlinie erstellen aus. 4. Wählen Sie den Tab JSON. 5. Geben Sie das folgende JSON-Dokument ein oder fügen Sie es ein: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::<Account-A-ID>:role/DynamoDB-FullAccess-For-Account-B" } ] }` wobei die `Resource` Eigenschaft den ARN der Rolle enthält, die Sie in der vorherigen Geschichte in Konto A erstellt haben. 6. Wählen Sie Weiter: Markierungen. 7. (Optional) Fügen Sie der Richtlinie Metadaten hinzu, indem Sie Tags	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als Schlüssel-Wert-Paare anfügen. 8. Wählen Sie Weiter: Prüfen aus. 9. Geben Sie für Richtlini enname einen eindeutig en Namen für Ihre Richtlini e ein (z. B. DynamoDB - FullAccess-Policy-in-Accou nt-A) und fügen Sie eine optionale Richtlinienbeschre ibung hinzu. 10. Wählen Sie Richtlinie erstellen aus. Weitere Informationen zum Erstellen von Richtlinien finden Sie in der IAM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle basierend auf der Richtlinie.	Diese Rolle wird von den Lambda-Funktionen in Konto B zum Lesen und Schreiben in die DynamoDB-Tabelle in Konto A verwendet. 1. Wählen Sie in Konto B im Navigationsbereich der IAM-Konsole Rollen und dann Rolle erstellen aus. 2. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität wählen) die Option AWS service (Service) aus. 3. Wählen Sie für den Anwendungsfall Lambda aus. 4. Wählen Sie Weiter: Berechtigungen aus. 5. Geben Sie im Feld Richtlini en filtern DynamoDB ein. 6. Wählen Sie in der Liste der DynamoDB-Richtlinien DynamoDB -FullAccess-Policy-in-Account-A aus, die Sie in der vorherigen Geschichte erstellt haben. 7. Wählen Sie Weiter: Name, Überprüfung und Erstellung von . 8. Geben Sie unter Rollennam e einen eindeutigen Namen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für Ihre Rolle ein (z. B. DynamoDB -FullAccess-in-Account-A) und fügen Sie eine optionale Rollenbeschreibung hinzu. 9. Überprüfen Sie alle Abschnitte und fügen Sie der Rolle (optional) Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. 10. Wählen Sie Rolle erstellen aus. Sie können diese Rolle jetzt im nächsten Epos an die Lambda-Funktionen anfügen. Weitere Informationen zum Erstellen von Rollen finden Sie in der IAM-Dokumentation.	

Erstellen von Lambda-Funktionen in Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion, um Daten in DynamoDB zu schreiben.	1. Melden Sie sich bei Konto B unter an `https://<account-ID-for-Account-B>.signin.aws.amazon.com/console` .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda/. 3. Wählen Sie im Navigationsbereich der Konsole Funktionen und dann Funktion erstellen aus. 4. Geben Sie für Name lambda_write_function ein. 5. Wählen Sie für Laufzeit Python 3.8 oder höher aus. 6. Wählen Sie für Berechtigungen, Ändern der Standardausführungsrolle die Option Vorhandene Rolle verwenden aus. 7. Wählen Sie für Vorhandene Rolle die Option DynamoDB-FullAccess-in-Account-A aus. 8. Wählen Sie Funktion erstellen. 9. Fügen Sie auf der Registerkarte Code den Beispielcode der Lambda-Schreibfunktion ein, der im Abschnitt Zusätzliche Informationen in diesem Muster bereitgestellt wird. Stellen Sie sicher, dass Sie den richtigen Rollen-ARN (aus dem Epos Create a role in Account A) für das `RoleArn` Feld	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	angeben und `region_name` zu ändern, wo die DynamoDB-Tabelle in Konto A erstellt wird (aus dem Epos Create a DynamoDB table in Account A). Wenn Sie dies nicht tun, wird ein `ResourceNotFoundException` Fehler ausgegeben. 10. Um den Code bereitzustellen, wählen Sie Bereitstellen aus. 11. Führen Sie die Funktion aus, indem Sie Test auswählen. Dadurch werden Sie aufgefordert, ein Testereignis zu konfigurieren. Erstellen Sie ein neues Ereignis mit Ihrem bevorzugten Namen, z. B. MyTestEventForWrite, und speichern Sie die Konfiguration. 12. Führen Sie die Funktion erneut aus, indem Sie Test auswählen. Dadurch wird der Code mit dem von Ihnen angegebenen Ereignisnamen ausgeführt. 13. Überprüfen Sie die Ausgabe der Funktion. Er sollte der Ausgabe ähneln, die im Abschnitt Lambda-Sc	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hreibfunktion unter Zusätzlic he Informationen angezeigt wird. Diese Ausgabe zeigt an, dass die Funktion auf die DynamoDB-Tabelle in Konto A zugegriffen hat und Daten darin schreiben konnte. Weitere Informationen zum Erstellen von Lambda-Fu nktionen finden Sie in der Lambda-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion, um Daten aus DynamoDB zu lesen.	1. Wählen Sie im Navigationsbereich der Lambda-Konsole Funktionen und dann Funktion erstellen aus. 2. Geben Sie für Name lambda_read_function ein. 3. Wählen Sie für Laufzeit Python 3.8 oder höher aus. 4. Wählen Sie für Berechtigungen , Ändern der Standardausführungsrolle die Option Vorhandene Rolle verwenden aus. 5. Wählen Sie für Vorhandene Rolle die Option DynamoDB-FullAccess-in-Account-A aus. 6. Wählen Sie Funktion erstellen. 7. Fügen Sie auf der Registerkarte Code den Beispielcode der Lambda-Lesefunktion ein, der in diesem Muster im Abschnitt Zusätzliche Informationen bereitgestellt wird. Stellen Sie sicher, dass Sie den richtigen Rollen-ARN (aus dem Epos Create a role in Account A) für das `RoleArn` Feld angeben und `region_name` zu ändern, wo die DynamoDB-Tabelle in	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konto A erstellt wird (aus dem Epos Create a DynamoDB table in Account A). Wenn Sie dies nicht tun, wird ein `ResourceNotFoundException` Fehler ausgegeben. 8. Um den Code bereitzustellen, wählen Sie Bereitstellen aus. 9. Führen Sie die Funktion aus, indem Sie Test auswählen. Dadurch werden Sie aufgefordert, ein Testereignis zu konfigurieren. Erstellen Sie ein neues Ereignis mit Ihrem bevorzugten Namen, z. B. MyTestEventForRead, und speichern Sie die Konfiguration. 10. Führen Sie die Funktion erneut aus, indem Sie Test auswählen. Dadurch wird der Code mit dem von Ihnen angegebenen Ereignisnamen ausgeführt. 11. Überprüfen Sie die Ausgabe der Funktion. Er sollte der Ausgabe ähneln, die im Abschnitt Lambda-Lesefunktion unter Zusätzliche Informationen angezeigt wird. Diese Ausgabe zeigt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an, dass die Funktion auf die DynamoDB-Tabelle in Konto A zugegriffen hat und die Daten lesen konnte, die Sie der Tabelle hinzugefügt haben. Weitere Informationen zum Erstellen von Lambda-Fu nktionen finden Sie in der Lambda-Dokumentation.	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Ressourcen, die Sie erstellt haben.	Wenn Sie dieses Muster in einer Test- oder Machbarke itsnachweis-Umgebung (PoC) ausführen, löschen Sie die von Ihnen erstellten Ressourcen, um Kosten zu vermeiden. 1. Löschen Sie in Konto B die beiden Lambda-Funktionen und andere Ressourcen, die Sie für die Verbindun g mit DynamoDB erstellt haben. 2. Löschen Sie in Konto A die DynamoDB-Tabelle, die Sie erstellt haben. 3. IAM-Richtlinien kosten nichts, sodass Sie sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unverändert lassen können. Aus Sicherheitsgründen empfehlen wir jedoch, die folgenden Rollen und Richtlinien zu löschen, die Sie für dieses Muster erstellt haben: • Konto A: DymamoDB - Full-Access-for-Account-A-Rolle • Konto B: DynamoDB - FullAccess-in-Account-A-Rolle • Konto B: DynamoDB - FullAccess-Policy-in-Account-A-Richtlinie	

Zugehörige Ressourcen

- Erste Schritte mit der AWS CLI (AWS CLI-Dokumentation)
- Konfigurieren der AWS CLI (AWS CLI-Dokumentation)
- Erste Schritte mit DynamoDB (DynamoDB-Dokumentation)
- Erste Schritte mit Lambda (AWS Lambda-Dokumentation)
- Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer (IAM-Dokumentation)
- Erstellen von IAM-Richtlinien (IAM-Dokumentation)
- Kontoübergreifende Auswertungslogik für Richtlinien (IAM-Dokumentation)
- Referenz zu IAM-JSON-Richtlinienelementen (IAM-Dokumentation)

Zusätzliche Informationen

Der Code in diesem Abschnitt dient nur zu Veranschaulichungs- und Testzwecken. Wenn Sie dieses Muster in einer Produktionsumgebung implementieren, verwenden Sie den Code als Referenz und passen Sie ihn für Ihre eigene Umgebung an.

Lambda-Schreibfunktion

Beispielcode

```
import boto3
from datetime import datetime


sts_client = boto3.client('sts')
sts_session = sts_client.assume_role(RoleArn='arn:aws:iam::<Account-A ID>:role/
DynamoDB-FullAccess-For-Account-B', RoleSessionName='test-dynamodb-session')


KEY_ID = sts_session['Credentials']['AccessKeyId']
ACCESS_KEY = sts_session['Credentials']['SecretAccessKey']
TOKEN = sts_session['Credentials']['SessionToken']


dynamodb_client = boto3.client('dynamodb',
                               region_name='<DynamoDB-table-region-in-account-A',
                               aws_access_key_id=KEY_ID,
                               aws_secret_access_key=ACCESS_KEY,
                               aws_session_token=TOKEN)

def lambda_handler(event, context):
     now = datetime.now()
     date_time = now.strftime("%m/%d/%Y, %H:%M:%S")
     data = dynamodb_client.put_item(TableName='Table-Acccount-A', Item={"category":
 {"S": "Fruit"},"item": {"S": "Apple"},"time": {"S": date_time}})
     return data
```

Beispielausgabe

Lambda-Lesefunktion

Beispielcode

```
import boto3
from datetime import datetime


sts_client = boto3.client('sts')
sts_session = sts_client.assume_role(RoleArn='arn:aws:iam::<Account-A ID>:role/
DynamoDB-FullAccess-For-Account-B', RoleSessionName='test-dynamodb-session')


KEY_ID = sts_session['Credentials']['AccessKeyId']
ACCESS_KEY = sts_session['Credentials']['SecretAccessKey']
TOKEN = sts_session['Credentials']['SessionToken']


dynamodb_client = boto3.client('dynamodb',
                               region_name='<DynamoDB-table-region-in-account-A>',
                               aws_access_key_id=KEY_ID,
                               aws_secret_access_key=ACCESS_KEY,
                               aws_session_token=TOKEN)


def lambda_handler(event, context):
     response = dynamodb_client.get_item(TableName='Table-Acccount-A', Key={'category':
{'S':'Fruit'}, 'item':{'S':'Apple'}})
     return response
```

Beispielausgabe

Konfigurieren der gegenseitigen TLS-Authentifizierung für Anwendungen, die auf Amazon EKS ausgeführt werden

Erstellt vonendra Siddappa (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Sicherheit, Identität, Compliance	AWS-Services: Amazon EKS; Amazon Route 53

Übersicht

Zertifikatbasierte gegenseitige Transport Layer Security (TLS) ist eine optionale TLS-Komponente, die bidirektionale Peer-Authentifizierung zwischen Servern und Clients bietet. Bei gegenseitiger TLS müssen Clients während der Sitzungsaushandlung ein X.509-Zertifikat bereitstellen. Der Server verwendet dieses Zertifikat, um den Client zu identifizieren und zu authentifizieren.

Gegenseitiges TLS ist eine gängige Anforderung für Internet of Things (IoT)-Anwendungen und kann für business-to-business Anwendungen oder Standards wie Open Banking verwendet werden.

Dieses Muster beschreibt, wie Sie gegenseitiges TLS für Anwendungen konfigurieren, die auf einem Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster ausgeführt werden, indem Sie einen NGINX-Controller für eingehenden Datenverkehr verwenden. Sie können die integrierten gegenseitigen TLS-Funktionen für den NGINX-Controller für eingehenden Datenverkehr aktivieren, indem Sie die Ressource für eingehenden Datenverkehr kommentieren. Weitere Informationen zu gegenseitigen TLS-Anmerkungen auf NGINX-Controllern finden Sie unter Client-Zertifikatauthentifizierung in der Kubernetes-Dokumentation.

Wichtig: Dieses Muster verwendet selbstsignierte Zertifikate. Wir empfehlen, dieses Muster nur mit Test-Clustern und nicht in Produktionsumgebungen zu verwenden. Wenn Sie dieses Muster in einer Produktionsumgebung verwenden möchten, können Sie AWS Private Certificate Authority (AWS Private CA) oder Ihren vorhandenen PKI-Standard (Public Key Infrastructure) verwenden, um private Zertifikate auszustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto.
- Ein vorhandener Amazon-EKS-Cluster.
- AWS Command Line Interface (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert unter macOS , Linux oder Windows.
- Das kubectl-Befehlszeilen-Dienstprogramm, das für den Zugriff auf den Amazon-EKS-Cluster installiert und konfiguriert ist. Weitere Informationen dazu finden Sie unter Installieren von kubectl in der Amazon-EKS-Dokumentation.
- Ein vorhandener DNS-Name (Domain Name System) zum Testen der Anwendung.

Einschränkungen

- Dieses Muster verwendet selbstsignierte Zertifikate. Wir empfehlen, dieses Muster nur mit Test-Clustern und nicht in Produktionsumgebungen zu verwenden.

Architektur

Technologie-Stack

- Amazon EKS
- Amazon Route 53
- Kubectl

Tools

- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Kubectl ist ein Befehlszeilendienstprogramm, mit dem Sie mit einem Amazon-EKS-Cluster interagieren.

Polen

Generieren der selbstsignierten Zertifikate

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie den CA-Schlüssel und das Zertifikat.	Generieren Sie den Schlüssel und das Zertifikat der Zertifizierungsstelle (CA), indem Sie den folgenden Befehl ausführen. `openssl req -x509 -sha256 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 356 -nodes -subj '/CN=Test Cert Authority'`	DevOps Techniker
Generieren Sie den Serverschlüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat.	Generieren Sie den Serverschlüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat, indem Sie den folgenden Befehl ausführen. `openssl req -new -newkey rsa:4096 -keyout server.key -out server.csr -nodes -subj '/CN= <your_domain_name> ' && openssl x509 -req -sha256 -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt` Wichtig: Stellen Sie sicher, dass Sie durch <your_dom	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ain_name>` Ihren vorhandenen Domänennamen ersetzen.	
Generieren Sie den Clientschlüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat.	Generieren Sie den Clientschlüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat, indem Sie den folgenden Befehl ausführen. `openssl req -new -newkey rsa:4096 -keyout client.key -out client.csr -nodes -subj '/CN=Test' && openssl x509 -req -sha256 -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt`	DevOps Techniker

Bereitstellen des NGINX-Controllers für eingehenden Datenverkehr

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den NGINX-Controller für eingehenden Datenverkehr in Ihrem Amazon-EKS-Cluster bereit.	Stellen Sie den NGINX-Controller für eingehenden Datenverkehr mit dem folgenden Befehl bereit. `kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.7.0/deploy/static`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`/provider/aws/deployment.yaml`	
Stellen Sie sicher, dass der NGINX-Controller-Service für eingehenden Datenverkehr ausgeführt wird.	Überprüfen Sie mit dem folgenden Befehl, ob der NGINX-Controller-Service für eingehenden Datenverkehr ausgeführt wird. `kubectl get svc -n ingress-nginx` Wichtig: Stellen Sie sicher, dass das Feld der Serviceadresse den Domänennamen des Network Load Balancers enthält.	DevOps Techniker

Erstellen Sie einen Namespace im Amazon-EKS-Cluster, um gegenseitige TLS zu testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Namespace im Amazon-EKS-Cluster.	Erstellen Sie einen Namespace mit dem Namen `mtls` in Ihrem Amazon-EKS-Cluster, indem Sie den folgenden Befehl ausführen. `kubectl create ns mtls` Dadurch wird die Beispielanwendung bereitgestellt, um gegenseitiges TLS zu testen.	DevOps Techniker

Erstellen der Bereitstellung und des Services für die Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Kubernetes-Bereitstellung und den Service im mtls-Namespace.	Erstellen Sie eine Datei namens `mtls.yaml` . Fügen Sie folgenden Code in die Datei ein.
	
	`kind: Deployment`
	`apiVersion: apps/v1`
	`metadata:`
	`  name: mtls-app`
	`  labels:`
	`  app: mtls`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app: mtls`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: mtls`
	`  spec:`
	`  containers:`
	`  - name: mtls-app`
	`  image: hashicorp/http-echo`
	`  args:`
	`  - "-text=mTLS is working"`
	
	`---`
	
	`kind: Service`
	`apiVersion: v1`
	`metadata:`
	`  name: mtls-service`
	`spec:`
	`  selector:`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>app: mtls
	ports:
	- port: 5678 #
	Default port for image</pre>
	Erstellen Sie die Kubernetes-Bereitstellung und den Service im -`mtls`Namespace, indem Sie den folgenden Befehl ausführen.
	<pre>kubectl create -f
	mtls.yaml -n mtls</pre>	

Stellen Sie sicher, dass die Kubernetes-Bereitstellung erstellt wurde.	Führen Sie den folgenden Befehl aus, um zu überprüfe n, ob die Bereitstellung erstellt wurde und einen Pod mit dem Status „Verfügbar“ hat.
	<pre>kubectl get deploy -n
	mtls</pre>
		DevOps Techniker

Stellen Sie sicher, dass der Kubernetes-Service erstellt wurde.	Überprüfen Sie, ob der Kubernetes-Service erstellt wurde, indem Sie den folgenden Befehl ausführen.
	<pre>kubectl get service -n
	mtls</pre>
		DevOps Techniker

Erstellen eines Secrets im mtls-Namespace

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Secret für die Ingress-Ressource.	Führen Sie den folgenden Befehl aus, um mithilfe der Zertifikate, die Sie zuvor erstellt haben, ein Secret für den NGINX-Controller für eingehenden Datenverkehr zu erstellen. `kubectl create secret generic mtls-certs --from-file=tls.crt=server.crt --from-file=tls.key=server.key --from-file=ca.crt=ca.crt -n mtls` Ihr Secret verfügt über ein Serverzertifikat für den Client zur Identifizierung des Servers und ein CA-Zertifikat für den Server zur Überprüfung der Clientzertifikate.	DevOps Techniker

Erstellen der Ingress-Ressource im mtls-Namespace

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die ingress-Ressource im mtls-Namespace.	Erstellen Sie eine Datei namens `ingress.yaml` . Fügen Sie den folgenden Code in die Datei ein (ersetzen Sie durch `<your_domain_name>`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Ihren vorhandenen Domänennamen).
	
	`apiVersion: networking.k8s.io/v1`
	`kind: Ingress`
	`metadata:`
	`  annotations:`
	`  nginx.ingress.kubernetes.io/auth-tls-verify-client: "on"`
	`  nginx.ingress.kubernetes.io/auth-tls-secret: mtls/mtls-certs`
	`  name: mtls-ingress`
	`spec:`
	`  ingressClassName: nginx`
	`  rules:`
	`  - host: "*.<your_domain_name>"`
	`  http:`
	`  paths:`
	`  - path: /`
	`  pathType: Prefix`
	`  backend:`
	`  service:`
	`  name: mtls-service`
	`  port:`
	`  number: 5678`
	`  tls:`
	`  - hosts:`
	`  - "*.<your_domain_name>"`
	`  secretName: mtls-certs`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellen Sie die ingress-Ressource im -`mtls`Namespace, indem Sie den folgenden Befehl ausführen. `kubectl create -f ingress.yaml -n mtls` Das bedeutet, dass der NGINX-Controller für eingehenden Datenverk ehr Datenverkehr an Ihre Beispielanwendung weiterlei ten kann.	
Überprüfen Sie, ob die Ressource für eingehenden Datenverkehr erstellt wurde.	Überprüfen Sie, ob die Ressource für eingehenden Datenverkehr erstellt wurde, indem Sie den folgenden Befehl ausführen. `kubectl get ing -n mtls` Wichtig: Stellen Sie sicher, dass die Adresse der Ingress-Ressource den Load Balancer anzeigt, der für den NGINX-Ingress-Controller erstellt wurde.	DevOps Techniker

Konfigurieren Sie DNS so, dass der Hostname auf den Load Balancer verweist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CNAME-Datensatz, der auf den Load Balancer für den NGINX-Controller für eingehenden Datenverkehr verweist.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Route 53-Konsole und erstellen Sie einen kanonischen Namen (CNAME)-Datensatz, der `mtls.<your_domain_name>` auf den Load Balancer für den NGINX-Controller für eingehenden Datenverkehr verweist. Weitere Informationen finden Sie unter Erstellen von Datensätzen mithilfe der Route 53-Konsole in der Route 53-Dokumentation.	DevOps Techniker

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die gegenseitige TLS-Einrichtung ohne Zertifikate.	Führen Sie den folgenden Befehl aus. `curl -k https://mtls.<your_domain_name>` Sie sollten die Fehlermeldung „400 Kein erforderliches SSL-	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zertifikat wurde gesendet“ erhalten.	
Testen Sie die gegenseitige TLS-Einrichtung mit Zertifikaten.	Führen Sie den folgenden Befehl aus. `curl -k https://mtls.<your_domain_name> --cert client.crt --key client.key` Sie sollten die Antwort „mTLS funktioniert“ erhalten.	DevOps Techniker

Zugehörige Ressourcen

- Erstellen von Datensätzen mithilfe der Amazon Route 53-Konsole
- Verwenden eines Network Load Balancer smit dem NGINX Ingress Controller auf Amazon EKS
- Client-Zertifikatauthentifizierung

Erstellen eines benutzerdefinierten Protokollparsers für Amazon ECS mithilfe eines Firelens-Protokollrouters

Erstellt von Varun Sharma (AWS)

Umgebung: Produktion	Technologien: DevOps; Container und Microservices	Workload: Alle anderen Workloads
AWS-Services: Amazon ECS		

Übersicht

Firelens ist ein Protokollrouter für Amazon Elastic Container Service (Amazon ECS) und AWS Fargate. Sie können Firelens verwenden, um Containerprotokolle von Amazon ECS an Amazon CloudWatch und andere Ziele weiterzuleiten (z. B. Splunk oder Sumo Logic). Firelens funktioniert mit Fluentd oder Fluent Bit als Protokollierungsagent, was bedeutet, dass Sie Amazon-ECS-Aufgabendefinitionsparameter verwenden können, um Protokolle weiterzuleiten.

Wenn Sie Protokolle auf Quellebene analysieren, können Sie Ihre Protokolldaten analysieren und Abfragen durchführen, um effizienter und effektiver auf betriebliche Probleme zu reagieren. Da verschiedene Anwendungen unterschiedliche Protokollierungsmuster haben, müssen Sie einen benutzerdefinierten Parser verwenden, der die Protokolle strukturiert und die Suche an Ihrem Endziel erleichtert.

Dieses Muster verwendet einen Firelens-Protokollrouter mit einem benutzerdefinierten Parser, um Protokolle CloudWatch von einer Spring Boot-Beispielanwendung, die auf Amazon ECS ausgeführt wird, an zu übertragen. Anschließend können Sie Amazon CloudWatch Logs Insights verwenden, um die Protokolle basierend auf benutzerdefinierten Feldern zu filtern, die vom benutzerdefinierten Parser generiert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert auf Ihrem lokalen Computer.

- Docker, installiert und konfiguriert auf Ihrem lokalen Computer.
- Eine vorhandene auf Spring Boot basierende containerisierte Anwendung in Amazon Elastic Container Registry (Amazon ECR).

Architektur

Technologie-Stack

- CloudWatch
- Amazon ECR
- Amazon ECS
- Fargate
- Docker
- Fluent Bit

Tools

- Amazon ECR – Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon ECS – Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Stoppen und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Identity and Access Management (IAM) – IAM ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services.
- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Docker – Docker ist eine offene Plattform für die Entwicklung, den Versand und die Ausführung von Anwendungen.

Code

Die folgenden Dateien sind an dieses Muster angehängt:

- `customFluentBit.zip` – Enthält die Dateien zum Hinzufügen der benutzerdefinierten Parsing- und -Konfigurationen.
- `firelens_policy.json` – Enthält das Richtliniendokument zum Erstellen einer IAM-Richtlinie.
- `Task.json` – Enthält eine Beispielaufgabendefinition für Amazon ECS.

Polen

Erstellen eines benutzerdefinierten Fluent-Bit-Images

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon ECR-Konsole und erstellen Sie ein Repository namens `fluentbit_custom` . Weitere Informationen dazu finden Sie unter Erstellen eines Repositorys in der Amazon-ECR-Dokumentation.	Systemadministrator, Entwickler
Entpacken Sie das customFluentBitZIP-Paket.	1. Laden Sie das -`customFluentBit.zip` Paket (angefügt) auf Ihren lokalen Computer herunter. 2. Entpacken Sie das `customFluentBit` Verzeichnis, indem Sie den folgenden Befehl ausführen: `unzip -d customFluentBit.zip` 3. Das Verzeichnis enthält die folgenden Dateien, die zum	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinzufügen der benutzerd efinierten Parsing- und - Konfigurationen erforderlich sind: • `parsers/springboot _parser.conf` – Enthält die Parser-Ri chtlinie und definiert das Muster für den regulären Ausdruck (Regex) für den benutzerdefinierte n Parser. Sie können das Regex-Muster für Ihren spezifischen Parser hinzufügen. • `conf/pars e_springboot.conf` – Enthält den Filter und die Service-Richtlinie. • Das Dockerfile	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das benutzerd efinierte Docker-Image.	1. Ändern Sie das Verzeichnis in `customFluentBit .` 2. Öffnen Sie die Amazon-ECR-Konsole, wählen Sie das `fluentbit _custom` Repository und dann Push-Befehle anzeigen aus. 3. Laden Sie Ihr Projekt hoch. 4. Nachdem der Upload abgeschlossen ist, kopieren Sie die URL des Builds. Diese URL ist erforderlich, wenn Sie einen Container in Amazon ECS erstellen Weitere Informationen dazu finden Sie unter Pushing a Docker image in der Amazon-ECR-Dokumentation.	Systemadministrator, Entwickler

Einrichten des Amazon-ECS-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-ECS-Cluster.	Erstellen Sie einen Amazon-ECS-Cluster, indem Sie den Anweisungen im Abschnitt Nur Netzwerkvorlage unter Erstellen eines Clusters in der Amazon-ECS-Dokumentation folgen.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Stellen Sie sicher, dass Sie VPC erstellen wählen, um eine neue Virtual Private Cloud (VPC) für Ihren Amazon-ECS-Cluster zu erstellen.	

Einrichten der Amazon-ECS-Aufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die IAM-Rolle für die Amazon-ECS-Aufgabe nausführung ein.	Erstellen Sie eine IAM-Rolle für die Amazon-ECS-Aufgabe nausführung mithilfe der `-AmazonECSTaskExecutionRolePolicy` verwalteten Richtlinie. Weitere Informationen dazu finden Sie unter IAM-Rolle für die Amazon-ECS-Aufgabenausführung in der Amazon-ECS-Dokumentation. Hinweis: Stellen Sie sicher, dass Sie den Amazon-Ressourcennamen (ARN) der IAM-Rolle aufzeichnen.	Systemadministrator, Entwickler
Hängen Sie die IAM-Richtlinie an die IAM-Rolle für die Amazon-ECS-Aufgabe nausführung an.	1. Erstellen Sie eine IAM-Richtlinie mithilfe des `firelens_policy.json` (angefügten) Richtlinienendokuments. Weitere Informationen dazu finden Sie unter Erstellen von Richtlinien auf der Registerk	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	arte JSON in der IAM-Dokumentation. 2. Fügen Sie diese Richtlini e an die IAM-Rolle für die Amazon-ECS-Aufgabe nausführung an, die Sie zuvor erstellt haben. Weitere Informationen dazu finden Sie unter Hinzufüge n von IAM-Richtlinien (AWS CLI) in der IAM-Dokum entation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Amazon-ECS-Aufgabendefinition ein.	1. Aktualisieren Sie die folgenden Abschnitte in der `Task.json` Beispielaufgabendefinition (angefügt): • Aktualisieren Sie `executionRoleArn` und `taskRoleArn` mit dem ARN der IAM-Rolle für die Aufgabenausführung • Aktualisieren Sie das Image in `containerDefinitions` mit dem benutzerdefinierten Fluent-Bit-Docker-Image, das Sie zuvor erstellt haben • Aktualisieren Sie das Image in `containerDefinitions` mit dem Namen Ihres Anwendungs-Images 2. Öffnen Sie die Amazon-ECS-Konsole, wählen Sie Aufgabendefinitionen, wählen Sie Neue Aufgabendefinition erstellen und wählen Sie dann auf der Seite Kompatibilitäten auswählen Fargate aus. 3. Wählen Sie Über Json konfigurieren, fügen Sie die	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aktualisierte `Task.json` Datei in den Textbereich ein und wählen Sie dann Speichern aus. 4. Erstellen Sie die Aufgabend efinition. Weitere Informationen dazu finden Sie unter Erstellen einer Aufgabendefinition in der Amazon-ECS-Dokumentation.	

Ausführen der Amazon-ECS-Aufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Amazon-ECS-Aufgabe aus.	Wählen Sie in der Amazon-ECS-Konsole Cluster aus, wählen Sie den Cluster aus, den Sie zuvor erstellt haben, und führen Sie dann die eigenständige Aufgabe aus. Weitere Informationen dazu finden Sie unter Ausführen einer eigenständigen Aufgabe in der Amazon-ECS-Dokumen tation.	Systemadministrator, Entwickler

Überprüfen der CloudWatch Protokolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokolle.	1. Öffnen Sie die - CloudWatch Konsole, wählen Sie Protokollgruppen und dann aus `/aws/ecs/containerinsights/{{cluster_ARN}}/firelens/application`. 2. Überprüfen Sie die Protokolle, insbesondere die vom benutzerdefinierten Parser hinzugefügten benutzerdefinierten Felder. 3. Verwenden Sie CloudWatch , um Protokolle basierend auf den benutzerdefinierten Feldern zu filtern.	Systemadministrator, Entwickler

Zugehörige Ressourcen

- Docker-Grundlagen für Amazon ECS
- Amazon ECS auf AWS Fargate
- Konfigurieren grundlegender Serviceparameter

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine Pipeline und ein AMI mit CodePipeline und HashiCorp Packer

Erstellt von Akash Kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: DevOps	Ziel: Amazon Machine Images (AMI)
R-Typ: Rehost	Arbeitslast: Alle anderen Workloads	Technologien: DevOps; Modernisierung; Web- und mobile Apps

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zum Erstellen einer Pipeline in der Amazon Web Services (AWS) -Cloud mithilfe von AWS CodePipeline und eines Amazon Machine Image (AMI) mithilfe von HashiCorp Packer. Das Muster basiert auf der Praxis der kontinuierlichen Integration, die das Erstellen und Testen von Code mit einem Git-basierten Versionskontrollsystem automatisiert. In diesem Muster erstellen und klonen Sie mithilfe von AWS ein Code-Repository CodeCommit. Erstellen Sie anschließend ein Projekt und konfigurieren Sie Ihren Quellcode mithilfe von AWS CodeBuild. Erstellen Sie abschließend ein AMI, das in Ihr Repository übernommen wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Linux-AMI zum Starten von Amazon Elastic Compute Cloud (Amazon EC2) -Instances
- HashiCorp Packer 0.12.3 oder höher
- CloudWatch Amazon-Veranstaltungen (optional)
- CloudWatch Amazon-Protokolle (optional)

Architektur

Das folgende Diagramm zeigt ein Beispiel für Anwendungscode, der die Erstellung eines AMI mithilfe der Architektur dieses Musters automatisiert.

Das Diagramm zeigt den folgenden Workflow:

1. Der Entwickler überträgt Codeänderungen in ein privates CodeCommit Git-Repository. Wird dann CodePipeline verwendet, CodeBuild um den Build zu initiieren und dem Amazon Simple Storage Service (Amazon S3) -Bucket neue Artefakte hinzuzufügen, die für die Bereitstellung bereit sind.
2. CodeBuild verwendet Packer, um das AMI auf der Grundlage einer JSON-Vorlage zu bündeln und zu verpacken. Wenn diese Option aktiviert ist, können CloudWatch Events die Pipeline automatisch starten, wenn eine Änderung im Quellcode auftritt.

Technologie-Stack

- CodeBuild
- CodeCommit
- CodePipeline
- CloudWatch Ereignisse (optional)

Tools

- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und produziert Artefakte, die sofort einsatzbereit sind.
- AWS CodeCommit — AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat in der AWS-Cloud speichern und verwalten können. CodeCommit macht es für Sie überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu verwalten oder sich Gedanken über die Skalierung der Infrastruktur zu machen.
- AWS CodePipeline — AWS CodePipeline ist ein Continuous Delivery Service, mit dem Sie die zur Veröffentlichung Ihrer Software erforderlichen Schritte modellieren, visualisieren und automatisieren können.

- HashiCorp Packer — HashiCorp Packer ist ein Open-Source-Tool zur Automatisierung der Erstellung identischer Maschinenimages aus einer einzigen Quellkonfiguration. Packer ist leichtgewichtig, läuft auf allen gängigen Betriebssystemen und erstellt Maschinenabbilder für mehrere Plattformen parallel.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `buildspec.yml`— Diese Datei wird verwendet CodeBuild , um ein Artefakt für die Bereitstellung zu erstellen und zu erstellen.
- `amazon-linux_packer-template.json`— Diese Datei verwendet Packer, um ein Amazon Linux AMI zu erstellen.

Epen

Richten Sie das Code-Repository ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Repository.	Erstellen Sie ein CodeCommit Repository.	AWS-Systemadministrator
Klonen Sie das Repository	Connect zum CodeCommit Repository her, indem Sie das Repository klonen.	App-Developer
Übertragen Sie den Quellcode in das Remote-Repository.	1. Erstellen Sie einen Commit, um die `amazon-linux_packer-template.json` Dateien `buildspec.yml` und zu Ihrem lokalen Repository hinzuzufügen. 2. Übertragen Sie den Commit von Ihrem lokalen Repositor	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	y in das CodeCommit Remote-Repository.	

Erstellen Sie ein CodeBuild Projekt für die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Build-Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeBuild AWS-Konsole und wählen Sie dann Create build project aus. 2. Geben Sie unter Projektname den Namen Ihres Projekts ein. 3. Wählen Sie als Quellanbieter AWS aus CodeCommit. 4. Wählen Sie für Repository das Repository aus, in dem Sie die Code-Pipeline erstellen möchten. 5. Wählen Sie für Umgebungs-Image die Option Verwaltetes Image oder Benutzerdefiniertes Image aus. 6. Wählen Sie für Operating system (Betriebssystem) die Option Ubuntu aus. 7. Wählen Sie für RunTime(s) die Option Standard.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie für Image (Abbild) die Option aws/codebuild/standard:4.0 aus. 9. Wählen Sie für Image-Version die Option Immer das neueste Image für diese Runtime-Version verwenden aus. 10. Wählen Sie für Umgebung die Option Linux aus. 11. Aktivieren Sie das Kontrollkästchen Privilegiert. 12. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 13. Wählen Sie für Buildspezifikationen die Option Buildspec-Datei verwenden oder Build-Befehle einfügen aus. 14. (Optional) Wählen Sie im Abschnitt Artefakte für Typ die Option Keine Artefakte aus. 15. (Empfohlen) Um Build-Output-Logs in Logs hochzuladen, wählen Sie CloudWatch Logs aus. CloudWatch 16. (Optional) Um Build-Ausgabeprotokolle auf Amazon S3 hochzuladen, aktiviere	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n Sie das Kontrollkästchen S3-Protokolle. 17. Wählen Sie Create build project (Build-Projekt erstellen) aus.	

Richten Sie die Pipeline ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pipeline-Name	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodePipeline AWS-Konsole und wählen Sie dann Create Pipeline aus. 2. Geben Sie unter Pipeline-Name einen Namen für die Pipeline ein. 3. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 4. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein. 5. Wählen Sie im Abschnitt Erweiterte Einstellungen für Artifact Store die Option Standardstandort aus, wenn Amazon S3 einen Bucket erstellen und die Artefakte im Bucket speichern soll.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um einen vorhandenen S3-Bucket zu verwenden , wählen Sie Benutzerd efinierter Speicherort. Wählen Sie Weiter aus. 6. Wählen Sie als Quellanbi eter AWS aus CodeCommi t. 7. Wählen Sie als Repositor y-Name das Repositor y aus, das Sie zuvor geklont haben. Wählen Sie als Branch-Name Ihren Quellcode-Branch aus. 8. Wählen Sie für Optionen zur Änderungserkennung Amazon CloudWatch Events (empfohlen), um die Pipeline zu starten, oder AWS CodePipel ine, um regelmäßig nach Änderungen zu suchen. Wählen Sie Weiter aus. 9. Wählen Sie als Build-Anb ieter AWS aus CodeBuild. 10. Wählen Sie als Projektna me das Build-Projekt aus, das Sie im Epic Ein CodeBuild Projekt für die Anwendung erstellen erstellt haben. 11. Wählen Sie Ihre Build-Opt ionen und dann Weiter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	12. Wählen Sie „Bereitstellungsphase überspringen“. 13. Wählen Sie Create pipeline (Pipeline erstellen) aus.	

Zugehörige Ressourcen

- Arbeiten mit Repositorys in AWS CodeCommit
- Arbeit mit Build-Projekten
- Arbeiten mit Pipelines in CodePipeline

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale EC2-Instances bereit mit CodePipeline

Erstellt von Akash Kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: DevOps	Ziel: Amazon EC2/On-Premise
R-Typ: Rehost	Technologien: DevOps; Modernisierung; Web- und mobile Apps	AWS-Dienste: AWS CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zum Erstellen einer Pipeline in der Amazon Web Services (AWS) -Cloud und zum Bereitstellen aktualisierter Artefakte für lokale Amazon Elastic Compute Cloud (Amazon EC2) -Instances in AWS. CodePipeline Das Muster basiert auf der Praxis der kontinuierlichen Integration. Diese Vorgehensweise automatisiert das Erstellen und Testen von Code mit einem Git-basierten Versionskontrollsystem. In diesem Muster erstellen und klonen Sie mithilfe von AWS ein Code-Repository CodeCommit. Anschließend erstellen Sie ein Projekt und konfigurieren Ihren Quellcode mithilfe von AWS CodeBuild. Schließlich erstellen Sie Ihre Anwendung und konfigurieren ihre Zielumgebung für lokale EC2-Instances mithilfe von AWS. CodeDeploy

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Benutzerdefinierte Tags zur Identifizierung von EC2-Instances während der Bereitstellung
- CodeDeploy Agent, auf EC2-Instances installiert
- Ihre erforderliche Runtime-Software, installiert auf EC2-Instances
- Amazon Corretto 8 für das Java Development Kit
- Apache Tomcat-Webserver, installiert
- CloudWatch Amazon-Veranstaltungen (optional)

- Ein key pair für die Anmeldung am Webserver (optional)
- Ein Apache Maven-Anwendungsprojekt für eine Webanwendung

Architektur

Das folgende Diagramm zeigt ein Beispiel für eine Java-Webanwendung, die mithilfe der Architektur dieses Musters auf lokalen EC2-Instances bereitgestellt wird.

Das Diagramm zeigt den folgenden Workflow:

1. Der Entwickler überträgt Codeänderungen in ein privates CodeCommit Git-Repository.
2. CodePipeline verwendet CodeBuild , um den Build zu initiieren und neue Artefakte hinzuzufügen, die für die Bereitstellung im Amazon Simple Storage Service (Amazon S3) -Bucket bereit sind.
3. CodePipeline verwendet den CodeDeploy Agenten, um alle Abhängigkeiten vorzuinstallieren, die für die Änderungen am Bereitstellungsartefakt erforderlich sind.
4. CodePipeline verwendet den CodeDeploy Agenten, um die Artefakte aus dem S3-Bucket auf Ziel-EC2-Instances bereitzustellen. Wenn diese Option aktiviert ist, können CloudWatch Events die Pipeline automatisch starten, wenn eine Änderung im Quellcode auftritt.

Technologie-Stack

- CodeBuild
- CodeCommit
- CodeDeploy
- CodePipeline
- CloudWatch Ereignisse (optional)

Tools

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und erzeugt Artefakte, die sofort einsatzbereit sind.

- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen auf Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `buildspec.yml`— Diese Datei spezifiziert die Aktionen, die CodeBuild erforderlich sind, um ein Artefakt für die Bereitstellung zu erstellen und zu erstellen.
- `appspec.yml`— Diese Datei spezifiziert die Aktionen, die CodeDeploy erforderlich sind, um eine Anwendung zu erstellen und eine Zielumgebung für lokale EC2-Instances zu konfigurieren.
- `install_dependencies.sh`— Diese Datei installiert Abhängigkeiten für den Apache Tomcat-Webserver.
- `start_server.sh`— Diese Datei startet den Apache Tomcat-Webserver.
- `stop_server.sh`— Diese Datei stoppt den Apache Tomcat-Webserver.

Epen

Richten Sie das Code-Repository ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Repository.	Erstellen Sie ein CodeCommit Repository.	AWS-Systemadministrator
Klonen Sie das Repository	Connect zum CodeCommit Repository her, indem Sie das Repository klonen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie den Quellcode in das Remote-Repository.	1. Erstellen Sie einen Commit, um die `appspec.yml` Dateien `buildspec.yml` und zu Ihrem lokalen Repository hinzuzufügen. 2. Übertragen Sie den Commit von Ihrem lokalen Repository in das CodeCommit Remote-Repository.	App-Developer

Erstellen Sie ein CodeBuild Projekt für die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Build-Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeBuild AWS-Konsole und wählen Sie dann Create build project aus. 2. Geben Sie unter Projektname den Namen Ihres Projekts ein. 3. Wählen Sie als Quellanbieter AWS aus CodeCommit. 4. Wählen Sie für Repository das Repository aus, in dem Sie die Code-Pipeline erstellen möchten. 5. Wählen Sie für Umgebungs-Image die Option Verwaltet	AWS-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	es Image oder Benutzerd efiniertes Image aus. 6. Wählen Sie für Operating system (Betriebssystem) die Option Amazon Linux 2 aus. 7. Wählen Sie für RunTime(s) die Option Standard. 8. Wählen Sie für Image aws/ codebuild/amazonlinux2- aarch64-standard:2.0 aus. 9. Wählen Sie für Image-Version die Option Immer das neueste Image für diese Runtime-Version verwenden aus. 10. Wählen Sie für Servicerolle die Option Neue Servicero lle oder Bestehende Servicerolle aus. 11. Wählen Sie für Buildspez ifikationen die Option Buildspec-Datei verwenden oder Build-Befehle einfügen aus. 12. (Optional) Wählen Sie Artefakt hinzufügen, um Artefakte zu konfigurieren. 13. (Optional) Um Build-Out put-Logs auf Amazon hochzuladen CloudWatc h, wählen Sie CloudWatch Logs.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	14. Wählen Sie Create build project (Build-Projekt erstellen) aus.	

Konfigurieren Sie die Bereitstellung von Artefakten für lokale EC2-Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendung.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeDeploy AWS-Konsole und wählen Sie dann Anwendung erstellen. 2. Geben Sie unter Anwendungsname einen Namen für Ihre Anwendung ein. 3. Wählen Sie für Compute-Plattform die Option EC2/On-Premises aus. 4. Wählen Sie Anwendung erstellen und dann Bereitstellungsgruppe erstellen aus. 5. Geben Sie unter Name der Bereitstellungsgruppe einen Namen ein. 6. Erstellen Sie eine Servicerolle für CodeDeploy. Hinweis: Die Servicerolle muss über Berechtigungen verfügen, um CodeDeploy	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zugriff auf Ihre Zielumgebung zu gewähren. 7. Wählen Sie unter Servicerolle die Servicerolle aus, die Sie in Schritt 6 erstellt haben. 8. Wählen Sie je nach Ihren Geschäftsanforderungen als Bereitstellungstyp entweder Direkt vor Ort oder Blau/Grün aus. 9. Wählen Sie für die Umgebungskonfiguration die Optionen aus, die Ihren Geschäftsanforderungen entsprechen. 10. (Optional) Erstellen Sie eine separate Zielgruppe für Ihren Load Balancer in der Amazon EC2 EC2-Konsole und kehren Sie dann zur Seite „Bereitstellungsgruppe erstellen“ der CodeDeploy AWS-Konsole zurück, um Ihren Load Balancer und Ihre Zielgruppe auszuwählen. 11. Wählen Si Create deployment group (Bereitstellungsgruppe erstellen).	

Richten Sie die Pipeline ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Pipeline.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodePipeline AWS-Konsole und wählen Sie dann Create Pipeline aus. 2. Geben Sie unter Pipeline-Name einen Namen für die Pipeline ein. 3. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 4. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein. 5. Wählen Sie im Abschnitt Erweiterte Einstellungen für Artifact Store die Option Standardstandort aus, wenn Amazon S3 einen Bucket erstellen und die Artefakte im Bucket speichern soll. Um einen vorhandenen S3-Bucket zu verwenden, wählen Sie Benutzerdefinierter Speicherort. Wählen Sie Weiter aus. 6. Wählen Sie als Quellanbieter AWS aus CodeCommit.	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie als Repository-Name das Repository aus, das Sie zuvor geklont haben. Wählen Sie als Branch-Name Ihren Quellcode-Branch aus. 8. Wählen Sie für Optionen zur Änderungserkennung Amazon CloudWatch Events (empfohlen) oder AWS CodePipeline. Wählen Sie Weiter aus. 9. Wählen Sie als Build-Anbieter AWS aus CodeBuild. 10. Wählen Sie als Projektname das Build-Projekt aus, das Sie im Abschnitt CodeBuild Projekt für die Anwendung erstellen dieses Musters erstellt haben. 11. Wählen Sie Ihre Build-Optionen und dann Weiter. 12. Wählen Sie für Deploy Provider die Option AWS aus CodeDeploy. 13. Wählen Sie einen Anwendungsnamen und eine Bereitstellungsgruppe aus und klicken Sie dann auf Weiter. 14. Wählen Sie Create pipeline (Pipeline erstellen) aus.	

Zugehörige Ressourcen

- Arbeiten mit Repositorys in AWS CodeCommit
- Arbeit mit Build-Projekten
- Arbeiten mit Anwendungen in CodeDeploy
- Arbeiten mit Pipelines in CodePipeline

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte

Erstellt vonl Raj Jayarajan (AWS), Amarnath Reddy (AWS), MAHESH RAGHUNANDANAN (AWS) und Vijesh Vijayakumaran Nair (AWS)

Code-Repository: automated-ci-pipeline-creation	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur; Serverless; Cloudnativ
Workload: Alle anderen Workloads	AWS-Services: AWS CodeBuild; AWS CodePipeline; AWS Lambda ; AWS Step Functions ; AWS CodeCommit	

Übersicht

Dieses Muster zeigt, wie dynamische Continuous Integration (CI)-Pipelines für Java- und Python-Projekte mithilfe von AWS-Entwicklertools automatisch erstellt werden.

Da Technologie-Stacks diversifizieren und Entwicklungsaktivitäten zunehmen, kann es schwierig werden, CI-Pipelines zu erstellen und zu verwalten, die in einer Organisation konsistent sind. Durch die Automatisierung des Prozesses in AWS Step Functions können Sie sicherstellen, dass Ihre CI-Pipelines in ihrer Nutzung und ihrem Ansatz konsistent sind.

Um die Erstellung dynamischer CI-Pipelines zu automatisieren, verwendet dieses Muster die folgenden Variableneingaben:

- Programmiersprache (nur Java oder Python)
- Pipeline-Name
- Erforderliche Pipeline-Phasen

Hinweis: Step Functions orchestriert die Pipeline-Erstellung mithilfe mehrerer AWS-Services. Weitere Informationen zu den in dieser Lösung verwendeten AWS-Services finden Sie im Abschnitt Tools dieses Musters.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon S3-Bucket in derselben AWS-Region, in der diese Lösung bereitgestellt wird
- Ein AWS Identity and Access Management (IAM)-Prinzipal, der über die erforderlichen AWS-CloudFormation Berechtigungen verfügt, um die für diese Lösung erforderlichen Ressourcen zu erstellen

Einschränkungen

- Dieses Muster unterstützt nur Java- und Python-Projekte.
- Die in diesem Muster bereitgestellten IAM-Rollen folgen dem Prinzip der geringsten Berechtigung. Die Berechtigungen der IAM-Rollen müssen basierend auf den spezifischen Ressourcen aktualisiert werden, die Ihre CI-Pipeline erstellen muss.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Systems Manager
- AWS Step Functions
- AWS Lambda
- Amazon DynamoDB

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow zum automatischen Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte mithilfe von AWS-Entwicklertools.

Das Diagramm zeigt den folgenden Workflow:

1. Ein AWS-Benutzer stellt die Eingabeparameter für die CI-Pipeline-Erstellung im JSON-Format bereit. Diese Eingabe startet einen Step Functions-Workflow (Zustandsautomat), der mithilfe von AWS-Entwicklertools eine CI-Pipeline erstellt.
2. Eine Lambda-Funktion liest einen Ordner mit dem Namen input-reference , der in einem Amazon S3-Bucket gespeichert ist, und generiert dann eine buildspec.yml-Datei. Diese generierte Datei definiert die CI-Pipeline-Phasen und wird wieder in demselben Amazon S3-Bucket gespeichert, in dem die Parameterreferenzen gespeichert sind.
3. Step Functions überprüft die Abhängigkeiten des CI-Pipeline-Erstellungs-Workflows auf Änderungen und aktualisiert den Abhängigkeiten-Stack nach Bedarf.
4. Step Functions erstellt die CI-Pipeline-Ressourcen in einem CloudFormation Stack, einschließlich eines CodeCommit Repositorys, CodeBuild Projekts und einer CodePipeline Pipeline.
5. Der CloudFormation Stack kopiert den Beispielquellcode für den ausgewählten Technologie-Stack (Java oder Python) und die Datei buildspec.yml in das CodeCommit Repository.
6. Details zur CI-Pipeline-Laufzeit werden in einer DynamoDB-Tabelle gespeichert.

Automatisierung und Skalierung

- Dieses Muster ist nur für die Verwendung in einer einzelnen Entwicklungsumgebung vorgesehen. Konfigurationsänderungen sind für die Verwendung in mehreren Entwicklungsumgebungen erforderlich.
- Um Unterstützung für mehr als einen CloudFormation Stack hinzuzufügen, können Sie zusätzliche CloudFormation Vorlagen erstellen. Weitere Informationen finden Sie unter Erste Schritte mit AWS CloudFormation in der - CloudFormation Dokumentation.

Tools

Tools

- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Systems Manager Parameter Store bietet eine sichere, hierarchische Speicherung für die Verwaltung von Konfigurationsdaten und Secrets.

Code

Der Code für dieses Muster ist im GitHub automated-ci-pipeline-creationRepository verfügbar. Das Repository enthält die CloudFormation Vorlagen, die zum Erstellen der in diesem Muster beschriebenen Zielarchitektur erforderlich sind.

Bewährte Methoden

- Geben Sie keine Anmeldeinformationen (Geheimnisse) wie Token oder Passwörter direkt in CloudFormation Vorlagen oder Step-Functions-Aktionskonfigurationen ein. Wenn Sie dies tun, werden die Informationen in den DynamoDB-Protokollen angezeigt. Verwenden Sie stattdessen AWS Secrets Manager, um Secrets einzurichten und zu speichern. Verweisen Sie dann nach Bedarf auf die in Secrets Manager gespeicherten Secrets in den CloudFormation Vorlagen und Step-Functions-Aktionskonfigurationen. Weitere Informationen finden Sie unter Was ist AWS Secrets Manager? in der Secrets-Manager-Dokumentation.
- Konfigurieren Sie die serverseitige Verschlüsselung für CodePipeline Artefakte, die in Amazon S3 gespeichert sind. Weitere Informationen finden Sie unter Konfigurieren der serverseitigen Verschlüsselung für Artefakte, die in Amazon S3 für gespeichert sind CodePipeline in der - CodePipeline Dokumentation.
- Wenden Sie bei der Konfiguration von IAM-Rollen die geringsten Berechtigungen an. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.
- Stellen Sie sicher, dass Ihr Amazon S3-Bucket nicht öffentlich zugänglich ist. Weitere Informationen finden Sie unter Konfigurieren der Einstellung zum Blockieren des öffentlichen Zugriffs für Ihre S3-Buckets in der Amazon S3-Dokumentation.
- Stellen Sie sicher, dass Sie das Versioning für Ihren Amazon S3-Bucket aktivieren. Weitere Informationen finden Sie unter Verwenden der Versionsverwaltung in S3-Buckets in der Amazon S3-Dokumentation.
- Verwenden Sie IAM Access Analyzer bei der Konfiguration von IAM-Richtlinien. Das Tool bietet umsetzbare Empfehlungen, mit denen Sie sichere und funktionale IAM-Richtlinien erstellen können. Weitere Informationen finden Sie unter Verwenden von AWS Identity and Access Management Access Analyzer in der IAM-Dokumentation.
- Definieren Sie nach Möglichkeit bestimmte Zugriffsbedingungen bei der Konfiguration von IAM-Richtlinien.
- Aktivieren Sie die Amazon- CloudWatch Protokollierung für Überwachungs- und Prüfungszwecke. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch Logs? in der - CloudWatch Dokumentation.

Sekunden

Konfigurieren der Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-S3-Bucket.	Erstellen Sie einen Amazon S3-Bucket (oder verwenden Sie einen vorhandenen Bucket), um die erforderlichen CloudFormation Vorlagen, Quellcode und Eingabedateien für die Lösung zu speichern. Weitere Informationen finden Sie unter Schritt 1: Erstellen Ihres ersten S3-Buckets in der Amazon S3-Dokumentation. Hinweis: Der Amazon S3-Bucket muss sich in derselben AWS-Region befinden, in der Sie die Lösung bereitstellen.	AWS DevOps
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub automated-ci-pipeline-creation Repository, indem Sie den folgenden Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/automated-ci-pipeline-creation.git` Weitere Informationen finden Sie unter Klonen eines	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repositorys in der - GitHub Dokumentation.	
Laden Sie den Ordner Lösungsvorlagen aus dem geklonten GitHub Repository in Ihren Amazon S3-Bucket hoch.	Kopieren Sie den Inhalt aus dem geklonten Solution-Templates-Ordner und laden Sie ihn in den Amazon S3-Bucket hoch, den Sie erstellt haben. Weitere Informationen finden Sie unter Hochladen von Objekten in der Amazon S3-Dokumentation. Hinweis: Stellen Sie sicher, dass Sie nur den Inhalt des Ordners Solution-Templates hochladen. Sie können die Dateien nur auf Stammebene des Amazon S3-Buckets hochladen.	AWS DevOps

Bereitstellen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CloudFormation Stack, um die Lösung mithilfe der Datei template.yml im geklonten GitHub Repository bereitzustellen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS- CloudFormation Konsole . 2. Wählen Sie Stack erstellen aus. Eine Dropdown-Liste wird angezeigt.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie in der Dropdown-Liste Mit neuen Ressourcen (Standard) aus. Die Seite Stack erstellen wird geöffnet. 4. Aktivieren Sie im Abschnitt Vorlage angeben das Kontrollkästchen neben Vorlagendatei hochladen. 5. Wählen Sie Datei auswählen aus. Navigieren Sie dann zum Stammordner des geklonten GitHub Repositorys und wählen Sie die Datei template.yml aus. Wählen Sie dann Open (Öffnen) aus. 6. Wählen Sie Weiter aus. Die Seite Stack-Details angeben wird geöffnet. 7. Geben Sie im Abschnitt Parameter die folgenden Parameter an: • Geben Sie für S3TemplateBucketName den Namen des Amazon S3-Buckets ein, den Sie zuvor erstellt haben, der den Quellcode und die Referenzen für diese Lösung enthält. Stellen Sie sicher, dass der Bucket-Namensparam	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eter in Kleinbuchstaben geschrieben ist. • Geben Sie für DynamoDBTable einen Namen für die DynamoDB-Tabelle ein, die der CloudFormation Stack erstellt. • StateMach ineNameGeben Sie für einen Namen für den Step Functions-Zustands automaten ein, den der CloudFormation Stack erstellt. 8. Wählen Sie Weiter aus. Die Seite Stack-Optionen konfigurieren wird geöffnet. 9. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfiguri eren) Next (Weiter) aus. Ändern Sie keinen der Standardwerte. Die Seite Überprüfen wird geöffnet. 10. Überprüfen Sie die Einstellu ngen für die Stack-Ers tellung. Wählen Sie dann Stack erstellen aus, um Ihren Stack zu starten. Hinweis: Während Ihr Stack erstellt wird, wird er auf der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Seite Stacks mit dem Status CREATE_IN_PROGRESS aufgeführt. Stellen Sie sicher, dass Sie warten, bis sich der Status des Stacks in CREATE_COMPLETE ändert, bevor Sie die verbleibenden Schritte in diesem Muster ausführen.	

Testen der Einrichtung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die von Ihnen erstellte Schrittfunktion aus.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die Step Functions-Konsole. 2. Öffnen Sie die von Ihnen erstellte Schrittfunktion. 3. Wählen Sie Start execution (Ausführung starten) aus. Geben Sie dann Ihre Eingabewerte für den Workflow im JSON-Form at ein (siehe die folgenden Beispieleingaben). 4. Wählen Sie Start execution (Ausführung starten) aus. JSON-Formatierung `{ "details": {`	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
    "tech_stack":
 "Name of the Tech Stack
 (python/java)",
    "project_name":
 "Name of the Project
 that you want to create
 with",
    "pre_build":
 "Choose the step if
 it required in the
 buildspec.yml file
 i.e., yes/no",
    "build": "Choose the
 step if it required in
 the buildspec.yml file
 i.e., yes/no",
    "post_build":
 "Choose the step if
 it required in the
 buildspec.yml file
 i.e., yes/no",
    "reports": "Choose
 the step if it required
 in the buildspec.yml
 file i.e., yes/no",
  }
}
```

Java-JSON-Eingabebeispiel

```
{
  "details": {
    "tech_stack":
 "java",
    "project_name":
 "pipeline-java-pjt",
    "pre_build": "yes",
    "build": "yes",
    "post_build":
 "yes",
    "reports": "yes"
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
  }
}
```

Python-JSON-Eingabebeispiel

```
{
  "details": {
    "tech_stack":
 "python",
    "project_name":
 "pipeline-python-p
jt",
    "pre_build": "yes",
    "build": "yes",
    "post_build":
 "yes",
    "reports": "yes"
  }
}
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass das CodeCommit Repository für die CI-Pipeline erstellt wurde.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodeCommit Konsole . 2. Überprüfen Sie auf der Seite Repositorys, ob der Name des von Ihnen erstellten CodeCommit Repositorys in der Liste der Repositorys angezeigt wird. Dem Namen des Repositorys wird Folgendes angehängt: pipeline-java-pjt-Repo 3. Öffnen Sie das CodeCommit Repository und überprüfen Sie, ob der Beispielquellcode zusammen mit buildspec.yml-Dateien an den Hauptzweig übertragen wird.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CodeBuild Projektressourcen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodeBuild Konsole . 2. Überprüfen Sie auf der Seite Projekte erstellen , ob der Name des von Ihnen erstellten CodeBuild Projekts in der Liste der Projekte angezeigt wird. Dem Namen des Projekts wird Folgendes angehängt: pipeline-java-pjt-Build 3. Wählen Sie den Namen Ihres CodeBuild Projekts aus, um das Projekt zu öffnen. Überprüfen und validieren Sie dann die folgenden Konfigurationen: • Projektkonfiguration • Quelle • Umgebung • Build-Spezifikation • Batch-Konfiguration • Artefakte	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die CodePipeline Stufen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodePipeline Konsole . 2. Überprüfen Sie auf der Seite Pipelines, ob der Name der Pipeline, die Sie erstellt haben, in der Liste der Pipelines angezeigt wird. Dem Namen der Pipeline wird Folgendes angehängt: pipeline-java-pjt-Pipeline 3. Wählen Sie den Namen Ihrer Pipeline aus, um die Pipeline zu öffnen. Überprüfen und validieren Sie dann jede Phase der Pipeline, einschließlich Commit und Deploy .	AWS DevOps
Bestätigen Sie, dass die CI-Pipeline erfolgreich ausgeführt wurde.	1. Wählen Sie in der CodePipeline Konsole auf der Seite Pipelines den Namen Ihrer Pipeline aus, um den Status der Pipeline anzuzeigen. 2. Stellen Sie sicher, dass jede Phase der Pipeline den Status Erfolgreich hat.	AWS DevOps

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Ressourcen-Stack in CloudFormation.	Löschen Sie den Ressource n-Stack der CI-Pipeline in CloudFormation. Weitere Informationen finden Sie unter Löschen eines Stacks in der AWS-CloudFormation Konsole in der - CloudFormation Dokumentation. Hinweis: Stellen Sie sicher, dass Sie den Stack mit dem Namen <project_name>-stack löschen.	AWS DevOps
Löschen Sie die Abhängigk eiten der CI-Pipeline in Amazon S3 und CloudForm ation.	1. Leeren Sie den Amazon S3-Bucket mit dem Namen DeploymentArtifactBucket. Weitere Informationen finden Sie unter Leeren eines Buckets in der Amazon S3-Dokumentation. 2. Löschen Sie den Abhängigk eits-Stack der CI-Pipeline in CloudFormation. Weitere Informationen finden Sie unter Löschen eines Stacks in der AWS- CloudForm ation Konsole in der - CloudFormation Dokumenta tion.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Stellen Sie sicher, dass Sie den Stack mit dem Namen löschenpipeline-creation-dependencies-stack.	
Löschen Sie den Amazon S3-Vorlagen-Bucket.	Löschen Sie den Amazon-S3 -Bucket, den Sie im Abschnitt Voraussetzungen konfiguri eren dieses Musters erstellt haben, in dem die Vorlagen für diese Lösung gespeichert werden. Weitere Informationen finden Sie unter Löschen eines Buckets in der Amazon S3-Dokumentation.	AWS DevOps

Zugehörige Ressourcen

- Erstellen eines Step Functions-Zustandsautomaten, der Lambda verwendet (Dokumentation zu AWS Step Functions)
- AWS Step Functions WorkFlow Studio (Dokumentation zu AWS Step Functions)
- DevOps und AWS
- Wie CloudFormation funktioniert AWS? (AWS- CloudFormation Dokumentation)
- Vervollständigen von CI/CD mit AWS CodeCommit, AWS CodeDeploy, CodeBuildAWS und AWS CodePipeline (AWS-Blogbeitrag)
- IAM- und AWS STS-Kontingente, Namensanforderungen und Zeichenlimits (IAM-Dokumentation)

Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit

Erstellt von Dhrubajyoti Mukherjee (AWS) und Jean-Francois Landreau (AWS)

Quellcode-Repository: Stellen Sie CloudWatch Synthetics Canaries mit Terraform bereit	Umgebung: Produktion	Technologien: DevOps; Unternehmensproduktivität; Softwareentwicklung und Tests; Infrastruktur; Web- und mobile Apps
AWS-Services: Amazon CloudWatch; Amazon S3; Amazon SNS; Amazon VPC; AWS Identity and Access Management		

Übersicht

Es ist wichtig, den Zustand eines Systems aus Kundensicht zu überprüfen und sicherzustellen, dass Kunden eine Verbindung herstellen können. Dies ist schwieriger, wenn die Kunden den Endpunkt nicht ständig anrufen. Amazon CloudWatch Synthetics unterstützt die Erstellung von Canaries, mit denen sowohl öffentliche als auch private Endgeräte getestet werden können. Durch die Verwendung von Canaries können Sie den Status eines Systems ermitteln, auch wenn es nicht verwendet wird. Diese Kanarien sind entweder Node.js Puppeteer-Skripte oder Python Selenium-Skripte.

Dieses Muster beschreibt, wie HashiCorp Terraform verwendet wird, um Canaries bereitzustellen, die private Endpunkte testen. Es bettet ein Puppeteer-Skript ein, das testet, ob eine URL zurückkehrt. `200-OK` Das Terraform-Skript kann dann in das Skript integriert werden, das den privaten Endpunkt bereitstellt. Sie können die Lösung auch ändern, um öffentliche Endpunkte zu überwachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto mit einer Virtual Private Cloud (VPC) und privaten Subnetzen
- Die URL des Endpunkts, der von den privaten Subnetzen aus erreicht werden kann
- Terraform ist in der Bereitstellungsumgebung installiert

Einschränkungen

Die aktuelle Lösung funktioniert für die folgenden CloudWatch Synthetics-Laufzeitversionen:

- syn-nodejs-puppeteer-3.4
- syn-nodejs-puppeteer-3,5
- syn-nodejs-puppeteer-3,6
- syn-nodejs-puppeteer-3,7

Wenn neue Runtime-Versionen veröffentlicht werden, müssen Sie möglicherweise die aktuelle Lösung aktualisieren. Sie müssen die Lösung auch ändern, um mit den Sicherheitsupdates Schritt zu halten.

Produktversionen

- Terraform 1.3.0

Architektur

Amazon CloudWatch Synthetics basiert auf CloudWatch Lambda und Amazon Simple Storage Service (Amazon S3). Amazon CloudWatch bietet einen Assistenten zum Erstellen der Canaries und ein Dashboard, das den Status der Canaries Runs anzeigt. Die Lambda-Funktion führt das Skript aus. Amazon S3 speichert die Protokolle und Screenshots der Canary Runs.

Dieses Muster simuliert einen privaten Endpunkt über eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die in den Zielsubnetzen bereitgestellt wird. Die Lambda-Funktion erfordert elastische Netzwerkschnittstellen in der VPC, in der der private Endpunkt bereitgestellt wird.

Das Diagramm zeigt Folgendes:

1. Der Synthetics Canary initiiert die kanarische Lambda-Funktion.
2. Die kanarische Lambda-Funktion stellt eine Verbindung zur elastic network interface her.
3. Die Canary-Lambda-Funktion überwacht den Status des Endpunkts.
4. Der Synthetics Canary überträgt Laufdaten und CloudWatch Metriken in den S3-Bucket.
5. Auf der Grundlage der Metriken wird ein CloudWatch Alarm ausgelöst.
6. Der CloudWatch Alarm leitet das Thema Amazon Simple Notification Service (Amazon SNS) ein.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS. Dieses Muster verwendet VPC-Endpunkte und elastische Netzwerkschnittstellen.

Andere Dienste

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastruktur als Code (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. Dieses Muster verwendet Terraform, um die Infrastruktur bereitzustellen.
- Puppeteer ist eine Node.js Bibliothek. Die CloudWatch Synthetics-Laufzeit verwendet das Puppeteer-Framework.

Code

Die Lösung ist im Cloud-Repository verfügbar. GitHub watch-synthetics-canary-terraform Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

Epen

Implementieren Sie die Lösung für die Überwachung einer privaten URL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Anforderungen für die Überwachung der privaten URL.	Erfassen Sie die vollständige URL-Definition: Domäne, Parameter und Header. Verwenden Sie VPC-Endpunkte CloudWatch, um privat mit Amazon S3 und Amazon zu kommunizieren. Beachten Sie, wie der Endpunkt auf die VPC und die Subnetze zugreifen kann. Beachten Sie die Häufigkeit von Canary Runs.	Cloud-Architekt, Netzwerkadministrator
Ändern Sie die bestehende Lösung, um die private URL zu überwachen.	Ändern Sie die `terraform.tfvars` Datei: • `name`— Der Name deines Kanarienvogels. • `runtime_version` — Die Runtime-Version des Canary. Wir empfehlen die Verwendung von syn-nodejs-puppeteer -3.7. • `take_screenshot` — Ob ein Screenshot aufgenommen werden soll.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `api_hostname` — Der Hostname des Endpunkts, der überwacht wird. • `api_path`— Der Pfad des überwachten Endpunkts. • `vpc_id`— Die VPC-ID, die von der Canary-Lambda-Funktion verwendet wird. • `subnet_ids` — Die Subnetz-IDs, die von der Canary-Lambda-Funktion verwendet werden. • `frequency` — Die Lauffrequenz des Canary in Minuten. • `alert_sns_topic` — Das SNS-Thema, an das die CloudWatch Alarmbena chrichtigung gesendet wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Lösung bereit und betreiben Sie sie.	Gehen Sie wie folgt vor, um die Lösung bereitzustellen:
	1. Initialisieren Sie Terraform aus dem `cloudwatch-synthetics-canary-terraform` Verzeichnis in Ihrer Entwicklungsumgebung.
	`terraform init`
	2. Planen und überprüfen Sie die Änderungen.
	`terraform plan`
	3. Stellen Sie die Lösung bereit.
	`terraform apply`
		Cloud-Architekt, DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Das Löschen der bereitgestellten Ressourcen bleibt hängen.	Löschen Sie die Canary-Lambda-Funktion, die entsprechende elastic network interface und die Sicherheitsgruppe manuell in dieser Reihenfolge.

Zugehörige Ressourcen

- Synthetische Überwachung verwenden

- Überwachen Sie API Gateway Gateway-Endpunkte mit Amazon CloudWatch Synthetics (Blogbeitrag)

Zusätzliche Informationen

Artefakte aus dem Repository

Die Repository-Artefakte haben die folgende Struktur.

```
.
### README.md
### main.tf
### modules
#   ### canary
#   ### canary-infra
### terraform.tfvars
### tf.plan
### variable.tf
```

Die `main.tf` Datei enthält das Kernmodul und stellt zwei Untermodule bereit:

- `canary-infra`stellt die für die Kanaren benötigte Infrastruktur bereit.
- `canary`setzt die Kanarischen Inseln ein.

Die Eingabeparameter für die Lösung befinden sich in der `terraform.tfvars` Datei. Sie können das folgende Codebeispiel verwenden, um einen Canary zu erstellen.

```
module "canary" {
    source = "./modules/canary"
    name   = var.name
    runtime_version = var.runtime_version
    take_screenshot = var.take_screenshot
    api_hostname = var.api_hostname
    api_path = var.api_path
    reports-bucket = module.canary_infra.reports-bucket
    role = module.canary_infra.role
    security_group_id = module.canary_infra.security_group_id
    subnet_ids = var.subnet_ids
    frequency = var.frequency
    alert_sns_topic = var.alert_sns_topic
```

```
}
```

Es folgt die entsprechende .var-Datei.

```
name   = "my-canary"
runtime_version = "syn-nodejs-puppeteer-3.7"
take_screenshot = false
api_hostname = "mydomain.internal"
api_path = "/path?param=value"
vpc_id = "vpc_id"
subnet_ids = ["subnet_id1"]
frequency = 5
alert_sns_topic = "arn:aws:sns:eu-central-1:111111111111:yyyyy"
```

Die Lösung aufräumen

Wenn Sie dies in einer Entwicklungsumgebung testen, können Sie die Lösung bereinigen, um Kosten zu vermeiden.

1. Navigieren Sie in der AWS-Managementkonsole zur Amazon S3 S3-Konsole. Leeren Sie den Amazon S3 S3-Bucket, den die Lösung erstellt hat. Stellen Sie sicher, dass Sie bei Bedarf eine Sicherungskopie der Daten erstellen.
2. Führen Sie in Ihrer Entwicklungsumgebung den `destroy` Befehl aus dem `cloudwatch-synthetics-canary-terraform` Verzeichnis aus.

   ```
   terraform destroy
   ```

Bereitstellen einer CI/CD-Pipeline für Java-Microservices auf Amazon ECS

Erstellt von Vijay Thompson (AWS) und Sankar Sangubotla (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Container und Microservices	AWS-Services: AWS CodeBuild; Amazon EC2 Container Registry ; Amazon ECS; AWS Fargate; AWS CodePipeline

Übersicht

Dieses Muster führt Sie durch die Schritte zur Bereitstellung einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) für Java-Microservices auf einem vorhandenen Amazon Elastic Container Service (Amazon ECS)-Cluster mithilfe von AWS CodeBuild. Wenn der Entwickler die Änderungen festschreibt, wird die CI/CD-Pipeline initiiert und der Build-Prozess beginnt in CodeBuild. Wenn der Build abgeschlossen ist, wird das Artefakt an Amazon Elastic Container Registry (Amazon ECR) übertragen und der neueste Build von Amazon ECR wird übernommen und an den Amazon-ECS-Service übertragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene Java-Microservices-Anwendung, die auf Amazon ECS ausgeführt wird
- Vertrautheit mit AWS CodeBuild und AWS CodePipeline

Architektur

Quelltechnologie-Stack

- Java-Microservices, die auf Amazon ECS ausgeführt werden
- Code-Repository in Amazon ECR
- AWS Fargate

Quellarchitektur

Zieltechnologie-Stack

- Amazon ECR
- Amazon ECS
- AWS Fargate
- AWS CodePipeline
- AWS CodeBuild

Zielarchitektur

Automatisierung und Skalierung

CodeBuild `buildspec.yml`-Datei:

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws --version
      - $(aws ecr get-login --region $AWS_DEFAULT_REGION --no-include-email)
      - REPOSITORY_URI=$AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/
$IMAGE_REPO
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=build-$(echo $CODEBUILD_BUILD_ID | awk -F":" '{print $2}')
  build:
    commands:
      - echo Build started on `date`
      - echo building the Jar file
      - mvn clean install
      - echo Building the Docker image...
      - docker build -t $REPOSITORY_URI:$BUILD_TAG .
      - docker tag $REPOSITORY_URI:$BUILD_TAG $REPOSITORY_URI:$IMAGE_TAG
```

```
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $REPOSITORY_URI:$BUILD_TAG
      - docker push $REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      - printf '[{"name":"%s","imageUri":"%s"}]' $DOCKER_CONTAINER_NAME
 $REPOSITORY_URI:$IMAGE_TAG > imagedefinitions.json
      - cat imagedefinitions.json
artifacts:
    files:
     - imagedefinitions.json
     - target/DockerDemo.jar
```

Tools

AWS-Services

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können. AWS CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in der Warteschlange verbleiben.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen. Sie können AWS CodePipeline in Services von Drittanbietern wie integrieren GitHuboder AWS-Services wie AWS CodeCommit oder Amazon ECR verwenden.
- Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Registrierung, mit der Entwickler Docker-Container-Images einfach speichern, verwalten und bereitstellen können. Amazon ECR ist in Amazon ECS integriert, um Ihren development-to-production Workflow zu vereinfachen. Amazon ECR hostet Ihre Images in einer hochverfügbaren und skalierbaren Architektur, sodass Sie Container für Ihre Anwendungen zuverlässig bereitstellen können. Die Integration mit AWS Identity and Access Management (IAM) ermöglicht die Steuerung jedes Repositorys auf Ressourcenebene.
- Amazon Elastic Container Service (Amazon ECS) hoch skalierbarer, leistungsstarker Container-Orchestrierungsservice, der Docker-Container unterstützt und es Ihnen ermöglicht, containerisierte Anwendungen einfach auf AWS auszuführen und zu skalieren. Amazon ECS macht es überflüssig, Ihre eigene Container-Orchestrierungssoftware zu installieren und zu betreiben, einen Cluster

virtueller Maschinen zu verwalten und zu skalieren oder Container auf diesen virtuellen Maschinen zu planen.

- AWS Fargate ist eine Rechen-Engine für Amazon ECS, mit der Sie Container ausführen können, ohne Server oder Cluster verwalten zu müssen. Mit AWS Fargate müssen Sie keine Cluster virtueller Maschinen mehr bereitstellen, konfigurieren und skalieren, um Container auszuführen. Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Cluster skaliert werden oder das Cluster-Packing optimiert werden.

Andere Tools

- Docker ist eine Plattform, mit der Sie Anwendungen in Paketen erstellen, testen und bereitstellen können, die als Container bezeichnet werden.
- Git ist ein verteiltes Versionskontrollsystem zur Verfolgung von Änderungen am Quellcode während der Softwareentwicklung. Es ist für die Koordination der Arbeit zwischen Programmierern konzipiert, kann aber verwendet werden, um Änderungen in jeder Reihe von Dateien zu verfolgen. Zu seinen Zielen gehören Geschwindigkeit, Datenintegrität und Unterstützung verteilter, nicht linearer Workflows. Sie können AWS auch CodeCommit als Alternative zu Git verwenden.

Polen

Einrichten des Build-Projekts in AWS CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeBuild Build-Projekt.	Erstellen Sie in der AWS-CodeBuild Konsole ein Build-Projekt und geben Sie dessen Namen an.	App-Entwickler, AWS-Syste madministrator
Wählen Sie die Quelle aus.	Dieses Muster verwendet Git für das Code-Repository. Wählen Sie daher GitHub aus der Liste der verfügbaren Optionen aus. Wählen Sie ein öffentliches Repository oder aus Ihrem GitHub Konto aus.	App-Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein Repository aus.	Wählen Sie das Repository aus, aus dem Sie den Code erstellen möchten.	App-Entwickler, AWS-Systemadministrator
Wählen Sie die Umgebung aus.	Sie können mit Docker aus einer Liste verwalteter Images auswählen oder ein benutzerdefiniertes Image auswählen. Dieses Muster verwendet das folgende verwaltete Image: • Amazon Linux 2 • Laufzeit: Standard • Image-Version 1.0	App-Entwickler, AWS-Systemadministrator
Wählen Sie eine Servicerolle aus.	Sie können eine Servicerolle erstellen oder aus einer Liste vorhandener Rollen auswählen.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hinzufügen von Umgebungsvariablen	Konfigurieren Sie im Abschnitt Zusätzliche Konfiguration die folgenden Umgebungsvariablen: • AWS_DEFAULT_REGION für die Standard-AWS-Region • AWS_ACCOUNT_ID für die Benutzerkontonummer • IMAGE_REPO für das private Amazon-ECR-Repository • BUILD_TAG für die Version des Builds (der neueste Build ist der Wert für diese Variable) • DOCKER_CONTAINER_NAME für den Namen des Containers in der Aufgabe Diese Variablen sind Platzhalter in der `buildspec.yml` Datei und werden durch ihre jeweiligen Werte ersetzt.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine buildspec-Datei.	Sie können eine `buildspec.yml` Datei am selben Speicherort wie erstellen `pom.xml` und die Konfiguration hinzufügen, die in diesem Muster bereitgestellt wird, oder den Online-Buildspec-Editor verwenden und die Konfiguration hinzufügen. Konfigurieren Sie die Umgebungsvariablen mit den entsprechenden Werten, indem Sie die angegebenen Schritte ausführen.	App-Entwickler, AWS-Systemadministrator
Konfigurieren Sie das Projekt für Artefakte.	(Optional) Konfigurieren Sie das Build-Projekt bei Bedarf für Artefakte.	App-Entwickler, AWS-Systemadministrator
Konfigurieren Sie Amazon CloudWatch Logs.	(Optional) Konfigurieren Sie Amazon CloudWatch Logs für das Build-Projekt, falls erforderlich. Dieser Schritt ist optional, wird aber empfohlen.	App-Entwickler, AWS-Systemadministrator
Konfigurieren Sie Amazon S3-Protokolle.	(Optional) Konfigurieren Sie Amazon Simple Storage Service (Amazon S3)-Protokolle für das Build-Projekt, wenn Sie die Protokolle speichern möchten.	App-Entwickler, AWS-Systemadministrator

Konfigurieren der Pipeline in AWS CodePipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline.	Erstellen Sie in der AWS-CodePipeline Konsole eine Pipeline und geben Sie deren Namen an. Weitere Informationen zum Erstellen einer Pipeline finden Sie in der AWS- CodePipeline Dokumentation.	App-Entwickler, AWS-Systemadministrator
Wählen Sie eine Servicerolle aus.	Erstellen Sie eine Servicerolle oder wählen Sie aus der Liste der vorhandenen Servicerollen aus. Wenn Sie eine Servicerolle erstellen, geben Sie einen Namen für die Rolle ein und wählen Sie die Option für aus, um die Rolle CodePipeline zu erstellen.	App-Entwickler, AWS-Systemadministrator
Wählen Sie einen Artefaktspeicher aus.	Wenn Sie in den erweiterten Einstellungen möchten, dass Amazon S3 einen Bucket erstellt und die Artefakte darin speichert, verwenden Sie den Standardspeicherort für den Artefaktspeicher. Oder wählen Sie einen benutzerdefinierten Speicherort aus und geben Sie einen vorhandenen Bucket an. Sie können das Artefakt auch mit einem Verschlüsselungsschlüssel verschlüsseln.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Quellanbieter an.	Wählen Sie für Quellanbieter GitHub (Version 2) aus.	App-Entwickler, AWS-Systemadministrator
Wählen Sie das Repository und den Zweig des Codes aus.	Wenn Sie nicht angemeldet sind, geben Sie die Verbindungsdetails an, um eine Verbindung zu herzustellen GitHub, und wählen Sie dann den Repository-Namen und den Branch-Namen aus.	App-Entwickler, AWS-Systemadministrator
Optionen zur Änderungserkennung.	Wählen Sie Pipeline bei Änderung des Quellcodes starten und wechseln Sie zur nächsten Seite.	App-Entwickler, AWS-Systemadministrator
Wählen Sie einen Build-Anbieter aus.	Wählen Sie für Build-Anbieter AWS CodeBuild aus und geben Sie dann die Details zur AWS-Region und zum Projektnamen für das Build-Projekt an. Wählen Sie für Build-Typ die Option Single Build aus.	App-Entwickler, AWS-Systemadministrator
Wählen Sie einen Bereitstellungsanbieter aus.	Wählen Sie für Anbieter bereitstellen die Option Amazon ECS aus. Wählen Sie den Clusternamen, den Servicenamen, die Image-Definitionsdatei, falls vorhanden, und einen Bereitstellungs-Timeout-Wert, falls erforderlich. Wählen Sie Create pipeline (Pipeline erstellen) aus.	App-Entwickler, AWS-Systemadministrator

Zugehörige Ressourcen

- AWS ECS-Dokumentation
- AWS ECR-Dokumentation
- AWS- CodeBuild Dokumentation
- AWS- CodeCommit Dokumentation
- AWS- CodePipeline Dokumentation
- Erstellen einer Continuous Delivery Pipeline für Ihre Container-Images mit Amazon ECR als Quelle (Blogbeitrag)

Verwenden von AWS CodeCommit und AWS CodePipeline zum Bereitstellen einer CI/CD-Pipeline in mehreren AWS-Konten

Erstellt von Kirankumar Chandrashekar (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps	Workload: Alle anderen Workloads
AWS-Services: AWS; CodeCommitAWS CodePipeline		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) für Ihre Anwendungscode-Workloads in separaten Amazon Web Services (AWS)-Konten für DevOps, Entwickler, Staging und Produktionsworkflows bereitstellen.

Sie können eine Strategie für mehrere AWS-Konten verwenden, um ein hohes Maß an Ressourcen- oder Sicherheitsisolierung bereitzustellen, Kosten zu optimieren und Ihren Produktions-Workflow aufzuteilen.

Der Code Ihrer Anwendung bleibt in all diesen separaten AWS-Konten identisch und wird in einem zentralen AWS- CodeCommit Repository verwaltet, das von Ihrem DevOps Konto gehostet wird. Ihre Entwickler-, Staging- und Produktionskonten verfügen über separate Git-Zweige in diesem CodeCommit Repository.

Wenn beispielsweise Code an die Git-Verzweigung des Entwicklers in Ihrem zentralen CodeCommit Repository übergeben wird, benachrichtigt Amazon EventBridge in Ihrem DevOps Konto EventBridge in Ihrem Entwicklerkonto über die Änderungen des Repositorys. In Ihrem Entwicklerkonto gehen AWS CodePipeline und die Quellphase in den `InProgress` Status über. Die Quellphase wird von der Git-Verzweigung des Entwicklers im zentralen CodeCommit Repository aus konfiguriert und CodePipeline übernimmt eine Servicerolle für das DevOps Konto.

Der Inhalt des CodeCommit Repositorys im Entwicklerzweig wird in einen Artefaktspeicher in einem Amazon Simple Storage Service (Amazon S3)-Bucket hochgeladen und mit einem AWS Key Management Service (AWS KMS)-Schlüssel verschlüsselt. Nachdem sich der Status der Quellphase

`Succeeded` in in geändert hat CodePipeline, wird der Code in die nächste Phase der Pipeline-Ausführung überführt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Bestehende AWS-Konten für jede erforderliche Umgebung (DevOps, Entwickler, Staging und Produktion). Diese Konten können von AWS Organizations gehostet werden.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.

Architektur

Technologie-Stack

- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS Organizations
- Amazon S3

Tools

- AWS CodeBuild – CodeBuild ist ein vollständig verwalteter Service zur kontinuierlichen Integration, der Quellcode kompiliert, Tests ausführt und Softwarepakete erstellt, die bereitgestellt werden können.
- AWS CodeCommit – CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet
- AWS CodePipeline – CodePipeline ist ein vollständig verwalteter kontinuierlicher Bereitstellungsservice, mit dem Sie Ihre Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturaktualisierungen automatisieren können.

- Amazon EventBridge – EventBridge ist ein Serverless-Event-Bus-Service zum Verbinden Ihrer Anwendungen mit Daten aus einer Vielzahl von Quellen.
- AWS Identity and Access Management (IAM) – IAM unterstützt Sie bei der sicheren Verwaltung des Zugriffs auf AWS-Services und -Ressourcen.
- AWS KMS – AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Verwaltung kryptografischer Schlüssel und deren Verwendung in einer Vielzahl von AWS-Services und in Ihren Anwendungen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.

Polen

Erstellen von Ressourcen in Ihrem DevOps AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Melden Sie sich bei der AWS-Managementkonsole für Ihr DevOps Konto an und öffnen Sie die - CodeCommit Konsole. Erstellen Sie ein Repository und richten Sie alle erforderlichen Git-Verzweigungen für Ihre AWS-Entwickler-, Staging- und Produktionskonten ein. Hilfe zu dieser und anderen Artikeln finden Sie im Abschnitt „Verwandte Ressourcen“.	DevOps Techniker
Erstellen Sie Anmeldeinformationen für das CodeCommit Repository.	Erstellen Sie in der IAM-Konsole Anmeldeinformationen, damit Anwendungsentwickler die Codebasis der Anwendung aus dem CodeCommit Repository pushen und abrufen können.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für CodePipeline Servicero llen.	Erstellen Sie in der IAM-Konsole eine IAM-Rolle, die von allen Ihren CodePipeline Servicerollen für den Zugriff auf das zentrale CodeCommit Repository verwendet werden kann.	Cloud-Administrator
Richten Sie die EventBridge Regeln für Ihre anderen AWS-Konten ein.	Richten Sie in der Amazon-EventBridge Konsole Regeln ein, um Benachrichtigungen über relevante CodeCommi t Repository-Änderungen an EventBridge in den einzelnen AWS-Entwickler-, Staging- und Produktionskonten zu senden.	Cloud-Administrator
Erstellen Sie einen AWS KMS-Schlüssel.	Erstellen Sie in der AWS KMS-Konsole einen KMS-Schlüssel, der es CodePipel ine Ihren einzelnen Entwickle r-, Staging- und Produktio ns-AWS-Konten ermöglicht, Artefakte zu verschlüsseln und zu entschlüsseln.	Cloud-Administrator

Erstellen von Ressourcen in Ihren anderen AWS-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie EventBridge für den Empfang von Ereignissen vom DevOps AWS-Konto ein.	Melden Sie sich bei der AWS-Managementkonsole für eines Ihrer einzelnen AWS-Konten an (Entwickler, Staging oder	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Produktion). Richten Sie in der Amazon- EventBridge Konsole ein, EventBridge um CodeCommit Repository-Änderungsereignisse von Ihrem DevOps Konto zu empfangen.	
Erstellen Sie einen S3-Bucket.	Erstellen Sie in der Amazon S3-Konsole einen S3-Bucket zum Speichern von CodePipeline Artefakten.	Cloud-Administrator
Erstellen Sie alle erforderlichen AWS-Ressourcen für CodePipeline Stufen.	Erstellen Sie alle anderen AWS-Ressourcen, die für die CodePipeline Phasen erforderlich sind. Diese Ressourcen variieren je nach Rolle jedes AWS-Kontos in Ihrer CI/CD-Pipeline.	Cloud-Administrator
Erstellen Sie eine IAM-Rolle.	Erstellen Sie in der IAM-Konsole eine IAM-Rolle für die CodePipeline Servicerolle. Diese Servicerolle muss in der Lage sein, die IAM-Rolle im DevOps Konto zu übernehmen, um auf das CodeCommit Repository zugreifen zu können.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline in CodePipeline.	Erstellen Sie in der - CodePipeline Konsole eine Pipeline. Erstellen Sie dann eine Quellphase, die auf das CodeCommit Repositor y im DevOps Konto für den jeweiligen Git-Zweig verweist.	Cloud-Administrator
Wiederholen Sie die Schritte für alle Ihre AWS-Konten.	Wiederholen Sie diese Schritte für alle AWS-Konten, die im Rahmen Ihrer CI/CD-Strategie erforderlich sind.	Cloud-Administrator

Zugehörige Ressourcen

Erstellen von Ressourcen in Ihrem DevOps AWS-Konto

- Erstellen eines CodeCommit Repositorys
- Einrichten eines CodeCommit Repositorys
- Erstellen und Freigeben einer Verzweigung in Ihrem CodeCommit Repository
- Erstellen von Anmeldeinformationen für das CodeCommit Repository
- Erstellen einer IAM-Rolle für CodePipeline Servicerollen
- Einrichten einer Regel in EventBridge
- Erstellen eines AWS KMS-Schlüssels
- Einrichten von Kontorichtlinien und -rollen für CodePipeline

Erstellen von Ressourcen in Ihren anderen AWS-Konten

- Aktivieren von EventBridge , um Ereignisse von Ihrem DevOps AWS-Konto zu empfangen
- Erstellen eines S3-Buckets für CodePipeline Artefakte
- Erstellen aller anderen erforderlichen AWS-Ressourcen für CodePipeline Stufen
- Erstellen einer IAM-Rolle für eine CodePipeline Servicerolle

- Erstellen einer Pipeline in CodePipeline
- Erstellen einer Pipeline in CodePipeline , die Ressourcen aus einem anderen AWS-Konto verwendet

Sonstige Ressourcen

- Richten Sie Ihre AWS-Umgebung mit bewährten Methoden ein
- Authentifizierung und Zugriffskontrolle für CodeCommit

Bereitstellen einer Firewall mit AWS Network Firewall und AWS Transit Gateway

Erstellt von Shrikantpatil (AWS)

Code-Repository: –aws-network-firewall-deploymentwith-transit-gateway	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Netzwerk; Sicherheit, Identität, Compliance
AWS-Services: AWS Network Firewall; AWS Transit Gateway; Amazon VPC; Amazon CloudWatch		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Firewall mithilfe von AWS Network Firewall und AWS Transit Gateway bereitstellen. Die Network Firewall-Ressourcen werden mithilfe einer AWS- CloudFormation Vorlage bereitgestellt. Network Firewall skaliert automatisch mit Ihrem Netzwerkverkehr und kann Hunderttausende von Verbindungen unterstützen, sodass Sie sich keine Gedanken über den Aufbau und die Wartung Ihrer eigenen Netzwerksicherheitsinfrastruktur machen müssen. Ein Transit Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre Virtual Private Clouds (VPCs) und On-Premises-Netzwerke miteinander verbinden können.

In diesem Muster lernen Sie auch, eine Inspektions-VPC in Ihre Netzwerkarchitektur aufzunehmen. Schließlich wird in diesem Muster erläutert, wie Sie Amazon verwenden, CloudWatch um eine Echtzeit-Aktivitätsüberwachung für Ihre Firewall bereitzustellen.

Tipp: Es hat sich bewährt, die Verwendung eines Network Firewall-Subnetzes zur Bereitstellung anderer AWS-Services zu vermeiden. Dies liegt daran, dass Network Firewall den Datenverkehr von Quellen oder Zielen innerhalb des Subnetzes einer Firewall nicht überprüfen kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- AWS Identity and Access Management (IAM)-Rollen- und Richtlinienberechtigungen
- CloudFormation -Vorlagenberechtigungen

Einschränkungen

Sie könnten Probleme mit der Domainfilterung haben und eine andere Art von Konfiguration könnte erforderlich sein. Weitere Informationen finden Sie unter Zustandsbehaftete Domänenlistenregelgruppen in AWS Network Firewall in der Network Firewall-Dokumentation.

Architektur

Technologie-Stack

- Amazon CloudWatch -Protokolle
- Amazon VPC
- AWS Network Firewall
- AWS Transit Gateway

Zielarchitektur

Das folgende Diagramm zeigt, wie Sie Network Firewall und Transit Gateway verwenden, um Ihren Datenverkehr zu überprüfen:

Die Architektur umfasst die folgenden Komponenten:

- Ihre Anwendung wird in den beiden Spoke-VPCs gehostet. Die VPCs werden von Network Firewall überwacht.
- Die Ausgangs-VPC hat direkten Zugriff auf das Internet-Gateway, ist aber nicht durch Network Firewall geschützt.
- In der Inspektions-VPC wird Network Firewall bereitgestellt.

Automatisierung und Skalierung

Sie können verwendenCloudFormation, um dieses Muster zu erstellen, indem Sie Infrastruktur als Code verwenden.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, damit Sie sie überwachen und sicher archivieren können.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.
- AWS Network Firewall ist eine zustandsbehaftete, verwaltete Netzwerk-Firewall sowie ein Service zur Erkennung und Verhinderung von Eindringlingen für VPCs in der AWS Cloud.
- AWS Transit Gateway ist ein zentraler Hub, der VPCs und On-Premises-Netzwerke miteinander verbindet.

Code

Der Code für dieses Muster ist in der GitHub AWS Network Firewall-Bereitstellung mit Transit Gateway-Repository verfügbar. Sie können die CloudFormation Vorlage aus diesem Repository verwenden, um eine einzelne Inspektions-VPC bereitzustellen, die Network Firewall verwendet.

Polen

Erstellen der Spoke-VPC und Inspektions-VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die CloudFormation Vorlage vor und stellen Sie sie bereit.	1. Laden Sie die `cloudformation/aws_nw_fw.yml` Vorlage aus dem GitHub Repository herunter. 2. Aktualisieren Sie die Vorlage mit Ihren Werten. 3. Stellen Sie die Vorlage bereit.	AWS DevOps

Erstellen des Transit-Gateways und der Routen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Transit-Gateway.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole . 2. Wählen Sie im Navigationsbereich Transit-Gateways aus. 3. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus. 4. Geben Sie unter Name tag einen Namen für das Transit-Gateway ein. 5. Geben Sie unter Beschreibung eine Beschreibung für das Transit-Gateway ein. 6. Behalten Sie für Amazon Side Autonomous System Number (ASN) den ASN-Standardwert bei. 7. Wählen Sie die DNS-Unterstützungsoption aus. 8. Wählen Sie die Option VPN ECMP-Unterstützung aus. 9. Wählen Sie die Option Standardzuordnung der Routing-Tabelle aus. Diese Option ordnet die Transit-Gateway-Anfügungen automatisch der Standard-	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Routing-Tabelle für das Transit-Gateway zu. 10. Wählen Sie die Option Standard-Verbreitung von Routing-Tabellen aus. Mit dieser Option werden die Transit-Gateway-An fügungen automatisch an die Standard-Routing-T abelle für das Transit-G ateway weitergegeben. 11. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.	
Erstellen Sie Transit-Gateway-Anfügungen.	Erstellen Sie eine Transit-Gateway-Anfügung für Folgendes: • Eine Inspektionsanfügung in der Inspektions-VPC und dem Transit-Gateway-Su bnetz • Eine SpokeVPCA-Anfügung in der Spoke VPCA und im privaten Subnetz • Ein SpokeVPCB-Anhang in der Spoke-VPCB und im privaten Subnetz • Ein EgressVPC-Anhang in der Egress-VPC und einem privaten Subnetz	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Transit-Gateway-Routing-Tabelle.	1. Erstellen Sie eine Transit-Gateway-Routing-Tabelle für die Spoke-VPC. Diese Routing-Tabelle muss allen anderen VPCs als der Inspektions-VPC zugeordnet sein. 2. Erstellen Sie eine Transit-Gateway-Routing-Tabelle für die Firewall. Diese Routing-Tabelle darf nur der Inspektions-VPC zugeordnet sein. 3. Fügen Sie der Transit-Gateway-Routing-Tabelle für die Firewall eine Route hinzu: • `0.0.0/0`Verwenden Sie für den EgressVPC-Anhang. • Verwenden Sie für den CIDR-Block SpokeVPCA den SpokeVPC1-Anhang. • Verwenden Sie für den CIDR-Block SpokeVPCB den SpokeVPC2-Anhang. 4. Fügen Sie der Transit-Gateway-Routing-Tabelle für die Spoke-VPC eine Route hinzu. `0.0.0/0`Verwenden Sie für den Anhang Überprüfungs-VPC.	AWS DevOps

Erstellen der Firewall und Routen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Firewall in der Inspektions-VPC.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole . 2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewalls aus. 3. Wählen Sie Firewall erstellen aus. 4. Geben Sie unter Name den Namen ein, den Sie zur Identifizierung dieser Firewall verwenden möchten. Sie können den Namen einer Firewall nicht mehr ändern, nachdem Sie sie erstellt haben. 5. Wählen Sie für VPC Ihre Inspektions-VPC aus. 6. Wählen Sie für Availability Zone und Subnetz die Zone und das Firewall-Subnetz aus, die Sie identifiziert haben. 7. Wählen Sie im Abschnitt Zugeordnete Firewall-Richtlinie die Option Zuordnen einer vorhanden en Firewall-Richtlinie und dann die Firewall-Richtlini	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e aus, die Sie zuvor erstellt haben. 8. Wählen Sie Firewall erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Firewall-Richtlinie.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole . 2. Wählen Sie im Navigationsbereich unter Netzwerk-Firewall die OptionFirewall-Richtlinien aus. 3. Wählen Sie auf der Seite Firewall-Richtlinie beschreiben die Option Firewall-Richtlinie erstellen aus. 4. Geben Sie unter Name den Namen ein, den Sie für die Firewall-Richtlinie verwenden möchten. Sie verwenden den Namen, um die Richtlinie zu identifizieren, wenn Sie die Richtlinie später in diesem Muster Ihrer Firewall zuordnen. Sie können den Namen einer Firewall-Richtlinie nicht mehr ändern, nachdem Sie sie erstellt haben. 5. Wählen Sie Weiter aus. 6. Wählen Sie auf der Seite Regelgruppen hinzufügen im AbschnittStateless-Regelgruppe die Option Zustandslose Regelgruppen hinzufügen aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Aktivieren Sie im Dialogfeld Aus vorhandenen Regelgruppen hinzufügen das Kontrollkästchen für die zustandslose Regelgruppe, die Sie zuvor erstellt haben. Wählen Sie Regelgruppen hinzufügen aus. Hinweis: Am unteren Rand der Seite zeigt der Kapazitätszähler der Firewall-Richtlinie die durch das Hinzufügen dieser Regelgruppe verbrauchte Kapazität neben der maximal zulässigen Kapazität für eine Firewall-Richtlinie an. 8. Legen Sie die zustandslose Standardaktion auf Weiter zu zustandsbehafteten Regeln fest. 9. Wählen Sie im Abschnitt Zustandsbehaftete Regelgruppe die Option Zustandsbehaftete Regelgruppen hinzufügen und aktivieren Sie dann das Kontrollkästchen für die zuvor erstellte Zustandsregelgruppe. Wählen Sie Regelgruppen hinzufügen aus. 10. Wählen Sie Weiter, um den Rest des Einrichtungsassist	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enten zu durchlaufen, und wählen Sie dann Firewall-Richtlinie erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Ihre VPC-Routing-Tabellen.	Routing-Tabellen der Überprüfungs-VPC 1. Fügen Sie in der ANF Subnetz-Routing-Tabelle (`Inspection-ANFRT`) `0.0.0/0` zur Transit-Gateway-ID hinzu. 2. Fügen Sie in der Routing-Tabelle des Transit-Gateway-Subnetzes (`Inspection-TGWRT`) `0.0.0/0` zur EgressVPC hinzu. SpokeVPCA-Routing-Tabelle Fügen Sie in der privaten Routing-Tabelle `0.0.0.0/0` zur Transit-Gateway-ID hinzu. Spoke-VPCB-Routing-Tabelle Fügen Sie in der privaten Routing-Tabelle `0.0.0.0/0` zur Transit-Gateway-ID hinzu. VPC-Routing-Tabellen für ausgehenden Verkehr Fügen Sie in der öffentlichen Routing-Tabelle für ausgehenden Verkehr den CIDR-Block SpokeVPCA und Spoke VPCB zur Transit-Gateway-ID hinzu. Wiederholen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie denselben Schritt für das private Subnetz.	

Einrichten CloudWatch von zur Durchführung von Netzwerkprüfungen in Echtzeit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Protokollierungskonfiguration der Firewall.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole . 2. Wählen Sie im Navigationsbereich unter Netzwerk-Firewall die OptionFirewalls aus. 3. Wählen Sie auf der Seite Firewalls den Namen der Firewall aus, die Sie bearbeiten möchten. 4. Wählen Sie die Registerkarte Firewall-Details aus. Wählen Sie im Abschnitt Protokollierung die Option Bearbeiten aus. 5. Passen Sie die Auswahl des Protokolltyps nach Bedarf an. Sie können die Protokollierung für Warnungs- und Flow-Protokolle konfigurieren. • Warnung – Sendet Protokolle für Datenverkehr, der einer zustandsb	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ehafteten Regel entsprich t, bei der die Aktion auf Warnung oder Löschen gesetzt ist. Weitere Informationen zu zustandsbehafteten Regeln und Regelgrup pen finden Sie unter Regelgruppen in AWS Network Firewall . • Flow – Sendet Protokoll e für den gesamten Netzwerkverkehr, den die zustandslose Engine an die zustandsbehaftete Regel-Engine weiterleitet. 6. Wählen Sie für jeden ausgewählten Protokolltyp den Zieltyp aus und geben Sie dann die Informationen für das Protokollierungszi el an. Weitere Informati onen finden Sie unter AWS Network Firewall-Protokoll ierungsziele in der Network Firewall-Dokumentation. 7. Wählen Sie Speichern.	

Überprüfen der Einrichtung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine EC2-Instance, um die Einrichtung zu testen.	Starten Sie zwei Amazon Elastic Compute Cloud (Amazon EC2)-Instances in der Spoke-VPC: eine für Jumpbox und eine für Testkonnektivität.	AWS DevOps
Überprüfen Sie die Metriken.	Metriken werden zuerst nach dem Service-Namespace und dann nach den verschiedenen Dimensionskombinationen in jedem Namespace gruppiert. Der CloudWatch Namespace für Network Firewall ist `AWS/NetworkFirewall` . 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigationsbereich Metriken aus. 3. Wählen Sie auf der Registerkarte Alle Metriken die Region und dann AWS/NetworkFirewall aus.	AWS DevOps

Zugehörige Ressourcen

- Einfache Single-Zone-Architektur mit einem Internet-Gateway
- Multi-Zone-Architektur mit einem Internet-Gateway
- Architektur mit einem Internet-Gateway und einem NAT-Gateway

Bereitstellen eines AWS Glue-Auftrags mit einer AWS CodePipeline CI/CD-Pipeline

Erstellt von Bruno Klein (AWS) und Luis Henrique Massao Yamada (AWS)

Umgebung: Produktion	Technologien: DevOps; Big Data	AWS-Services: AWS Glue ; AWS CodeCommit; AWS CodePipeline; AWS Lambda

Übersicht

Dieses Muster zeigt, wie Sie Amazon Web Services (AWS) CodeCommit und AWS CodePipeline in AWS Glue integrieren und AWS Lambda verwenden können, um Aufträge zu starten, sobald ein Entwickler seine Änderungen in ein Remote-AWS- CodeCommit Repository überträgt.

Wenn ein Entwickler eine Änderung an ein ETL-Repository (Extract, Transform, Load) sendet und die Änderungen an AWS überträgt CodeCommit, wird eine neue Pipeline aufgerufen. Die Pipeline initiiert eine Lambda-Funktion, die einen AWS Glue-Auftrag mit diesen Änderungen startet. Der AWS Glue-Auftrag führt die ETL-Aufgabe aus.

Diese Lösung ist in der Situation hilfreich, in der Unternehmen, Entwickler und Dateningenieure Aufträge starten möchten, sobald Änderungen festgeschrieben und an die Ziel-Repositorys übertragen werden. Es trägt dazu bei, ein höheres Maß an Automatisierung und Reproduzierbarkeit zu erreichen und somit Fehler während des Starts und Lebenszyklus des Auftrags zu vermeiden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Git auf dem lokalen Computer installiert
- Amazon Cloud Development Kit (Amazon CDK) auf dem lokalen Computer installiert
- Python auf dem lokalen Computer installiert
- Der Code im Abschnitt Anhänge

Einschränkungen

- Die Pipeline ist abgeschlossen, sobald der AWS Glue-Auftrag erfolgreich gestartet wurde. Es wartet nicht auf den Abschluss des Auftrags.
- Der im Anhang angegebene Code dient nur zu Demonstrationszwecken.

Architektur

Zieltechnologie-Stack

- AWS Glue
- AWS Lambda
- AWS CodePipeline
- AWS CodeCommit

Zielarchitektur

Der Prozess besteht aus den folgenden Schritten:

1. Der Entwickler oder Dateningenieur nimmt eine Änderung am ETL-Code vor, überträgt die Änderung und überträgt sie an AWS CodeCommit.
2. Der Push initiiert die Pipeline.
3. Die Pipeline initiiert eine Lambda-Funktion, die das Repository `codecommit:GetFile` aufruft und die Datei in Amazon Simple Storage Service (Amazon S3) hochlädt.
4. Die Lambda-Funktion startet einen neuen AWS Glue-Auftrag mit dem ETL-Code.
5. Die Lambda-Funktion beendet die Pipeline.

Automatisierung und Skalierung

Die Beispielanfügung zeigt, wie Sie AWS Glue in AWS integrieren können CodePipeline. Es bietet ein Basisbeispiel, das Sie für Ihren eigenen Gebrauch anpassen oder erweitern können. Weitere Informationen finden Sie im Abschnitt „Epics“.

Tools

- AWS CodePipeline – AWS CodePipeline ist ein vollständig verwalteter kontinuierlicher Bereitstellungsservice, mit dem Sie Ihre Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturaktualisierungen automatisieren können.
- AWS CodeCommit – AWS CodeCommit ist ein vollständig verwalteter Service zur Quellcodeverwaltung, der sichere, Git-basierte Repositorys hostet.
- AWS Lambda – AWS Lambda ist ein Serverless-Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen.
- AWS Glue – AWS Glue ist ein Serverless-Datenintegrationsservice, der das Erkennen, Vorbereiten und Kombinieren von Daten für Analysen, Machine Learning und Anwendungsentwicklung vereinfacht.
- Git-Client – Git bietet GUI-Tools, oder Sie können die Befehlszeile oder ein Desktop-Tool verwenden, um die erforderlichen Artefakte von zu überprüfen GitHub.
- AWS CDK – Das AWS CDK ist ein Open-Source-Softwareentwicklungs-Framework, mit dem Sie Ihre Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen definieren können.

Polen

Stellen Sie den Beispielcode bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS CLI.	Konfigurieren Sie die AWS-Befehlszeilenschnittstelle (AWS CLI), um auf Ihr aktuelles AWS-Konto abzuzielen und sich mit diesem zu authentifizieren. Anweisungen finden Sie in der AWS CLI-Dokumentation.	Entwickler, DevOps Techniker
Extrahieren Sie die Beispielprojektdateien.	Extrahieren Sie die Dateien aus dem Anhang, um einen	Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ordner zu erstellen, der die Beispielprojektdateien enthält.	

Stellen Sie den Beispielcode bereit.	Nachdem Sie die Dateien extrahiert haben, führen Sie am Speicherort Extract die folgenden Befehle aus, um ein Baseline-Beispiel zu erstellen:
	`cdk bootstrap`
	`cdk deploy`
	`git init`
	`git remote add origin <code-commit-repository-url>`
	`git stage .`
	`git commit -m "adds sample code"`
	`git push --set-upstream origin main`
	Nach dem letzten Befehl können Sie den Status der Pipeline und des AWS Glue-Auftrags überwachen.
		Entwickler, DevOps Techniker

Passen Sie den Code an.	Passen Sie den Code für die etl.py-Datei an Ihre Geschäftsanforderungen an. Sie können den ETL-Code überarbeiten, die Pipeline-Phasen ändern oder die Lösung erweitern.	Dateningenieur

Zugehörige Ressourcen

- Erste Schritte mit dem AWS-CDK

- Hinzufügen von Aufträgen in AWS Glue
- Integrationen von Quellaktionen in CodePipeline
- Aufrufen einer AWS Lambda-Funktion in einer Pipeline in CodePipeline
- AWS Glue-Programmierung
- AWS CodeCommit GetFile -API

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Bereitstellen eines Amazon EKS-Clusters aus AWS Cloud9 mithilfe eines EC2-Instance-Profils

Erstellt von Sagar Panigrahi (AWS)

Umgebung: Produktion	Technologien: DevOps; Container und Microservices	Workload: Alle anderen Workloads
AWS-Services: Amazon EKS; AWS Cloud9; AWS Identity and Access Management; AWS CloudFormation		

Übersicht

Dieses Muster beschreibt, wie Sie mit AWS Cloud9 und AWS einen Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster CloudFormation erstellen, der betrieben werden kann, ohne den programmgesteuerten Zugriff für Benutzer in Ihrem Amazon Web Services (AWS)-Konto zu aktivieren.

AWS Cloud9 ist eine cloudbasierte integrierte Entwicklungsumgebung (IDE), mit der Sie Ihren Code mithilfe eines Browsers schreiben, ausführen und debuggen können. AWS Cloud9 wird als Kontrollzentrum verwendet, das einen Amazon EKS-Cluster mithilfe von Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Profilen und AWS- CloudFormation Vorlagen bereitstellt.

Sie können dieses Muster verwenden, wenn Sie keine AWS Identity and Access Management (IAM)-Benutzer erstellen und stattdessen IAM-Rollen verwenden möchten. Die rollenbasierte Zugriffskontrolle (RBAC) regelt den Zugriff auf Ressourcen basierend auf den Rollen einzelner Benutzer. Dieses Muster zeigt, wie RBAC innerhalb eines Amazon-EKS-Clusters aktualisiert wird, um den Zugriff auf eine bestimmte IAM-Rolle zu ermöglichen.

Die Einrichtung des Musters hilft Ihrem DevOps Team auch dabei, AWS Cloud9-Funktionen zu verwenden, um Infrastructure as Code (IaC)-Ressourcen für die Erstellung der Amazon EKS-Infrastruktur zu warten und zu entwickeln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Erstellen von IAM-Rollen und -Richtlinien für das Konto. Die IAM-Rolle für den Benutzer muss die `AWSCloud9Administrator` Richtlinie enthalten. Die `eksNodeRoles` Rollen `AWSServiceRoleForAmazonEKS` und müssen ebenfalls erstellt werden, da sie zum Erstellen eines Amazon-EKS-Clusters erforderlich sind.
- Kenntnisse der Kubernetes-Konzepte.

Einschränkungen

- Dieses Muster beschreibt, wie Sie einen einfachen Amazon-EKS-Cluster erstellen. Für Produktions-Cluster müssen Sie die AWS- CloudFormation Vorlage aktualisieren.
- Das Muster stellt keine zusätzlichen Kubernetes-Komponenten bereit (z. B. Fluentd , Ingress-Controller oder Speichercontroller).

Architektur

Trichter-Stack

- AWS Cloud9
- AWS CloudFormation
- Amazon EKS
- IAM

Automatisierung und Skalierung

Sie können dieses Muster erweitern und es in Pipelines für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) integrieren, um die vollständige Bereitstellung von Amazon EKS zu automatisieren.

Tools

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen müssen und sich mehr auf Ihre Anwendungen konzentrieren können.
- AWS Cloud9 – AWS Cloud9 bietet eine umfassende Codebearbeitungserfahrung mit Unterstützung für mehrere Programmiersprachen und Laufzeit-Debugger sowie ein integriertes Terminal.
- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Kubectl – `kubectl` ist ein Befehlszeilendienstprogramm, mit dem Sie mit einem Amazon-EKS-Cluster interagieren können.

Polen

Erstellen der IAM-Rollen für das EC2-Instance-Profil

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die IAM-Konsole, wählen Sie Richtlinien und dann Richtlinie erstellen aus. Wählen Sie die Registerkarte JSON und fügen Sie den Inhalt aus der Datei policy-role-eks-instance-profile-for-cloud9.json (angefügt) ein. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidierung generiert wurden, und wählen Sie dann Richtlinie überprüfen aus. Füllen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie das Feld Name für die Richtlinie aus. Wir empfehlen Ihnen, `eks-instance-profile-for-cloud9` für den Richtliniennamen zu verwenden. Überprüfen Sie unter Summary die Richtlini enzusammenfassung, um die Berechtigungen einzusehe n, die von Ihrer Richtlinie gewährt werden. Wählen Sie dann Richtlinie erstellen aus.	
Erstellen Sie eine IAM-Rolle mithilfe der -Richtlinie.	Wählen Sie in der IAM-Konsole Rollen und dann Rolle erstellen aus. Wählen Sie AWS Service und dann EC2 aus der Liste aus. Wählen Sie Weiter: Berechtig ungen und suchen Sie nach der IAM-Richtlinie, die Sie zuvor erstellt haben. Wählen Sie die entsprechenden Tags für Ihre Anforderungen aus. Geben Sie im Abschnitt Überprüfen einen Namen für die Rolle ein. Wir empfehlen Ihnen, `role-eks-instance-profile-for-cloud9` für den Rollennamen zu verwenden. Wählen Sie dann Create Role.	Cloud-Administrator

Erstellen einer IAM-Richtlinie und -Rolle für Amazon EKS RBAC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie.	Wählen Sie in der IAM-Konsole Richtlinien und dann Richtlinie erstellen aus. Wählen Sie die Registerkarte JSON und fügen Sie den Inhalt aus der policy-for-eks-rbacJSON-Datei ein (angefügt). Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidierung generiert wurden, und wählen Sie dann Richtlinie überprüfen aus. Füllen Sie das Feld Name für die Richtlinie aus. Wir empfehlen Ihnen, `policy-for-eks-rbac` für den Richtliniennamen zu verwenden. Überprüfen Sie unter Summary die Richtlinienzusammenfassung, um die Berechtigungen einzusehen, die von Ihrer Richtlinie gewährt werden. Wählen Sie dann Richtlinie erstellen aus.	Cloud-Administrator
Erstellen Sie eine IAM-Rolle mithilfe der -Richtlinie.	Wählen Sie in der IAM-Konsole Rollen und dann Rolle erstellen aus. Wählen Sie AWS Service und dann EC2 aus der Liste aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wählen Sie Weiter: Berechtigungen und suchen Sie nach der IAM-Richtlinie, die Sie zuvor erstellt haben. Wählen Sie die entsprechenden Tags für Ihre Anforderungen aus. Geben Sie im Abschnitt Review einen Namen für die Rolle ein. Wir empfehlen Ihnen, `role-eks-admin-for-rbac` für den Rollennamen zu verwenden. Wählen Sie dann Create Role.	

Erstellen der AWS Cloud9-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS Cloud9-Umgebung.	Öffnen Sie die AWS Cloud9-Konsole und wählen Sie Umgebung erstellen aus. Geben Sie auf der Seite Name-Umgebung einen Namen für Ihre Umgebung ein. Wir empfehlen Ihnen, `eks-management-env` für den Umgebungsnamen zu verwenden. Konfigurieren Sie die verbleibenden Einstellungen entsprechend Ihren Anforderungen und wählen Sie dann Nächster Schritt aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wählen Sie auf der Seite Review (Überprüfung) die Option Create environment (Umgebung erstellen) aus. Warten Sie, bis AWS Cloud9 Ihre Umgebung erstellt. Dies kann mehrere Minuten dauern. Weitere Informationen zu den verfügbaren Konfigurationsoptionen finden Sie unter Erstellen einer EC2-Umgebung in der AWS Cloud9-Dokumentation.	
Entfernen Sie die temporären IAM-Anmeldeinformationen für AWS Cloud9.	Nachdem Ihre AWS Cloud9-Umgebung bereitgestellt wurde, wählen Sie im Zahnradsymbol Einstellungen aus. Wählen Sie unter Einstellungen die Option AWS-Einstellungen und dann Anmeldeinformationen aus. Deaktivieren Sie die von AWS verwalteten temporären Anmeldeinformationen und schließen Sie die Registerkarte .	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das EC2-Instance-Profil an die zugrunde liegende EC2-Instance an.	Öffnen Sie die Amazon EC2-Konsole und wählen Sie die EC2-Instance aus, die Ihrer Umgebung in AWS Cloud9 entspricht. Wenn Sie den von uns empfohlenen Namen verwendet haben, heißt die EC2-Instance `aws-cloud9-eks-management-env` . Wählen Sie die EC2-Instance, dann Aktionen und dann Instance-Einstellungen aus. Wählen Sie IAM-Rolle anfügen/ersetzen aus. Suchen Sie nach `role-eks-instance-profile-for-cloud9` oder dem Namen der IAM-Rolle, die Sie zuvor erstellt haben, und wählen Sie dann Anwenden aus.	Cloud-Administrator

Erstellen des Amazon-EKS-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Amazon-EKS-Cluster.	Laden Sie die Vorlage eks-cfn.yaml (angefügt) für AWS herunter und öffnen Sie sie CloudFormation. Bearbeiten Sie die Vorlage entsprechend Ihren Anforderungen.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Öffnen Sie die AWS Cloud9-Umgebung und wählen Sie Neue Datei aus. Fügen Sie die zuvor erstellte AWS-CloudFormation Vorlage in das Feld ein. Wir empfehlen , eks-cfn.yaml als Vorlagenn amen zu verwenden. Führen Sie im AWS Cloud9-Terminal den folgenden Befehl aus, um den Amazon EKS-Cluster zu erstellen: `aws cloudformation create-stack --stack-name eks-cluster --template-body file://eks-cfn.yaml --region <your_AWS_Region>` Wenn der AWS- CloudForm ation Aufruf erfolgreich ist, erhalten Sie den Amazon-Re ssourcennamen (ARN) des AWS- CloudFormation Stacks in Ihrer Ausgabe. Die Stack-Erstellung kann zwischen 10 und 20 Minuten dauern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status des Amazon-EKS-Clusters.	Öffnen Sie in der AWS-CloudFormation Konsole die Seite Stacks und wählen Sie dann den Stack-Namen aus. Der Stack wird erstellt, wenn der Stack-Statuscode anzeigt`CREATE_COMPLETE` . Weitere Informationen finden Sie unter Anzeigen von AWS-CloudFormation Stack-Daten und Ressourcen in der AWS-CloudFormation Dokumentation.	Cloud-Administrator

Zugriff auf die Kubernetes-Ressourcen im Amazon-EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie kubectl in der AWS Cloud9-Umgebung.	Installieren Sie `kubectl` in Ihrer AWS Cloud9-Umgebung, indem Sie den Anweisungen unter Installieren von kubectl in der Amazon EKS-Dokumentation folgen.	Cloud-Administrator
Aktualisieren Sie die neue Amazon EKS-Konfiguration in AWS Cloud9.	Führen Sie den folgenden Befehl im AWS Cloud9-Terminal aus, um die `kubeconfig` vom Amazon EKS-Cluster in die AWS Cloud9-Umgebung zu aktualisieren:	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws eks update-kubeconfig --name EKS-DEV2 --region <your_AWS_Region>` Wichtig: `EKS-DEV2` ist der Name des Amazon EKS-Clusters in der AWS- CloudFormation Vorlage, die Sie zum Erstellen des Clusters verwendet haben. Führen Sie den `kubectl get all -A` Befehl aus, um alle Kubernetes-Ressourcen anzuzeigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die Administrator-IAM-Rolle zum Kubernetes-RBAC hinzu.	Führen Sie den folgenden Befehl in Ihrem AWS Cloud9-Terminal aus, um die RBAC-Konfigurationszuordnung für Amazon EKS im Bearbeitungsmodus zu öffnen:
	`kubectl edit cm/aws-auth -n kube-system`
	Fügen Sie die folgenden Zeilen unter dem `mapRoles` Abschnitt an:
	`- groups:`
	`- system:masters`
	`rolearn: <ARN_of_IAM_role _from_second_epic>`
	`username: eksadmin`
	Verwenden Sie die Datei im YAML-Format, um Syntaxfehler zu vermeiden. Speichern Sie die Datei mit `-vi`Befehlen und beenden Sie dann die Datei.
	Hinweis: Durch Hinzufügen dieses Abschnitts informieren Sie den Kubernetes-RBAC, der vollen Administratorzugriff auf den Amazon-EKS-Cluster erhalten `<ARN_of_IAM_role _from_second_epic>` soll. Das
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bedeutet, dass die identifizierte IAM-Rolle administrative Aktionen auf dem Kubernetes-Cluster ausführen kann. AWS fügt den vorhandenen Abschnitt unter hinzu, `mapRoles` während der Amazon-EKS-Cluster bereitgestellt wird.	

Zugehörige Ressourcen

Referenzen

- modulare und skalierbare Amazon-EKS-Architektur (Schnellstart)
- Verwalten von Benutzern oder IAM-Rollen für Ihren Amazon-EKS-Cluster
- AWS- CloudFormation Vorlage zum Erstellen einer neuen Amazon EKS-Steuerebene

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Bereitstellen von Code in mehreren AWS-Regionen mithilfe von AWS CodePipeline, AWS CodeCommitund AWS CodeBuild

Erstellt von Rama Anand Krishna Varanasi (AWS)

Erstellt von: AWS	Umgebung: PoC oder Pilotprojekt	Technologien: Management und Governance; DevOps
AWS-Services: AWS CodeCommit; AWS CodePipeline; AWS CodeBuild		

Übersicht

Dieses Muster zeigt, wie Infrastruktur oder Architektur mithilfe von AWS über mehrere Amazon Web Services (AWS)-Regionen hinweg erstellt werden CloudFormation. Es umfasst kontinuierliche Integration (CI)/kontinuierliche Bereitstellung (CD) in mehreren AWS-Regionen für schnellere Bereitstellungen. Die Schritte in diesem Muster wurden getestet, um einen AWS- CodePipeline Auftrag zur Bereitstellung in drei AWS-Regionen als Beispiel zu erstellen. Sie können die Anzahl der Regionen je nach Anwendungsfall ändern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Zwei AWS Identity and Access Management (IAM)-Rollen für AWS CodeBuild und AWS CloudFormation mit den richtigen Richtlinien für , CodeBuild um die CI-Aufgaben Tests, Bündelung, Paketierung der Artefakte und Bereitstellung in mehreren AWS-Regionen parallel auszuführen. Hinweis: Überprüfen Sie die Richtlinien, die von erstellt wurden CodePipeline , um sicherzustellen, dass CodeBuild und AWS über die richtigen Berechtigungen in den CI- und CD-Phasen CloudFormation verfügen.
  - Eine CodeBuild Rolle mit den AmazonS3FullAccess- und -CloudWatchFullAccessRichtlinien. Diese Richtlinien ermöglichen den CodeBuild Zugriff, Ereignisse von AWS CodeCommit über Amazon zu überwachen CloudWatch und Amazon Simple Storage Service (Amazon S3) als Artefaktspeicher zu verwenden.

- Eine AWS- CloudFormation Rolle mit den folgenden Richtlinien, die AWS in der letzten Build-Phase die Möglichkeit geben CloudFormation, AWS Lambda-Funktionen zu erstellen oder zu aktualisieren, Amazon- CloudWatch Protokolle zu pushen oder zu überwachen und Änderungssätze zu erstellen und zu aktualisieren.
  - AWSLambdaFullAccess
  - AWSCodeDeployFullAccess
  - CloudWatchFullAccess
  - AWSCloudFormationFullAccess
  - AWSCodePipelineFullAccess

Architektur

Die Architektur und der Workflow dieses Musters für mehrere Regionen umfassen die folgenden Schritte.

1. Sie senden Ihren Code an ein CodeCommit Repository.
2. Nach Erhalt einer Codeaktualisierung oder eines Commit CodeCommit ruft ein CloudWatch Ereignis auf, das wiederum einen CodePipeline Auftrag startet.
3. CodePipeline aktiviert das CI, das von verarbeitet wird CodeBuild. Die folgenden Aufgaben werden ausgeführt.
   - Testen der AWS- CloudFormation Vorlagen (optional)
   - Verpackung der AWS- CloudFormation Vorlagen für jede Region, die in der Bereitstellung enthalten ist. Dieses Muster wird beispielsweise parallel für drei AWS-Regionen bereitgestellt, sodass die AWS- CloudFormation Vorlagen in drei S3-Buckets CodeBuild verpackt, einen in jeder angegebenen Region. Die S3-Buckets werden von nur CodeBuild als Artefakt-Repositorys verwendet.
4. CodeBuild packt die Artefakte als Eingabe für die nächste Bereitstellungsphase, die parallel in den drei AWS-Regionen ausgeführt wird. Wenn Sie eine andere Anzahl von Regionen angeben, CodePipeline wird in diesen Regionen bereitgestellt.

Tools

Tools

- AWS CodePipeline – CodePipeline ist ein kontinuierlicher Bereitstellungsservice, mit dem Sie die Schritte modellieren, visualisieren und automatisieren können, die erforderlich sind, um Ihre Softwareänderungen kontinuierlich freizugeben.
- AWS CodeBuild – CodeBuild ist ein vollständig verwalteter Build-Service, der Ihren Quellcode kompiliert, Einheitentests ausführt und Artefakte erzeugt, die bereitgestellt werden können.
- AWS CodeCommit – CodeCommit ist ein von Amazon Web Services gehosteter Service zur Versionskontrolle, mit dem Sie Komponenten (wie Quellcode und Binärdateien) privat in der Cloud speichern und verwalten können.
- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer Amazon Web Services-Ressourcen unterstützt, sodass Sie weniger Zeit für die Verwaltung dieser Ressourcen aufwenden müssen und sich stattdessen mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden.
- AWS Identity and Access Management – AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.

Code

Der folgende Beispielcode bezieht sich auf die -`BuildSpec.yaml`Datei (Build-Phase).

```
---
artifacts:
discard-paths: true
files:
- packaged-first-region.yaml
- packaged-second-region.yaml
- packaged-third-region.yaml
phases:
build:
commands:
- echo "********BUILD PHASE - CF PACKAGING**********"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_FIRST_REGION --output-template-file packaged-first-region.yaml --region
 $FIRST_REGION"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_SECOND_REGION --output-template-file packaged-second-region.yaml --region
 $SECOND_REGION"
```

```
- "aws cloudformation package --template-file sam-template-anand.yaml --s3-bucket
 $S3_THIRD_REGION --output-template-file packaged-third-region.yaml --region
 $THIRD_REGION"
install:
commands:
- echo "********BUILD PHASE - PYTHON SETUP**********"
runtime-versions:
python: 3.8
post_build:
commands:
- echo "********BUILD PHASE - PACKAGING COMPLETION**********"
pre_build:
commands:
- echo "********BUILD PHASE - DEPENDENCY SETUP**********"
- "npm install --silent --no-progress"
- echo "********BUILD PHASE - DEPENDENCY SETUP DONE**********"
version: 0.2
```

Polen

Vorbereiten des Codes und des CodeCommit Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die primäre AWS-Region für die Bereitstellung aus.	Melden Sie sich bei Ihrem AWS-Konto an und wählen Sie die primäre Region für die Bereitstellung aus. Das CodeCommit Repository wird sich in der primären Region befinden.	DevOps
Erstellen Sie das CodeCommit Repository.	Erstellen Sie das CodeCommit Repository und übertragen Sie den erforderlichen Code hinein. Der Code enthält im Allgemeinen die AWS-CloudFormation oder AWS SAM-Vorlagen, gegebenen falls den Lambda-Code und	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die CodeBuild `buildspec .yaml` Dateien als Eingabe für AWS CodePipeline.	
Übertragen Sie den Code in das CodeCommit Repository.	Laden Sie im Abschnitt Anhänge den Code für dieses Beispiel herunter und übertragen Sie dann den erforderlichen Code hinein. Im Allgemeinen kann der Code AWS- CloudFormation oder AWS SAM-Vorlagen, Lambda-Code und die CodeBuild `buildspec.yaml` Dateien als Eingabe für die Pipeline enthalten.	DevOps

Quellphase: Pipeline erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CodePipel ine Auftrag.	Wählen Sie in der - CodePipel ine Konsole Pipeline erstellen aus.	DevOps
Benennen Sie den CodePipel ine Auftrag und wählen Sie die Servicerolleneinstellung aus.	Geben Sie einen Namen für den Auftrag ein und behalten Sie die Standardeinstellung für die Servicerolle bei, sodass die Rolle mit den erforderl ichen Richtlinien CodePipeline erstellt.	DevOps
Geben Sie den Speicherort für den Artefaktspeicher an.	Behalten Sie unter Erweiterte Einstellungen die Standardo	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ption bei, sodass einen S3-Bucket CodePipeline erstellt, der für die Speicherung von Codeartefakten verwendet werden soll. Wenn Sie stattdessen einen vorhanden en S3-Bucket verwenden, muss sich der Bucket in der primären Region befinden, die Sie im ersten Epi angegeben haben.	
Geben Sie den Verschlüs selungsschlüssel an.	Behalten Sie die Standardo ption Standard-AWS-verwa lteter Schlüssel bei oder wählen Sie Ihren eigenen vom Kunden verwalteten AWS Key Management Service (AWS KMS)-Schlüssel.	DevOps
Geben Sie den Quellanbieter an.	Wählen Sie unter Quellanbi eter die Option AWS aus CodeCommit.	DevOps
Geben Sie das Repository an.	Wählen Sie das CodeCommi t Repository aus, das Sie im ersten Epi erstellt haben. Wenn Sie den Code in einer Verzweigung platziert haben, wählen Sie die Verzweigung aus.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie an, wie Codeänderungen erkannt werden.	Behalten Sie den Standardwert Amazon CloudWatch Events als Änderungsauslöser für bei, CodeCommit um den CodePipeline Auftrag zu starten.	DevOps

Build-Phase: Konfigurieren der Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Build-Anbieter an.	Wählen Sie für den Build-Anbieter AWS aus CodeBuild.	DevOps
Geben Sie die AWS-Region an.	Wählen Sie die primäre Region aus, die Sie im ersten Epic angegeben haben.	DevOps

Erstellungsphase: Erstellen und Konfigurieren des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen des Projekts	Wählen Sie Projekt erstellen und geben Sie einen Namen für das Projekt ein.	DevOps
Geben Sie das Umgebungs-Image an.	Verwenden Sie für diese Musterdemonstration das standardmäßige CodeBuild verwaltete Image. Sie haben auch die Möglichkeit, ein benutzerdefiniertes Docker-Image zu verwenden, falls Sie eines haben.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie das Betriebss ystem an.	Wählen Sie entweder Amazon Linux 2 oder Ubuntu aus.	DevOps
Geben Sie die Servicerolle an.	Wählen Sie die Rolle aus, für die Sie erstellt haben, CodeBuild bevor Sie mit der Erstellung des CodePipeline Auftrags begonnen haben. (Siehe Abschnitt Vorausset zungen.)	DevOps
Legen Sie zusätzliche Optionen fest.	Behalten Sie für Timeout und Timeout in der Warteschl ange die Standardwerte bei. Behalten Sie für Zertifikat die Standardeinstellung bei, es sei denn, Sie haben ein benutzerd efiniertes Zertifikat, das Sie verwenden möchten.	DevOps
Erstellen Sie die Umgebungs variablen.	Erstellen Sie für jede AWS-Region, in der Sie bereitste llen möchten, Umgebungs variablen, indem Sie den Namen des S3-Buckets und den Namen der Region angeben (z. B. us-east-1).	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen der buildspec-Datei an, falls es sich nicht um buildspec.yml handelt.	Lassen Sie dieses Feld leer, wenn der Dateiname der Standardwert ist, `buildspec.yaml` . Wenn Sie die buildspec-Datei umbenannt haben, geben Sie hier den Namen ein. Stellen Sie sicher, dass er mit dem Namen der Datei übereinstimmt, die sich im CodeCommit Repository befindet.	DevOps
Geben Sie die Protokollierung an.	Um Protokolle für Amazon CloudWatch Events anzuzeigen, behalten Sie die Standardeinstellung bei. Oder Sie können bestimmte Gruppen- oder Logger-Namen definieren.	DevOps

Überspringen der Bereitstellungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überspringen Sie die Bereitstellungsphase und schließen Sie die Erstellung der Pipeline ab.	Wenn Sie die Pipeline einrichten, CodePipeline können Sie in der Bereitstellungsphase nur eine Phase erstellen. Um in mehreren AWS-Regionen bereitzustellen, überspringen Sie diese Phase. Nachdem die Pipeline erstellt wurde, können Sie	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mehrere Phasen der Bereitste llung hinzufügen.	

Bereitstellungsphase: Konfigurieren der Pipeline für die Bereitstellung in der ersten Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Bereitste llungsphase eine Stufe hinzu.	Bearbeiten Sie die Pipeline und wählen Sie in der Bereitstellungsphase Stufe hinzufügen aus. Diese erste Phase bezieht sich auf die primäre Region.	DevOps
Geben Sie einen Aktionsna men für die Stufe an.	Geben Sie einen eindeutig en Namen ein, der die erste (primäre) Phase und Region widerspiegelt. Geben Sie beispielsweise primary_< region>_deploy ein.	DevOps
Geben Sie den Aktionsan bieter an.	Wählen Sie für Aktionsan bieter AWS aus CloudForm ation.	DevOps
Konfigurieren Sie die Region für die erste Phase.	Wählen Sie die erste (primäre) Region aus, dieselbe Region, in der CodePipeline und eingerichtet CodeBuild sind. Dies ist die primäre Region, in der Sie den Stack bereitstellen möchten.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie das Eingabear tefakt an.	Wählen Sie BuildArtifact. Dies ist die Ausgabe der Build-Pha se.	DevOps
Geben Sie die Aktion an, die ausgeführt werden soll.	Wählen Sie für Aktionsmodus die Option Stack erstellen oder aktualisieren aus.	DevOps
Geben Sie einen Namen für den CloudFormation Stack ein.		DevOps
Geben Sie die Vorlage für die erste Region an.	Wählen Sie den regionssp ezifischen Paketnamen aus, der von gepackt CodeBuild und für die erste (primäre) Region in den S3-Bucket verschoben wurde.	DevOps
Geben Sie die Funktionen an.	Funktionen sind erforderl ich, wenn die Stack-Vorlage IAM-Ressourcen enthält oder wenn Sie einen Stack direkt aus einer Vorlage erstellen, die Makros enthält. Verwenden Sie für dieses Muster CAPABILITY_IAM, CAPABILITY_NAMED_IAM, CAPABILITY_AUTO_EX PAND.	DevOps

Bereitstellungsphase: Konfigurieren der Pipeline für die Bereitstellung in der zweiten Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die zweite Phase der Bereitstellungsphase hinzu.	Um eine Stufe für die zweite Region hinzuzufügen, bearbeiten Sie die Pipeline und wählen Sie in der Bereitstellungsphase Stufe hinzufügen aus. Wichtig: Der Prozess zum Erstellen der zweiten Region entspricht dem der ersten Region, mit Ausnahme der folgenden Werte.	DevOps
Geben Sie einen Aktionsnamen für die zweite Phase an.	Geben Sie einen eindeutigen Namen ein, der die zweite Phase und die zweite Region widerspiegelt.	DevOps
Konfigurieren Sie die Region für die zweite Phase.	Wählen Sie die zweite Region aus, in der Sie den Stack bereitstellen möchten.	DevOps
Geben Sie die Vorlage für die zweite Region an.	Wählen Sie den regionsspezifischen Paketnamen aus, der von verpackt CodeBuild und in den S3-Bucket für die zweite Region verschoben wurde.	DevOps

Bereitstellungsphase: Konfigurieren der Pipeline für die Bereitstellung in der dritten Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die dritte Phase der Bereitstellungsphase hinzu.	Um eine Stufe für die dritte Region hinzuzufügen, bearbeiten Sie die Pipeline und wählen Sie in der Bereitstellungsphase Stufe hinzufügen aus. Wichtig: Der Prozess zum Erstellen der zweiten Region ist derselbe wie der der beiden vorherigen Regionen, mit Ausnahme der folgenden Werte.	DevOps
Geben Sie einen Aktionsnamen für die dritte Stufe an.	Geben Sie einen eindeutigen Namen ein, der die dritte Phase und die dritte Region widerspiegelt.	DevOps
Konfigurieren Sie die Region für die dritte Stufe.	Wählen Sie die dritte Region aus, in der Sie den Stack bereitstellen möchten.	DevOps
Geben Sie die Vorlage für die dritte Region an.	Wählen Sie den regionsspezifischen Paketnamen aus, der von verpackt CodeBuild und in den S3-Bucket für die dritte Region verschoben wurde.	DevOps

Bereinigen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die AWS-Ressourcen.	Um die Bereitstellung zu bereinigen, löschen Sie die CloudFormation Stacks in jeder Region. Löschen Sie dann die CodePipeline Ressourcen CodeCommit CodeBuild, und aus der primären Region.	DevOps

Zugehörige Ressourcen

- Was ist AWS CodePipeline?
- AWS Serverless-Anwendungsmodell
- AWS CloudFormation
- AWS CloudFormation -Architekturstrukturreferenz für AWS CodePipeline

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Exportieren von AWS Backup-Berichten aus einer Organisation in AWS Organizations als CSV-Datei

Erstellt vonl Raj Jayarajan (AWS) und Purushotham G K (AWS)

Code-Repository: aws-backup-report-generator	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur
Workload: Alle anderen Workloads	AWS-Services: AWS Backup ;AWS Identity and Access Management ;AWS Lambda ;Amazon S3; Amazon EventBridge	

Übersicht

Dieses Muster zeigt, wie AWS Backup-Auftragsberichte aus einer Organisation in AWS Organizations als CSV-Datei exportiert werden. Die Lösung verwendet AWS Lambda und Amazon EventBridge , um AWS Backup-Auftragsberichte nach Status zu kategorisieren, was bei der Konfiguration von statusbasierten Automatisierungen helfen kann.

AWS Backup unterstützt Organisationen bei der zentralen Verwaltung und Automatisierung des Datenschutzes über AWS-Services, in der Cloud und On-Premises. Für AWS Backup-Aufträge, die in AWS Organizations konfiguriert sind, ist die konsolidierte Berichterstattung jedoch nur in der AWS-Managementkonsole des Verwaltungskontos jeder Organisation verfügbar. Wenn Sie diese Berichterstattung außerhalb des Verwaltungskontos platzieren, können Sie den Aufwand für die Prüfung reduzieren und den Umfang für Automatisierungen, Benachrichtigungen und Warnungen erhöhen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine aktive Organisation in AWS Organizations, die mindestens ein Verwaltungskonto und ein Mitgliedskonto enthält

- AWS Backup, konfiguriert auf Organisationsebene in AWS Organizations (weitere Informationen finden Sie unter Automatisieren zentralisierter Backups in großem Umfang über AWS-Services hinweg mithilfe von AWS Backup im AWS Blog)
- Git , auf Ihrem lokalen Computer installiert und konfiguriert

Einschränkungen

Die in diesem Muster bereitgestellte Lösung identifiziert AWS-Ressourcen, die nur für AWS Backup-Aufträge konfiguriert sind. Der Bericht kann keine AWS-Ressourcen identifizieren, die nicht für die Sicherung über AWS Backup konfiguriert sind.

Architektur

Zieltechnologie-Stack

- AWS Backup
- AWS CloudFormation
- Amazon EventBridge
- AWS Lambda
- AWS Security Token Service (AWS STS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für den Export von AWS Backup-Auftragsberichten aus einer Organisation in AWS Organizations als CSV-Datei.

Das Diagramm zeigt den folgenden Workflow:

1. Eine Regel für geplante EventBridge Ereignisse ruft eine Lambda-Funktion im AWS-Mitgliedskonto (Berichterstellung) auf.
2. Die Lambda-Funktion verwendet dann AWS STS, um eine IAM-Rolle anzunehmen, die über die erforderlichen Berechtigungen zum Herstellen einer Verbindung mit dem Verwaltungskonto verfügt.

3. Die Lambda-Funktion führt dann Folgendes aus:

- Fordert den Bericht über konsolidierte AWS Backup-Aufträge vom AWS Backup-Service an
- Kategorisiert die Ergebnisse basierend auf dem AWS Backup-Auftragsstatus
- Konvertiert die Antwort in eine CSV-Datei
- Lädt die Ergebnisse in einen Amazon S3-Bucket im Berichtskonto in Ordnern hoch, die basierend auf ihrem Erstellungsdatum gekennzeichnet sind

Tools

Tools

- AWS Backup ist ein vollständig verwalteter Service, der Sie bei der Zentralisierung und Automatisierung des Datenschutzes über AWS-Services, in der Cloud und On-Premises unterstützt.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Code für dieses Muster ist im GitHub aws-backup-report-generatorRepository verfügbar.

Bewährte Methoden

- Bewährte Methoden für die Sicherheit in Amazon S3 (Amazon S3-Benutzerhandbuch)
- Bewährte Methoden für die Arbeit mit AWS Lambda-Funktionen (AWS Lambda-Entwicklerhandbuch)
- Bewährte Methoden für das Verwaltungskonto (Benutzerhandbuch für AWS Organizations)

Sekunden

Bereitstellen der Lösungskomponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub aws-backup-report-generator Repository, indem Sie den folgenden Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/aws-backup-report-generator.git` Weitere Informationen finden Sie unter Klonen eines Repositorys in den - GitHub Dokumenten.	AWS DevOps, DevOps Techniker
Stellen Sie die Lösungskomponenten im AWS-Mitgliedskonto (Berichterstellung) bereit.	1. Melden Sie sich im Mitgliedskonto (Berichterstellung) bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole . 2. Wählen Sie Create stack (Stack erstellen) und	DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann With new resources (standard) (Mit neuen Ressourcen (Standard)). 3. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen aus. 4. Wählen Sie Datei auswählen aus. Navigieren Sie dann zum Stammordner des geklonten GitHub Repositorys auf Ihrer lokalen Workstation und wählen Sie template-reporting.yaml aus. 5. Wählen Sie Öffnen und dann Weiter aus. 6. Geben Sie auf der Seite Stack-Details angeben für Stack-Name einen Namen für Ihren CloudFormation Stack ein. 7. Geben Sie für ManagementAccountID die AWS-Konto-ID für das Verwaltungskonto Ihrer Organisation in AWS Organizations ein. 8. Wählen Sie Weiter aus. 9. Wählen Sie auf der Seite Stack-Optionen konfigurieren die Option Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Aktivieren Sie auf der Seite Überprüfen das Kontrollkästchen, um zu bestätigen, dass Sie die Konfiguration überprüft haben. 11. Wählen Sie Stack erstellen aus. Der Stack zeigt den Status CREATE_COMPLETE an, wenn die Lösungskomponenten im Mitgliedskonto (Bericht) bereitgestellt werden.	

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die EventBridge Regel vor dem Testen ausgeführt wird.	Stellen Sie sicher, dass die EventBridge Regel ausgeführt wird, indem Sie mindestens 24 Stunden warten oder die Berichtshäufigkeit in der template-reporting.yml-Datei der CloudFormation Vorlage erhöhen. So erhöhen Sie die Berichtshäufigkeit 1. Öffnen Sie die Datei template-reporting.yml im geklonten Repository. 2. Suchen Sie in der Ereignisregel mit der	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	logischen ID LambdaSch edule„ScheduleExpression“. 3. Bearbeiten Sie den SchlüsselScheduleE xpression so, dass er einen gültigen Cron-Ausd ruck enthält. Mit dem folgenden Cron-Ausdruck wird beispielsweise die Ausführung der Ereignisr egel alle fünf Minuten geplant: `“cron (* /5 * * * *)”`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Amazon S3-Bucket auf den generierten Bericht.	1. Melden Sie sich im Mitgliedskonto (Berichterstattung) bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole . 2. Wählen Sie im Bereich Stacks den Namen des Stacks aus, den Sie erstellt haben. Wählen Sie dann die Registerkarte Ressourcen aus. 3. Suchen Sie im Bereich Ressourcen in der Spalte Logische ID nach BackupReportS3Bucket . Öffnen Sie dann den zugehörigen Amazon S3-Bucket in einer neuen Registerkarte, indem Sie den Link in der Spalte Physische ID neben dieser logischen ID auswählen. 4. Stellen Sie sicher, dass der Bucket einen Bericht enthält, der im folgenden Format generiert wird: BackupReports/<yyyy>/<mm>/<dd>/BackupReport-<BACKUP JOB STATUS>-<dd>-<Mon>-<yyy>.csv	AWS DevOps, DevOps Techniker

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Lösungskomponenten aus dem Mitgliedskonto (Berichtskonto).	1. Öffnen Sie im Mitgliedskonto (Berichterstattung) den Amazon S3-Bucket der Lösung. Anweisungen finden Sie in den Schritten 2-4 im Abschnitt Lösung testen dieses Musters im S3-Bucket auf die generierte Berichtshistorie überprüfen. 2. Löschen Sie den Inhalt des Buckets und leeren Sie den Bucket. Anweisungen finden Sie unter Leeren eines Buckets im Amazon S3-Benutzerhandbuch. 3. Melden Sie sich im Mitgliedskonto (Berichterstattung) bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole . 4. Aktivieren Sie im Bereich Stacks das Kontrollkästchen neben dem Namen des von Ihnen erstellten Stacks. Wählen Sie dann Löschen aus.	AWS DevOps, DevOps Techniker
Löschen Sie die Lösungskomponenten aus dem Verwaltungskonto.	1. Melden Sie sich im Verwaltungskonto bei der AWS-Managementkonsole	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an und öffnen Sie dann die CloudFormation Konsole . 2. Aktivieren Sie im Bereich Stacks das Kontrollk ästchen neben dem Namen des von Ihnen erstellten Stacks. Wählen Sie dann Löschen aus.	

Zugehörige Ressourcen

- Tutorial: Verwenden von AWS Lambda mit geplanten Ereignissen (AWS Lambda-Dokumentation)
- Erstellen geplanter Ereignisse zum Ausführen von AWS Lambda-Funktionen (AWS SDK for JavaScript documentation)
- IAM-Tutorial: Delegieren des Zugriffs in allen AWS-Konten mithilfe von IAM-Rollen (IAM-Dokumentation)
- Terminologie und Konzepte von AWS Organizations (Dokumentation zu AWS Organizations)
- Erstellen von Berichtsplänen mit der AWS Backup-Konsole (AWS Backup-Dokumentation)
- Erstellen eines Auditberichts (AWS Backup-Dokumentation)
- Erstellen von On-Demand-Berichten (AWS BackupDokumentation)
- Was ist AWS Backup? (Dokumentation zu AWS Backup)
- Automatisieren Sie zentralisierte Backups in großem Umfang über AWS-Services hinweg mithilfe von AWS Backup (AWS-Blogbeitrag)

Exportieren von Tags für eine Liste von Amazon EC2-Instances in eine CSV-Datei

Erstellt von S Ju (AWS) und Pac Joonhyun (AWS)

Code-Repository: ECEC2-Tags suchen und exportieren	Umgebung: Produktion	Technologien: DevOps
AWS-Services: Amazon EC2		

Übersicht

Dieses Muster zeigt, wie Sie Tags für eine Liste von Amazon Elastic Compute Cloud (Amazon EC2)-Instances programmgesteuert in eine CSV-Datei exportieren.

Mithilfe des bereitgestellten Python-Beispielskripts können Sie reduzieren, wie lange es dauert, Ihre Amazon EC2-Instances nach bestimmten Tags zu überprüfen und zu kategorisieren. Sie könnten beispielsweise das Skript verwenden, um schnell eine Liste von Instances zu identifizieren und zu kategorisieren, die Ihr Sicherheitsteam für Softwareupdates markiert hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Python 3 installiert und konfiguriert
- AWS Command Line Interface (AWS CLI) installiert und konfiguriert

Einschränkungen

Das in diesem Muster bereitgestellte Python-Beispielskript kann Amazon EC2-Instances nur anhand der folgenden Attribute durchsuchen:

- Instance-IDs
- Private IPv4-Adressen
- Öffentliche IPv4-Adressen

Tools

- Python ist eine Allzweck-Computer-Programmiersprache.
- virtualenv hilft Ihnen, isolierte Python-Umgebungen zu erstellen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Code-Repository

Das Python-Beispielskript für dieses Muster ist im GitHub search-ec2-instances-export-tags-Repository verfügbar.

Polen

Installieren und Konfigurieren der Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Hinweis: Wenn Sie beim Ausführen von AWS CLI-Befehlen Fehler erhalten, stellen Sie sicher, dass Sie die neueste AWS CLI-Version verwenden. Klonen Sie das GitHub search-ec2-instances-export-tagsRepository, indem Sie den folgenden Git-Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/search-ec2-instances-export-tags.git`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren und aktivieren Sie virtualenv.	1. Installieren Sie virtualenv, indem Sie den folgenden Befehl ausführen:
	`python3 -m pip install virtualenv`
	2. Erstellen Sie eine neue virtuelle Umgebung, indem Sie den folgenden Befehl ausführen:
	`python3 -m venv env`
	3. Aktivieren Sie die neue virtuelle Umgebung, indem Sie den folgenden Befehl ausführen:
	`source env/bin/activate`
	Weitere Informationen finden Sie im Virtualenv-Benutzerhandbuch.
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Abhängigkeiten.	1. Öffnen Sie das Codeverzeichnis, indem Sie den folgenden Befehl im Terminal ausführen:
	`cd search-ec2-instances-export-tags`
	2. Installieren Sie die `requirements.txt` Datei, indem Sie den folgenden pip-Befehl ausführen:
	`pip3 install -r requirements.txt`
		DevOps Techniker

Konfigurieren Sie ein benanntes AWS-Profil.	Falls noch nicht geschehen, konfigurieren Sie ein AWS-Namensprofil, das die erforderlichen Anmeldeinformationen für die Ausführung des Skripts enthält. Um ein benanntes Profil zu erstellen, führen Sie den Befehl aws configure aus. Weitere Informationen finden Sie unter Verwenden benannter Profile in der AWS CLI-Dokumentation.	DevOps Techniker

Konfigurieren und Ausführen des Python-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Eingabedatei.	Erstellen Sie eine Eingabedatei, die eine Liste der Amazon EC2-Instances enthält, nach denen das Skript Tags suchen und exportieren soll. Sie können Instance-IDs , private IPv4-Adressen oder öffentliche IPv4-Adressen auflisten.
	
	Wichtig: Stellen Sie sicher, dass jede Amazon EC2-Instance in der Eingabedatei in einer eigenen Zeile aufgeführt ist.
	
	Beispiel für eine Eingabedatei
	
	`1 i-0547c351bdfe85b9f`
	`2 54.157.194.156`
	`3 172.31.85.33`
	`4 54.165.198.144`
	`5 i-0b6223b5914111a4b`
	`6 172.31.85.44`
	`7 54.165.198.145`
	`8 172.31.80.219`
	`9 172.31.94.199`
		DevOps Techniker

Führen Sie das Python-Skript aus.	Führen Sie das Skript aus, indem Sie den folgenden Befehl im Terminal ausführen: `python search_instances.py -i`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`INPUTFILE -o OUTPUTFIL E -r REGION [-p PROFILE]`
	
	Hinweis: Ersetzen Sie `INPUTFILE` durch den Namen Ihrer Eingabeda tei. Ersetzen Sie durch `OUTPUTFILE` den Namen, den Sie der CSV-Ausga bedatei geben möchten. Ersetzen Sie durch `REGION` die AWS-Region, in der sich Ihre Amazon EC2-Resso urcen befinden. Wenn Sie ein benanntes AWS-Profi l verwenden, ersetzen Sie durch `PROFILE` das benannte Profil, das Sie verwenden.
	
	Führen Sie den folgenden Befehl aus, um eine Liste der unterstützten Parameter und deren Beschreibung abzurufen :
	
	`python search_in stances.py -h`
	
	Weitere Informationen und ein Beispiel für eine Ausgabedatei finden Sie in der `README.md` Datei im GitHub search-ec2-instances-export-tags-Repository.	

Zugehörige Ressourcen

- Konfigurieren der AWS CLI (AWS CLI-Benutzerhandbuch)

Generieren einer AWS- CloudFormation Vorlage mit verwalteten AWS Config-Regeln mithilfe vonoSphere

Erstellt von Lucas Nation (AWS) und Freddie Bol (AWS)

Umgebung: Produktion	Technologien: DevOps; Management und Governanc e; Sicherheit, Identität, Compliance	Workload: Microsoft; Open-Source
AWS-Services: AWS Config; AWS CloudFormation		

Übersicht

Viele Organisationen verwenden von AWS Config verwaltete Regeln, um die Compliance ihrer Amazon Web Services (AWS)-Ressourcen anhand gängiger bewährter Methoden zu bewerten. Diese Regeln können jedoch zeitaufwändig sein, und dieses Muster hilft Ihnen dabei,oSphere , eine Python-Bibliothek, zu nutzen, um verwaltete AWS Config-Regeln zu generieren und zu verwalten.

Das Muster hilft Ihnen bei der Verwaltung Ihrer verwalteten AWS Config-Regeln, indem Sie ein Python-Skript verwenden, um eine Microsoft Excel-Tabelle mit von AWS verwalteten Regeln in eine AWS- CloudFormation Vorlage zu konvertieren. BoloSphere fungiert als Infrastructure as Code (IaC), was bedeutet, dass Sie die Excel-Tabelle mit verwalteten Regeln aktualisieren können, anstatt eine Datei im JSON- oder YAML-Format zu verwenden. Anschließend verwenden Sie die Vorlage, um einen AWS- CloudFormation Stack zu starten, der die verwalteten Regeln in Ihrem AWS-Konto erstellt und aktualisiert.

Die AWS- CloudFormation Vorlage definiert jede verwaltete AWS Config-Regel mithilfe der Excel-Tabelle und hilft Ihnen, das manuelle Erstellen einzelner Regeln in der AWS-Managementkonsole zu vermeiden. Das Skript verwendet standardmäßig die Parameter jeder verwalteten Regel auf ein leeres Wörterbuch und die `ComplianceResourceTypes` Standardwerte des Bereichs von `THE_RULE_IDENTIFIER.template file`. Weitere Informationen zur Regel-ID finden Sie unter Erstellen von verwalteten AWS Config-Regeln mit AWS- CloudFormation Vorlagen in der AWS Config-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vertrautheit mit der Verwendung von AWS- CloudFormation Vorlagen zum Erstellen von verwalteten AWS Config-Regeln. Weitere Informationen dazu finden Sie unter Erstellen von verwalteten AWS Config-Regeln mit AWS- CloudFormation Vorlagen in der AWS Config-Dokumentation.
- Python 3, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Python-Dokumentation.
- Eine vorhandene integrierte Entwicklungsumgebung (IDE) wie AWS Cloud9. Weitere Informationen dazu finden Sie unter Was ist AWS Cloud9? in der AWS Cloud9-Dokumentation.
- Identifizieren Sie Ihre Organisationseinheiten (OUs) in einer Spalte in der `excel_config_rules.xlsx` Excel-Beispieltabelle (angefügt).

Polen

Anpassen und Konfigurieren der verwalteten AWS Config-Regeln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Excel-Beispieltabelle.	Laden Sie die `excel_config_rules.xlsx` Excel-Beispieltabelle (angefügt) herunter und kennzeichnen Sie sie als `Implemented` die von AWS Config verwalteten Regeln, die Sie verwenden möchten. Als markierte Regeln `Implemented` werden der AWS- CloudFormation Vorlage hinzugefügt.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Aktualisieren Sie die Datei config_rules_params.json mit AWS Config-Regelparametern.	Einige von AWS Config verwaltete Regeln erfordern Parameter und sollten mithilfe der `--param-file` Option als JSON-Datei an das Python-Skript übergeben werden. Die `access-keys-rotated` verwaltete Regel verwendet beispielsweise den folgenden `maxAccessKeyAge` Parameter: `{ "access-keys-rotated": { "InputParameters": { "maxAccessKeyAge": 90 } } }` In diesem Beispielparameter `maxAccessKeyAge` ist auf 90 Tage festgelegt. Das Skript liest die Parameterdatei und fügt alle hinzu`InputParameters`, die es findet.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Aktualisieren Sie die Datei config_rules_params.json mit AWS Config ComplianceResourceTypes .	Standardmäßig ruft das Python-Skript die `ComplianceResourceTypes` aus von AWS definierten Vorlagen ab. Wenn Sie den Geltungsbereich einer bestimmten verwalteten AWS Config-Regel überschreiben möchten, müssen Sie sie mithilfe der `--param-file` Option als JSON-Datei an das Python-Skript übergeben. Der folgende Beispielcode zeigt beispielsweise, wie `ComplianceResourceTypes` für auf die `["AWS::EC2::Volume"]` Liste gesetzt `ec2-volume-inuse-check` ist: `{ "ec2-volume-inuse-check": { "Scope": { "ComplianceResourceTypes": [ "AWS::EC2::Volume" ] } } }`	Developer

Ausführen des Python-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die pip-Pakete aus der Datei requirements.txt.	Laden Sie die `requirements.txt` Datei (angefügt) herunter und führen Sie den folgenden Befehl in Ihrer IDE aus, um die Python-Pakete zu installieren: `pip3 install -r requirements.txt`	Developer
Führen Sie das Python-Skript aus.	1. Laden Sie die `aws_config_rules.py` Datei (angefügt) auf Ihren lokalen Computer herunter. 2. Führen Sie den Befehl `python3 aws_config_rules.py --ou <OU_NAME>` aus. Hinweis: `--ou` definiert, welche OU-Spalte in der Excel-Tabelle ausgewählt werden soll. Sie können auch die folgenden optionalen Parameter hinzufügen: • `--config-rule-option` – Definiert die Regeln, die aus der Excel-Tabelle ausgewählt werden sollen. Der Standardwert ist der `-Implemented` Parameter.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `--excel-file` – Der Pfad für die Excel-Tabelle. Der Standardwert ist `aws_config_rules.xlsx` . • `--param-file` – Der Pfad der Parameter-JSON-Datei. Der Standardwert ist `config_rules_params.json` . • `--max-execution-frequency` – Definiert, wie oft die von AWS Config verwalteten Regeln ausgewertet werden. Die Optionen sind `One_Hour`, `Three_Hours` , `Six_Hours` `Twelve_Hours` , oder `TwentyFour_Hours` . Der Standardwert ist `TwentyFour_Hours` .	

Bereitstellen der verwalteten AWS Config-Regeln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den AWS-CloudFormation Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS-CloudFormation Konsole und wählen Sie dann Stack erstellen aus.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Seite Vorlage angeben die Option Vorlagendatei hochladen und laden Sie dann Ihre AWS- CloudFormation Vorlage hoch. 3. Geben Sie einen Stack-Namen an und wählen Sie dann Weiter aus. 4. Geben Sie Tags an und wählen Sie dann Weiter aus. 5. Wählen Sie Stack erstellen aus.	

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Gewähren Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto

Erstellt von Helge Aufderheide (AWS)

Umgebung: Produktion	Technologien: DevOps; Analytik; Machine Learning und KI; Management und Governance	AWS-Services: AWS CodeCommit; AWS Identity and Access Management ; Amazon SageMaker

Übersicht

Dieses Muster zeigt, wie Sie Amazon- SageMaker Notebook-Instances und -Benutzern temporären Zugriff auf ein AWS- CodeCommit Repository gewähren, das sich in einem anderen AWS-Konto befindet. Dieses Muster zeigt auch, wie Sie detaillierte Berechtigungen für bestimmte Aktionen erteilen können, die jede Entität für jedes Repository ausführen kann.

Organisationen speichern CodeCommit Repositorys häufig in einem anderen AWS-Konto als dem Konto, das ihre Entwicklungsumgebung hostet. Diese Einrichtung für mehrere Konten hilft bei der Kontrolle des Zugriffs auf die Repositorys und reduziert das Risiko einer versehentlichen Löschung. Um diese kontoübergreifenden Berechtigungen zu erteilen, empfiehlt es sich, AWS Identity and Access Management (IAM)-Rollen zu verwenden. Anschließend können vordefinierte IAM-Identitäten in jedem AWS-Konto die Rollen vorübergehend übernehmen, um eine kontrollierte Vertrauenskette für alle Konten zu erstellen.

Hinweis: Sie können ein ähnliches Verfahren anwenden, um anderen IAM-Identitäten kontoübergreifenden Zugriff auf ein CodeCommit Repository zu gewähren. Weitere Informationen finden Sie unter Konfigurieren des kontoübergreifenden Zugriffs auf ein AWS- CodeCommit Repository mithilfe von Rollen im AWS- CodeCommit Benutzerhandbuch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einem CodeCommit Repository (Konto A)

- Ein zweites aktives AWS-Konto mit einer SageMaker Notebook-Instance (Konto B)
- Ein AWS-Benutzer mit ausreichenden Berechtigungen zum Erstellen und Ändern von IAM-Rollen in Konto A
- Ein zweiter AWS-Benutzer mit ausreichenden Berechtigungen zum Erstellen und Ändern von IAM-Rollen in Konto B

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow zum Gewähren von kontoübergreifendem Zugriff auf ein CodeCommit Repository für eine SageMaker Notebook-Instance und Benutzer in einem AWS-Konto:

Das Diagramm zeigt den folgenden Workflow:

1. Die AWS-Benutzerrolle und die SageMaker Notebook-Instance-Rolle in Konto B übernehmen ein benanntes Profil .
2. Die Berechtigungsrichtlinie des benannten Profils gibt eine CodeCommit Zugriffsrolle in Konto A an, die das Profil dann annimmt.
3. Die Vertrauensrichtlinie der CodeCommit Zugriffsrolle in Konto A ermöglicht es dem benannten Profil in Konto B, die CodeCommit Zugriffsrolle zu übernehmen.
4. Die IAM-Berechtigungsrichtlinie des CodeCommit Repositorys in Konto A ermöglicht der CodeCommit Zugriffsrolle den Zugriff auf das CodeCommit Repository.

Technologie-Stack

- CodeCommit
- Git
- IAM
- pip
- SageMaker

Tools

- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- Git ist ein verteiltes Versionskontrollsystem zur Verfolgung von Änderungen am Quellcode während der Softwareentwicklung.
- git-remote-codecommit ist ein Dienstprogramm, mit dem Sie Code aus CodeCommit Repositorys pushen und abrufen können, indem Sie Git erweitern.
- pip ist das Paketinstallationsprogramm für Python. Sie können pip verwenden, um Pakete aus dem Python-Paketindex und anderen Indizes zu installieren.

Bewährte Methoden

Wenn Sie Berechtigungen mit IAM-Richtlinien festlegen, stellen Sie sicher, dass Sie nur die Berechtigungen erteilen, die zum Ausführen einer Aufgabe erforderlich sind. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Stellen Sie bei der Implementierung dieses Musters sicher, dass Sie Folgendes tun:

- Vergewissern Sie sich, dass die IAM-Prinzipien nur über die Berechtigungen verfügen, die für die Durchführung bestimmter, erforderlicher Aktionen in jedem Repository erforderlich sind. Es wird beispielsweise empfohlen, genehmigten IAM-Prinzipien zu erlauben, Änderungen an bestimmte Repository-Verzweigungen zu übertragen und zusammenzuführen, aber nur die Zusammenführung von Anforderungen an geschützte Verzweigungen anzufordern.
- Vergewissern Sie sich, dass IAM-Prinzipien je nach ihren jeweiligen Rollen und Verantwortlichkeiten für jedes Projekt unterschiedliche IAM-Rollen zugewiesen werden. Beispielsweise hat ein Entwickler andere Zugriffsberechtigungen als ein Release Manager oder AWS Administrator.

Polen

Konfigurieren der IAM-Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die CodeCommit Zugriffsrolle und die Berechtigungsrichtlinie.	Hinweis: Um den in diesem Epic dokumentierten manuellen Einrichtungsprozess zu automatisieren, können Sie eine AWS- CloudFormation Vorlage verwenden. Gehen Sie in dem Konto, das das CodeCommit Repository enthält (Konto A), wie folgt vor: 1. Erstellen Sie eine IAM-Rolle, die von der SageMaker Notebook-Instance-Rolle in Konto B übernommen werden kann. 2. Erstellen Sie eine IAM-Richtlinie, die Zugriff auf das Repository gewährt, und fügen Sie die Richtlinie an die Rolle an. Wählen Sie nur zu Testzwecken die von AWSCodeCommitPowerUser AWS verwaltete Richtlinie aus. Diese Richtlinie gewährt alle CodeCommit Berechtigungen mit Ausnahme der Möglichkeit, Ressourcen zu löschen.	Allgemeines AWS, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Ändern Sie die Vertrauen srichtlinie der Rolle so, dass Konto B als vertrauen swürdige Entität aufgeführt wird. Wichtig: Bevor Sie dieses Setup in Ihre Produktio nsumgebung verschieben, empfiehlt es sich, Ihre eigene IAM-Richtlinie zu schreiben, die die geringsten Berechtig ungen anwendet. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informati onen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erteilen Sie der Rolle der SageMaker Notebook-Instance in Konto B Berechtigungen, um die CodeCommit Zugriffsrolle in Konto A zu übernehmen.	Gehen Sie in dem Konto, das die IAM-Rolle der SageMaker Notebook-Instance enthält (Konto B), wie folgt vor: 1. Erstellen Sie eine IAM-Richtlinie, die es einer IAM-Rolle oder einem IAM-Benutzer ermöglicht, die CodeCommit Zugriffsrolle in Konto A zu übernehmen. Beispiel für eine IAM-Berechtigungsrichtlinie, die es einer IAM-Rolle oder einem Benutzer ermöglicht, eine kontoübergreifende Rolle zu übernehmen `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam:::accountA_ID:role/accountArole_ID" } }` 2. Hängen Sie die Richtlinie an die Rolle Ihrer	Allgemeines AWS, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SageMaker Notebook-Instance in Konto B an. 3. Lassen Sie die Rolle der SageMaker Notebook-Instance in Konto B die CodeCommit Zugriffsrolle in Konto A übernehmen. Hinweis: Informationen zum Anzeigen des Amazon-Ressourcennamens (ARN) Ihres Repositorys finden Sie unter Anzeigen von CodeCommit Repository-Details im AWS CodeCommit -Benutzerhandbuch.	

Einrichten Ihrer SageMaker Notebook-Instance in Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie ein Benutzerprofil auf der AWS SageMaker -Notebook-Instance ein, um die Rolle in Konto A zu übernehmen.	Wichtig: Stellen Sie sicher, dass Sie die neueste Version der AWS Command Line Interface (AWS CLI) installiert haben. Gehen Sie in dem Konto, das die SageMaker Notebook-Instance enthält (Konto B), wie folgt vor: 1. Melden Sie sich bei der AWS-Managementkons	Allgemeines AWS, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ole an und öffnen Sie die SageMaker -Konsole.
	2. Greifen Sie auf Ihre SageMaker Notebook-Instance zu. Die Jupyter-Schnittstelle wird geöffnet.
	3. Wählen Sie Neu und dann Terminal aus. In Ihrer Jupyter-Umgebung wird ein neues Terminalfenster geöffnet.
	4. Navigieren Sie zur ~/.aws/config-Datei der SageMaker Notebook-Instance. Fügen Sie der Datei dann ein Benutzerprofil hinzu, indem Sie die folgende Anweisung eingeben:
	
	`------.aws/config-`
	`-------------`
	`[profile remoterep`
	`ouser]`
	`role_arn = arn:aws:i`
	`am::<ID of Account`
	` A>:role/<rolename>`
	`role_session_name =`
	` remoteaccesssession`
	`region = eu-west-1`
	`credential_source  =`
	` Ec2InstanceMetadata`
	`----------------`
	`------------------`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das git-remote-codecommit Dienstprogramm .	Folgen Sie den Anweisungen in Schritt 2: Installieren git-remote-codecommit von im AWS- CodeCommit Benutzerhandbuch.	Data Scientist

Zugriff auf das Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie mit den Git-Befehlen oder auf das CodeCommit Repository zu SageMaker.	So verwenden Sie Git IAM-Prinzipale, die die Rolle der SageMaker Notebook-Instance in Konto B übernehmen, können jetzt Git-Befehle ausführen`git pull`, um auf das CodeCommit Repository in Konto A zuzugreifen. Benutzer können beispielsweise Befehle wie `git clone`, und ausführen `git push`. Anweisungen finden Sie unter Herstellen einer Verbindung mit einem AWS-CodeCommit Repository im AWS- CodeCommit Benutzerhandbuch. Informationen zur Verwendung von Git mit CodeCommitfinden Sie unter Erste Schritte mit AWS CodeCommit im	Git, Bash-Konsole

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS- CodeCommit Benutzerhandbuch. So verwenden Sie SageMaker Um Git von der SageMaker Konsole aus verwenden zu können, müssen Sie Git erlauben, Anmeldeinformationen aus Ihrem CodeCommit Repository abzurufen. Anweisungen finden Sie unter Zuordnen eines CodeCommit Repositorys in einem anderen AWS-Konto zu einer Notebook-Instance in der - SageMaker Dokumentation.	

Zugehörige Ressourcen

- Konfigurieren des kontoübergreifenden Zugriffs auf ein AWS- CodeCommit Repository mithilfe von Rollen (AWS- CodeCommit Dokumentation)
- IAM-Tutorial: Delegieren des Zugriffs in allen AWS-Konten mithilfe von IAM-Rollen (IAM-Dokumentation)

Zusätzliche Informationen

Beschränken von CodeCommit Berechtigungen auf bestimmte Aktionen

Um die Aktionen einzuschränken, die ein IAM-Prinzipal im CodeCommit Repository ausführen kann, ändern Sie die Aktionen, die in der CodeCommit Zugriffsrichtlinie zulässig sind.

Weitere Informationen zu CodeCommit API-Operationen finden Sie in der CodeCommit Berechtigungsreferenz im AWS- CodeCommit Benutzerhandbuch.

Hinweis: Sie können die von AWSCodeCommitPowerUser AWS verwaltete Richtlinie auch an Ihren Anwendungsfall anpassen.

Beschränken von CodeCommit Berechtigungen auf bestimmte Repositorys

Gehen Sie wie folgt vor, um eine Multi-Tenant-Umgebung zu erstellen, in der nur bestimmte Benutzer auf mehr als ein Code-Repository zugreifen können:

1. Erstellen Sie mehrere CodeCommit Zugriffsrollen in Konto A. Konfigurieren Sie dann die Vertrauensrichtlinie jeder Zugriffsrolle so, dass bestimmte Benutzer in Konto B die Rolle übernehmen können.
2. Schränken Sie ein, welche Code-Repositorys jede Rolle annehmen kann, indem Sie der Richtlinie jeder CodeCommit Zugriffsrolle eine „Ressourcen“-Bedingung hinzufügen.

Beispiel für eine „Ressourcen“-Bedingung, die den Zugriff eines IAM-Prinzipals auf ein bestimmtes CodeCommit Repository einschränkt

```
"Resource" : [<REPOSITORY_ARN>,<REPOSITORY_ARN> ]
```

Hinweis: Um mehrere Code-Repositorys in demselben AWS-Konto zu identifizieren und zu unterscheiden, können Sie den Namen der Repositorys unterschiedliche Präfixe zuweisen. Sie können beispielsweise Code-Repositorys mit Präfixen benennen, die auf verschiedene Entwicklergruppen wie myproject-subproject1-repo1 und myproject-subproject2-repo1 abgestimmt sind. Anschließend können Sie eine IAM-Rolle für jede Entwicklergruppe basierend auf ihren zugewiesenen Präfixen erstellen. Sie könnten beispielsweise eine Rolle namens myproject-subproject1-repoaccess erstellen und ihr Zugriff auf alle Code-Repositorys gewähren, die das Präfix myproject-subproject1 enthalten.

Beispiel für eine „Ressourcen“-Bedingung, die sich auf einen Code-Repository-ARN bezieht, der ein bestimmtes Präfix enthält

```
"Resource" : arn:aws:codecommit:<region>:<account-id>:myproject-subproject1-*
```

Implementieren einer GitHub Flow-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten

Erstellt von Bol Stephens (AWS) und Abhilash Vinod (AWS)

Code-Repository: git-branching-strategies-for-multiaccount-devops	Umgebung: Produktion	Technologien: DevOps; Softwareentwicklung und -tests; Strategie mit mehreren Konten
AWS-Services: AWS CodeArtifact; AWS CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Übersicht

Bei der Verwaltung eines Quellcode-Repositorys wirken sich verschiedene Verzweigungsstrategien auf die Softwareentwicklungs- und Veröffentlichungsprozesse aus, die Entwicklungsteams verwenden. Beispiele für gängige Verzweigungsstrategien sind Trunk, GitHub Flow und Gitflow. Diese Strategien verwenden verschiedene Zweige, und die in jeder Umgebung durchgeführten Aktivitäten unterscheiden sich. Organisationen, die DevOps Prozesse implementieren, würden von einem visuellen Leitfaden profitieren, der ihnen hilft, die Unterschiede zwischen diesen Verzweigungsstrategien zu verstehen. Die Verwendung dieser Visualisierung in Ihrer Organisation hilft Entwicklungsteams dabei, ihre Arbeit aufeinander abzustimmen und die Organisationsstandards einzuhalten. Dieses Muster bietet diese Visualisierung und beschreibt den Prozess der Implementierung einer GitHub Flow-Verzweigungsstrategie in Ihrer Organisation.

Dieses Muster ist Teil einer Dokumentationsreihe zur Auswahl und Implementierung von DevOps Verzweigungsstrategien für Organisationen mit mehreren AWS-Konten. Diese Reihe soll Ihnen helfen, die richtige Strategie und bewährte Methoden von Anfang an anzuwenden, um Ihre Erfahrung in der Cloud zu optimieren. GitHub Flow ist nur eine mögliche Verzweigungsstrategie, die Ihr Unternehmen verwenden kann. Diese Dokumentationsreihe behandelt auch Trunk- und Gitflow-Verzweigungsmodelle. Wenn Sie dies noch nicht getan haben, empfehlen wir Ihnen, die Auswahl

einer Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten zu lesen, bevor Sie die Anleitungen in diesem Muster implementieren. Bitte verwenden Sie die gebotene Vorsicht, um die richtige Verzweigungsstrategie für Ihre Organisation auszuwählen.

Dieses Handbuch enthält ein Diagramm, das zeigt, wie eine Organisation die GitHub Flow-Strategie implementieren könnte. Es wird empfohlen, die AWS Well-Architected DevOps Guidance zu lesen, um bewährte Methoden zu überprüfen. Dieses Muster umfasst empfohlene Aufgaben, Schritte und Einschränkungen für jeden Schritt des DevOps Prozesses.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git, installiert . Dies wird als Quellcode-Repository-Tool verwendet.
- Draw.io, installiert . Diese Anwendung wird verwendet, um das Diagramm anzuzeigen und zu bearbeiten.

Architektur

Zielarchitektur

Das folgende Diagramm kann wie ein Punnett-Quader (Wikipedia) verwendet werden. Sie richten die Verzweigungen auf der vertikalen Achse mit den AWS Umgebungen auf der horizontalen Achse aus, um zu bestimmen, welche Aktionen in jedem Szenario ausgeführt werden sollen. Die Zahlen geben die Reihenfolge der Aktionen im Workflow an. Dieses Beispiel führt Sie von einem `feature` Zweig bis zur Bereitstellung in der Produktion.

Weitere Informationen zu den AWS-Konten, Umgebungen und Verzweigungen in einem GitHub Flow-Ansatz finden Sie unter Auswählen einer Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten.

Automatisierung und Skalierung

Continuous Integration and Continuous Delivery (CI/CD) ist der Prozess der Automatisierung des Lebenszyklus von Softwareversionen. Es automatisiert viele oder alle manuellen Prozesse, die traditionell erforderlich sind, um neuen Code von einem ersten Commit in die Produktion zu erhalten. Eine CI/CD-Pipeline umfasst die Sandbox-, Entwicklungs-, Test-, Staging- und Produktionsumgebungen. In jeder Umgebung stellt die CI/CD-Pipeline jede Infrastruktur

bereit, die zum Bereitstellen oder Testen des Codes erforderlich ist. Mithilfe von CI/CD können Entwicklungsteams Änderungen am Code vornehmen, die dann automatisch getestet und bereitgestellt werden. CI/CD-Pipelines bieten auch Governance und Integritätsschutz für Entwicklungsteams, indem sie Konsistenz, Standards, bewährte Methoden und minimale Akzeptanzstufen für die Annahme und Bereitstellung von Features durchsetzen. Weitere Informationen finden Sie unter Praktische kontinuierliche Integration und kontinuierliche Bereitstellung auf AWS.

AWS bietet eine Reihe von Entwicklerservices, die Sie bei der Erstellung von CI/CD-Pipelines unterstützen. Beispielsweise AWS CodePipelineist ein vollständig verwalteter kontinuierlicher Bereitstellungsservice, mit dem Sie Ihre Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturaktualisierungen automatisieren können. AWS CodeCommitist darauf ausgelegt, skalierbare Git-Repositorys sicher zu hosten und Quellcode zu AWS CodeBuildkompilieren, Tests durchzuführen und ready-to-deploy Softwarepakete zu erstellen. Weitere Informationen finden Sie unterEntwicklertools auf AWS.

Tools

AWS -Services und -Tools

AWS bietet eine Reihe von Entwicklerservices, mit denen Sie dieses Muster implementieren können:

- AWS CodeArtifact ist ein hoch skalierbarer, verwalteter Artefakt-Repository-Service, mit dem Sie Softwarepakete für die Anwendungsentwicklung speichern und freigeben können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen für Amazon Elastic Compute Cloud (Amazon EC2) oder On-Premises-Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS)-Services.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.

Andere Tools

- Draw.io Desktop ist eine Anwendung zum Erstellen von Flussdiagrammen und Diagrammen. Das Code-Repository enthält Vorlagen im Drawio-Format für Draw.io.
- Bolma ist ein Online-Design-Tool, das für die Zusammenarbeit entwickelt wurde. Das Code-Repository enthält Vorlagen im .fig-Format für Bolma.

Code-Repository

Diese Quelldatei für das Diagramm in diesem Muster ist im Repository GitHub Git Branching Strategy for GitHub Flow verfügbar. Sie enthält Dateien in den Formaten PNG, draw.io undma. Sie können diese Diagramme ändern, um die Prozesse Ihrer Organisation zu unterstützen.

Bewährte Methoden

Folgen Sie den bewährten Methoden und Empfehlungen in AWS Well-Architected DevOps Guidance und wählen Sie eine Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten aus. Diese helfen Ihnen dabei, die GitHub Flow-basierte Entwicklung effektiv zu implementieren, die Zusammenarbeit zu fördern, die Codequalität zu verbessern und den Entwicklungsprozess zu optimieren.

Sekunden

Überprüfen der GitHub Flow-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Standard-GitHub Flow-Prozess.	1. In der Sandbox-Umgebung erstellt der Entwickler einen `feature` Zweig aus dem `main` Zweig und verwendet das Benennungsmuster `feature/<ticket>_<initials>_<short description>` . 2. Der Entwickler fügt dem `feature` Zweig einen oder mehrere Commits hinzu, die jeweils eine diskrete	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Änderung oder Verbesserung darstellen. 3. Der Entwickler öffnet eine Zusammenführungsanforderung (MR), um die Änderungen in der `main` Verzweigung zusammenzuführen. Dies initiiert einen Überprüfungsprozess. 4. Während des Überprüfungsprozesses besprechen Entwickler die Codeänderungen und geben Feedback. Ziel ist es, sicherzustellen, dass die Änderungen von hoher Qualität sind und den Standards des Projekts entsprechen. 5. Nachdem der Entwickler die Zusammenführungsanforderung erstellt hat, startet ein automatisierter Build-Prozess und stellt die Änderungen im `feature` Zweig in der Entwicklungsumgebung bereit. 6. Automatisierte Tests überprüfen die Integrität und Qualität der Änderungen, die in der Zusammenführungsanforderung gekapselt sind. Ein erfolgreicher Build, eine erfolgreiche	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung und erfolgreiche Tests sind erforderlich, um die Zusammenführungsanforderung abzuschließen. 7. Wenn der Überprüfungsprozess abgeschlossen ist, werden die Änderungen in der `main` Verzweigung zusammengeführt. 8. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Testumgebung manuell. 9. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Staging-Umgebung manuell. 10. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Produktionsumgebung manuell.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Bugfix-GitHub Flow-Prozess.	1. Der Entwickler erstellt einen `bugfix` Zweig aus dem `main` Zweig und verwendet das Benennungsmuster `bugfix/<ticket number>_<developer initials>_<descriptor>` . 2. Der Entwickler behebt das Problem, führt ein Commit für die Fehlerbehebung aus und erstellt die `bugfix` Verzweigung. 3. Der Entwickler öffnet eine Zusammenführungsanforderung, um den `bugfix` Zweig mit dem `main` Zweig zusammenzuführen. Dies initiiert einen Überprüfungsprozess. 4. Während des Überprüfungsprozesses besprechen Entwickler die Codeänderungen und geben Feedback. 5. Nach Abschluss der Überprüfung und Genehmigung schließt der Entwickler die Zusammenführungsanforderung der `bugfix` Verzweigung in die `main` Verzweigung ab.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in höheren Umgebungen manuell.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Hotfix-GitHub Flow-Prozess.	GitHub Flow ist darauf ausgelegt, eine kontinuierliche Bereitstellung zu ermöglich en, bei der Codeänder ungen häufig und zuverläss ig in höheren Umgebunge n bereitgestellt werden. Der Schlüssel ist, dass jeder `feature` Zweig jederzeit bereitstellbar ist. `Hotfix` Zweige, die den `bugfix` Zweigen `feature` oder ähnlich sind, können denselben Prozess wie einer dieser anderen Zweige verfolgen. Hotfixes haben jedoch aufgrund ihrer Wichtigkeit in der Regel eine höhere Priorität. Abhängig von den Richtlinien des Teams und der Unmittelbarkeit der Situation können bestimmte Schritte im Prozess beschleun igt werden. Codeüberp rüfungen für Hotfixes können beispielsweise schnell verfolgt werden. Während der Hotfix-Prozess den Feature- oder Bugfix-Prozess parallelisiert, kann die um Hotfixes herum liegende Wichtigkeit daher Änderungen an der prozedura len Einhaltung erfordern. Es ist wichtig, Richtlinien für	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Verwaltung von Hotfixes festzulegen, um sicherzus tellen, dass sie effizient und sicher verarbeitet werden.	

Fehlerbehebung

Problem	Lösung
Verzweigungskonflikte	Ein häufiges Problem, das beim GitHub Flow-Modell auftreten kann, besteht darin, dass ein Hotfix in der Produktion auftreten muss, aber eine entsprechende Änderung in einem `feature`-, - oder -`hotfix`Zweig erfolgen muss`bugfix`, in dem dieselben Ressourcen geändert werden. Wir empfehlen, Änderunge n von häufig `main` in niedrigere Zweige zusammenzuführen, um erhebliche Konflikte bei der Zusammenführung mit zu vermeiden `main`.
Reife des Teams	GitHub Flow fördert tägliche Bereitstellungen in höheren Umgebungen und unterstützt so die echte kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD). Es ist wichtig, dass das Team über die technische Reife verfügt, um Features zu erstellen und Automatisierungstests für sie zu erstellen. Das Team muss eine vollständige Überprüfung der Zusammenführungsanforderung durchführen, bevor die Änderungen genehmigt werden. Dies fördert eine robuste Entwicklungskultur, die Qualität, Rechenschaftspflicht und Effizienz im Entwicklungsprozess fördert.

Zugehörige Ressourcen

Dieser Leitfaden beinhaltet kein Training für Git. Wenn Sie dieses Training benötigen, stehen jedoch viele hochwertige Ressourcen im Internet zur Verfügung. Wir empfehlen Ihnen, mit der Git-Dokumentationsseite zu beginnen.

Die folgenden Ressourcen können Ihnen bei Ihrer GitHub Flow-Verzweigungsreise in der helfen AWS Cloud.

AWS DevOps Anleitung

- AWS DevOps Anleitung
- AWS Referenzarchitektur der Bereitstellungs-Pipeline
- Was ist DevOps?
- DevOps -Ressourcen

GitHub Flow-Anleitung

- GitHub Flow-Schnellstart-Tutorial (GitHub)
- Warum GitHub Flow?

Sonstige Ressourcen

- Methode zur Anwendung mit zwölf Faktoren (12factor.net)

Implementieren einer Gitflow-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten

Erstellt von Bol Stephens (AWS), Stephen DiCato (AWS), Tim Wondergem (AWS) und Abhilash Vinod (AWS)

Code-Repository: git-branching-strategies-for-multiaccount-devops	Umgebung: Produktion	Technologien: DevOps; Softwareentwicklung und -tests; Strategie mit mehreren Konten
AWS-Services: AWS CodeArtifact; AWS CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Übersicht

Bei der Verwaltung eines Quellcode-Repositorys wirken sich verschiedene Verzweigungsstrategien auf die Softwareentwicklungs- und Veröffentlichungsprozesse aus, die Entwicklungsteams verwenden. Beispiele für gängige Verzweigungsstrategien sind Trunk, Gitflow und GitHub Flow. Diese Strategien verwenden verschiedene Zweige, und die in jeder Umgebung durchgeführten Aktivitäten unterscheiden sich. Organisationen, die DevOps Prozesse implementieren, würden von einem visuellen Leitfaden profitieren, der ihnen hilft, die Unterschiede zwischen diesen Verzweigungsstrategien zu verstehen. Die Verwendung dieser Visualisierung in Ihrer Organisation hilft Entwicklungsteams dabei, ihre Arbeit aufeinander abzustimmen und die Organisationsstandards einzuhalten. Dieses Muster bietet diese Visualisierung und beschreibt den Prozess der Implementierung einer Gitflow-Verzweigungsstrategie in Ihrer Organisation.

Dieses Muster ist Teil einer Dokumentationsreihe zur Auswahl und Implementierung von DevOps Verzweigungsstrategien für Organisationen mit mehreren AWS-Konten. Diese Reihe soll Ihnen helfen, die richtige Strategie und bewährte Methoden von Anfang an anzuwenden, um Ihre Erfahrung in der Cloud zu optimieren. Gitflow ist nur eine mögliche Verzweigungsstrategie, die Ihr Unternehmen verwenden kann. Diese Dokumentationsreihe behandelt auch Trunk- und GitHub Flow-

Verzweigungsmodelle. Wenn Sie dies noch nicht getan haben, empfehlen wir Ihnen, die Auswahl einer Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten zu lesen, bevor Sie die Anleitungen in diesem Muster implementieren. Bitte verwenden Sie die gebotene Vorsicht, um die richtige Verzweigungsstrategie für Ihre Organisation auszuwählen.

Dieses Handbuch enthält ein Diagramm, das zeigt, wie eine Organisation die Gitflow-Strategie implementieren könnte. Es wird empfohlen, die AWS Well-Architected DevOps Guidance zu lesen, um bewährte Methoden zu überprüfen. Dieses Muster umfasst empfohlene Aufgaben, Schritte und Einschränkungen für jeden Schritt des DevOps Prozesses.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git, installiert . Dies wird als Quellcode-Repository-Tool verwendet.
- Draw.io, installiert . Diese Anwendung wird verwendet, um das Diagramm anzuzeigen und zu bearbeiten.
- (Optional) Gitflow-Plugin, installiert .

Architektur

Zielarchitektur

Das folgende Diagramm kann wie ein Punnett-Quader (Wikipedia) verwendet werden. Sie richten die Verzweigungen auf der vertikalen Achse mit den AWS Umgebungen auf der horizontalen Achse aus, um zu bestimmen, welche Aktionen in jedem Szenario ausgeführt werden sollen. Die Zahlen geben die Reihenfolge der Aktionen im Workflow an. In diesem Beispiel werden Sie von einem Feature-Zweig durch die Bereitstellung in der Produktion geführt.

Weitere Informationen zu AWS-Konten, Umgebungen und Verzweigungen in einem Gitflow-Ansatz finden Sie unter Auswählen einer Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten.

Automatisierung und Skalierung

Continuous Integration and Continuous Delivery (CI/CD) ist der Prozess der Automatisierung des Lebenszyklus von Softwareversionen. Es automatisiert viele oder alle manuellen Prozesse, die traditionell erforderlich sind, um neuen Code von einem ersten Commit in die Produktion

zu erhalten. Eine CI/CD-Pipeline umfasst die Sandbox-, Entwicklungs-, Test-, Staging- und Produktionsumgebungen. In jeder Umgebung stellt die CI/CD-Pipeline jede Infrastruktur bereit, die zum Bereitstellen oder Testen des Codes erforderlich ist. Mithilfe von CI/CD können Entwicklungsteams Änderungen am Code vornehmen, die dann automatisch getestet und bereitgestellt werden. CI/CD-Pipelines bieten auch Governance und Integritätsschutz für Entwicklungsteams, indem sie Konsistenz, Standards, bewährte Methoden und minimale Akzeptanzstufen für die Annahme und Bereitstellung von Features durchsetzen. Weitere Informationen finden Sie unter Praktische kontinuierliche Integration und kontinuierliche Bereitstellung auf AWS.

AWS bietet eine Suite von Entwicklerservices, die Sie beim Erstellen von CI/CD-Pipelines unterstützen. Beispielsweise AWS CodePipelineist ein vollständig verwalteter kontinuierlicher Bereitstellungsservice, mit dem Sie Ihre Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturaktualisierungen automatisieren können. AWS CodeCommitist darauf ausgelegt, skalierbare Git-Repositorys sicher zu hosten und Quellcode zu AWS CodeBuildkompilieren, Tests durchzuführen und ready-to-deploy Softwarepakete zu erstellen. Weitere Informationen finden Sie unterEntwicklertools auf AWS.

Tools

AWS -Services und -Tools

AWS bietet eine Reihe von Entwicklerservices, mit denen Sie dieses Muster implementieren können:

- AWS CodeArtifact ist ein hoch skalierbarer, verwalteter Artefakt-Repository-Service, mit dem Sie Softwarepakete für die Anwendungsentwicklung speichern und freigeben können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen für Amazon Elastic Compute Cloud (Amazon EC2) oder On-Premises-Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS)-Services.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.

Andere Tools

- Draw.io Desktop ist eine Anwendung zum Erstellen von Flussdiagrammen und Diagrammen. Das Code-Repository enthält Vorlagen im Drawio-Format für Draw.io.
- Bolma ist ein Online-Design-Tool, das für die Zusammenarbeit entwickelt wurde. Das Code-Repository enthält Vorlagen im .fig-Format fürma.
- (Optional) Das Gitflow-Plugin ist eine Sammlung von Git-Erweiterungen, die allgemeine Repository-Operationen für das Gitflow-Verzweigungsmodell bereitstellen.

Code-Repository

Diese Quelldatei für das Diagramm in diesem Muster ist im GitHub Repository Git Branching Strategy for GitFlow verfügbar. Sie enthält Dateien in den Formaten PNG, draw.io undma. Sie können diese Diagramme ändern, um die Prozesse Ihrer Organisation zu unterstützen.

Bewährte Methoden

Folgen Sie den bewährten Methoden und Empfehlungen in AWS Well-Architected DevOps Guidance und wählen Sie eine Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten aus. Diese helfen Ihnen, die Gitflow-basierte Entwicklung effektiv zu implementieren, die Zusammenarbeit zu fördern, die Codequalität zu verbessern und den Entwicklungsprozess zu optimieren.

Polen

Überprüfen der Gitflow-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Standard-Gitflow-Prozess.	1. In der Sandbox-Umgebung erstellt der Entwickler einen `feature` Zweig aus dem `develop` Zweig und verwendet das Benennung smuster `feature/<ticket>_<initials>_<short description>` .	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Der Entwickler entwickelt Code und stellt den Code iterativ in der Sandbox-U mgebung bereit, um das Ticket abzuschließen. Hinweis: Der Entwickle r kann optional einen `sandbox` Zweig erstellen , um eine automatisierte Build- oder Bereitste llungspipeline in der Sandbox-Umgebung auszuführen. 3. Der Entwickler erstellt mithilfe einer Squash-Zusammenführung eine Zusammenführungsan forderung von der `feature` Verzweigung in die `develop` Verzweigung. 4. Eine Pipeline für kontinuie rliche Integration und kontinuierliche Bereitste llung (CI/CD) erstellt und stellt den `develop` Zweig automatisch in der Entwicklungsumgebung bereit. 5. (Optional) Ein Entwickle r integriert zusätzliche `feature` Verzweigungen in den Entwicklerzweig,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bevor er mit den Veröffent lichungsaktivitäten fortfährt. 6. Wenn Sie bereit sind, die Funktionen in der `develop` Verzweigu ng zu veröffentlichen, erstellt der Entwickler eine `release` Verzweigung mit dem Namen `release/ v<number>` aus der `develop` Verzweigung. 7. Der Entwickler erstellt den Release-Zweig, der Artefakte zur Wiederver wendung in anderen Umgebungen veröffentlicht. 8. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Testumgebung manuell. 9. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Staging-Umgebung manuell. 10. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Produktionsumgebung manuell. 11. Der Entwickler führt den `release` Zweig in den `main` Zweig ein. Idealerweise verwendet der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Entwickler ein automatisiertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keine Squash-Zusammenführung. 12. Der Entwickler führt den `release` Zweig in den `develop` Zweig ein. Idealerweise verwendet der Entwickler ein automatisiertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keine Squash-Zusammenführung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Hotfix-Gitflow-Prozess.	1. Der Entwickler erstellt einen `hotfix` Zweig aus dem `main` Zweig und verwendet das Benennungsmuster `hotfix/<ticket>_<initials>_<short description>` . 2. Der Entwickler erstellt einen `release` Zweig aus dem `main` Zweig und benennt ihn `release/v<number>` . 3. Der Entwickler behebt das Problem, führt ein Commit für den Fehler aus und erstellt die `hotfix` Verzweigung. 4. Der Entwickler erstellt mithilfe einer Squash-Zusammenführung eine Zusammenführungsanforderung aus der `hotfix` Verzweigung in die `release/v<number>` Verzweigung. 5. Der Entwickler erstellt den `release` Zweig, der Artefakte zur Wiederverwendung in anderen Umgebungen veröffentlicht. 6. Ein Genehmiger genehmigt die Bereitstellung der	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Release-Artefakte in der Testumgebung manuell. 7. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Staging-Umgebung manuell. 8. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Produktionsumgebung manuell. 9. Der Entwickler führt den `release` Zweig in den `main` Zweig ein. Idealerweise verwendet der Entwickler ein automatis iertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keine Squash-Zu sammenführung. 10. Der Entwickler führt den `release` Zweig in den `develop` Zweig ein. Idealerweise verwendet der Entwickler ein automatis iertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keine Squash-Zu sammenführung. 11. Wenn ein Konflikt erkannt wird, erhalten Entwickler	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine Warnung und lösen den Konflikt mit einer Zusammenführungsan forderung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Fehlerfix-Gitflow-Prozess.	1. Der Entwickler erstellt einen `bugfix` Zweig aus dem aktuellen `release/v<number>` Zweig und verwendet das Benennungsmuster `bugfix/<ticket number>_<developer initials>_<descriptor>` . 2. Der Entwickler behebt das Problem, führt ein Commit für den Fehler aus und erstellt die `bugfix` Verzweigung. 3. Der Entwickler erstellt mithilfe einer Squash-Zusammenführung eine Zusammenführungsanforderung von der `bugfix` Verzweigung in die `release/v<number>` Verzweigung. 4. Der Entwickler erstellt den `release` Zweig, der Artefakte zur Wiederverwendung in anderen Umgebungen veröffentlicht. 5. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Testumgebung manuell. 6. Ein Genehmiger genehmigt die Bereitstellung der	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Release-Artefakte in der Stage-Umgebung manuell. 7. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Produktionsumgebung manuell. 8. Der Entwickler führt den `release` Zweig in den `main` Zweig ein. Idealerweise verwendet der Entwickler ein automatis iertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keine Squash-Zu sammenführung. 9. Der Entwickler führt den `release` Zweig in den `develop` Zweig ein. Idealerweise verwendet der Entwickler ein automatis iertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keine Squash-Zu sammenführung. 10. Wenn ein Konflikt erkannt wird, erhalten Entwickler eine Warnung und lösen den Konflikt mit einer Zusammenführungsan forderung.	

Fehlerbehebung

Problem	Lösung
Verzweigungskonflikte	Ein häufiges Problem, das beim Gitflow-Modell auftreten kann, besteht darin, dass ein Hotfix in der Produktion auftreten muss, aber eine entsprechende Änderung in einer niedrigeren Umgebung erfolgen muss, in der ein anderer Zweig dieselben Ressourcen ändert. Wir empfehlen Ihnen, jeweils nur einen einzigen Release-Zweig zu aktivieren. Wenn Sie mehr als einen aktiven gleichzeitig haben, können die Änderungen in den Umgebungen kollidier en und Sie können einen Zweig möglicherweise nicht in die Produktion verschieben.
Zusammenführen von	Versionen sollten wieder in den Hauptbere ich integriert werden und sich so schnell wie möglich entwickeln, um die Arbeit wieder in den primären Zweigen zu konsolidieren.
Squash-Zusammenführung	Verwenden Sie eine Squash-Zusammenfüh rung nur, wenn Sie von einem `feature` Zweig zu einem `develop` Zweig zusammenführen. Die Verwendung von Squash-Zusammenfüh rungen in höheren Zweigen führt zu Schwierig keiten beim Zusammenführen von Änderungen wieder nach unten zu niedrigeren Zweigen.

Zugehörige Ressourcen

Dieser Leitfaden beinhaltet kein Training für Git. Wenn Sie dieses Training benötigen, stehen jedoch viele hochwertige Ressourcen im Internet zur Verfügung. Wir empfehlen Ihnen, mit der Git-Dokumentationsseite zu beginnen.

Die folgenden Ressourcen können Ihnen bei Ihrer Gitflow-Verzweigungsreise in der helfen AWS Cloud.

AWS DevOps -Anleitung

- AWS DevOps Anleitung
- AWS Referenzarchitektur der Bereitstellungs-Pipeline
- Was ist DevOps?
- DevOps -Ressourcen

Gitflow-Anleitung

- Der ursprüngliche Gitflow-Blog (Vincent-Driessen-Blogbeitrag)
- Gitflow-Workflow (Atlassisch)
- Gitflow auf GitHub: So verwenden Sie Git-Flow-Workflows mit GitHub basierten Repos (YouTube Video)
- Git Flow Init-Beispiel (YouTube Video)
- Der Gitflow-Versionszweig von Anfang bis Ende (YouTube Video)

Sonstige Ressourcen

Methode zur Anwendung mit zwölf Faktoren (12factor.net)

Implementierung einer Trunk-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten

Erstellt von Bol Stephens (AWS) und Rayjan Bol (AWS)

Code-Repository: git-branching-strategies-for-multiaccount-devops	Umgebung: Produktion	Technologien: DevOps; Softwareentwicklung und -tests; Strategie mit mehreren Konten
AWS-Services: AWS CodeArtifact; AWS CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Übersicht

Bei der Verwaltung eines Quellcode-Repositorys wirken sich verschiedene Verzweigungsstrategien auf die Softwareentwicklungs- und Veröffentlichungsprozesse aus, die Entwicklungsteams verwenden. Beispiele für gängige Verzweigungsstrategien sind Trunk, GitHub Flow und Gitflow. Diese Strategien verwenden verschiedene Zweige, und die in jeder Umgebung durchgeführten Aktivitäten unterscheiden sich. Organisationen, die DevOps Prozesse implementieren, würden von einem visuellen Leitfaden profitieren, der ihnen hilft, die Unterschiede zwischen diesen Verzweigungsstrategien zu verstehen. Die Verwendung dieser Visualisierung in Ihrer Organisation hilft Entwicklungsteams dabei, ihre Arbeit aufeinander abzustimmen und die Organisationsstandards einzuhalten. Dieses Muster bietet diese Visualisierung und beschreibt den Prozess der Implementierung einer Trunk-Verzweigungsstrategie in Ihrer Organisation.

Dieses Muster ist Teil einer Dokumentationsreihe zur Auswahl und Implementierung von DevOps Verzweigungsstrategien für Organisationen mit mehreren AWS-Konten. Diese Reihe soll Ihnen helfen, die richtige Strategie und bewährte Methoden von Anfang an anzuwenden, um Ihre Erfahrung in der Cloud zu optimieren. Trunk ist nur eine mögliche Verzweigungsstrategie, die Ihr Unternehmen verwenden kann. Diese Dokumentationsreihe behandelt auch GitHub Flow -und Gitflow-Verzweigungsmodelle. Wenn Sie dies noch nicht getan haben, empfehlen wir Ihnen, die

Auswahl einer Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten zu lesen, bevor Sie die Anleitungen in diesem Muster implementieren. Bitte verwenden Sie die gebotene Vorsicht, um die richtige Verzweigungsstrategie für Ihre Organisation auszuwählen.

Dieses Handbuch enthält ein Diagramm, das zeigt, wie eine Organisation die Trunk-Strategie implementieren könnte. Es wird empfohlen, die offizielle AWS Well-Architected DevOps Guidance zu lesen, um bewährte Methoden zu überprüfen. Dieses Muster umfasst empfohlene Aufgaben, Schritte und Einschränkungen für jeden Schritt des DevOps Prozesses.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git, installiert . Dies wird als Quellcode-Repository-Tool verwendet.
- Draw.io, installiert . Diese Anwendung wird verwendet, um das Diagramm anzuzeigen und zu bearbeiten.

Architektur

Zielarchitektur

Das folgende Diagramm kann wie ein Punnett-Quader (Wikipedia) verwendet werden. Sie richten die Verzweigungen auf der vertikalen Achse mit den AWS Umgebungen auf der horizontalen Achse aus, um zu bestimmen, welche Aktionen in jedem Szenario ausgeführt werden sollen. Die Zahlen geben die Reihenfolge der Aktionen im Workflow an. Dieses Beispiel führt Sie von einem `feature` Zweig bis zur Bereitstellung in der Produktion.

Weitere Informationen zu AWS-Konten, Umgebungen und Verzweigungen in einem Trunk-Ansatz finden Sie unter Auswählen einer Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten.

Automatisierung und Skalierung

Continuous Integration and Continuous Delivery (CI/CD) ist der Prozess der Automatisierung des Lebenszyklus von Softwareversionen. Es automatisiert viele oder alle manuellen Prozesse, die traditionell erforderlich sind, um neuen Code von einem ersten Commit in die Produktion zu erhalten. Eine CI/CD-Pipeline umfasst die Sandbox-, Entwicklungs-, Test-, Staging- und Produktionsumgebungen. In jeder Umgebung stellt die CI/CD-Pipeline jede Infrastruktur

bereit, die zum Bereitstellen oder Testen des Codes erforderlich ist. Mithilfe von CI/CD können Entwicklungsteams Änderungen am Code vornehmen, die dann automatisch getestet und bereitgestellt werden. CI/CD-Pipelines bieten auch Governance und Integritätsschutz für Entwicklungsteams, indem sie Konsistenz, Standards, bewährte Methoden und minimale Akzeptanzstufen für die Annahme und Bereitstellung von Features durchsetzen. Weitere Informationen finden Sie unter Praktische kontinuierliche Integration und kontinuierliche Bereitstellung auf AWS.

AWS bietet eine Reihe von Entwicklerservices, die Sie bei der Erstellung von CI/CD-Pipelines unterstützen. Beispielsweise AWS CodePipelineist ein vollständig verwalteter kontinuierlicher Bereitstellungsservice, mit dem Sie Ihre Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturaktualisierungen automatisieren können. AWS CodeCommitist darauf ausgelegt, skalierbare Git-Repositorys sicher zu hosten und Quellcode zu AWS CodeBuildkompilieren, Tests durchzuführen und ready-to-deploy Softwarepakete zu erstellen. Weitere Informationen finden Sie unterEntwicklertools auf AWS.

Tools

AWS -Services und -Tools

AWS bietet eine Reihe von Entwicklerservices, mit denen Sie dieses Muster implementieren können:

- AWS CodeArtifact ist ein hoch skalierbarer, verwalteter Artefakt-Repository-Service, mit dem Sie Softwarepakete für die Anwendungsentwicklung speichern und freigeben können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen für Amazon Elastic Compute Cloud (Amazon EC2) oder On-Premises-Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS)-Services.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.

Andere Tools

- Draw.io Desktop – Eine Anwendung zum Erstellen von Flussdiagrammen und Diagrammen.
- Bolma ist ein Online-Design-Tool, das für die Zusammenarbeit entwickelt wurde. Das Code-Repository enthält Vorlagen im .fig-Format für Bolma.

Code-Repository

Diese Quelldatei für das Diagramm in diesem Muster ist im GitHub Git Branching Strategy for Trunk-Repository verfügbar. Sie enthält Dateien in den Formaten PNG, draw.io undma. Sie können diese Diagramme ändern, um die Prozesse Ihrer Organisation zu unterstützen.

Bewährte Methoden

Folgen Sie den bewährten Methoden und Empfehlungen in AWS Well-Architected DevOps Guidance und wählen Sie eine Git-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten aus. Diese helfen Ihnen, die Trunk-basierte Entwicklung effektiv zu implementieren, die Zusammenarbeit zu fördern, die Codequalität zu verbessern und den Entwicklungsprozess zu optimieren.

Sekunden

Überprüfen des Trunk-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Standard-Trunk-Prozess.	1. In der Sandbox-Umgebung erstellt der Entwickler einen `feature` Zweig aus dem `main` Zweig und verwendet das Benennung smuster `feature/<ticket>_<initials>_<short description>` . 2. Der Entwickler entwickelt Code und stellt den Code iterativ in der Sandbox-Umgebung bereit, um das Ticket abzuschließen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Der Entwickler kann optional einen `sandbox` Zweig erstellen, um eine automatisierte Build- oder Bereitstellungspipeline in der Sandbox-Umgebung auszuführen. 3. Der Entwickler erstellt eine Zusammenführungsanforderung von der `feature` Verzweigung in die `main` Verzweigung mithilfe einer Squash-Zusammenführung. 4. Eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) erstellt und veröffentlicht die Artefakte automatisch vom `main` Zweig in der Entwicklungsumgebung. 5. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Entwicklungsumgebung manuell. 6. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Testumgebung manuell. 7. Ein Genehmiger genehmigt die Bereitstellung der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Release-Artefakte in der Staging-Umgebung manuell. 8. Ein Genehmiger genehmigt die Bereitstellung der Release-Artefakte in der Produktionsumgebung manuell.	

Fehlerbehebung

Problem	Lösung
Verzweigungskonflikte	Ein häufiges Problem, das beim Trunk-Modell auftreten kann, besteht darin, dass ein Hotfix in der Produktion auftreten muss, aber eine entsprechende Änderung in einem `feature` Zweig erfolgen muss, in dem dieselben Ressourcen geändert werden. Wir empfehlen , Änderungen von häufig `main` in niedrigere Zweige zusammenzuführen, um signifikante Konflikte bei der Zusammenführung mit zu vermeiden`main`.

Zugehörige Ressourcen

Dieser Leitfaden beinhaltet keine Schulung für Git. Wenn Sie dieses Training benötigen, stehen jedoch viele hochwertige Ressourcen im Internet zur Verfügung. Wir empfehlen Ihnen, mit der Git-Dokumentationsseite zu beginnen.

Die folgenden Ressourcen können Ihnen bei Ihrer Trunk-Verzweigungsreise in der helfen AWS Cloud.

AWS DevOps -Anleitung

- AWS DevOps Anleitung
- AWS Referenzarchitektur der Bereitstellungs-Pipeline
- Was ist DevOps?
- DevOps -Ressourcen

Trunk-Anleitung

- Trunk-basierte Entwicklung

Sonstige Ressourcen

- App-Methode mit zwölf Faktoren (12factor.net)

Automatisches Erkennen von Änderungen und Initiieren verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit

Erstellt von Helton Boleiro (AWS), Petrus Boltalha (AWS) und Ricardoais (AWS)

Code-Repository: AWS CodeCommit Monorepo-Auslöser mit mehreren Pipelines	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur; Serverless
AWS-Services: AWS CodeCommit; AWS CodePipeline; AWS Lambda		

Übersicht

Dieses Muster hilft Ihnen, Änderungen am Quellcode einer monorepobasierten Anwendung in automatisch zu erkennen AWS CodeCommit und dann eine Pipeline in zu initiieren AWS CodePipeline , die die kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD)-Automatisierung für jeden Microservice ausführt. Dieser Ansatz bedeutet, dass jeder Microservice in Ihrer monorepo-basierten Anwendung über eine dedizierte CI/CD-Pipeline verfügen kann, die eine bessere Sichtbarkeit, einfachere Codefreigabe und verbesserte Zusammenarbeit, Standardisierung und Auffindbarkeit gewährleistet.

Die in diesem Muster beschriebene Lösung führt keine Abhängigkeitsanalyse zwischen den Microservices innerhalb des Monorepo durch. Es erkennt nur Änderungen im Quellcode und initiiert die passende CI/CD-Pipeline.

Das Muster verwendet AWS Cloud9 als integrierte Entwicklungsumgebung (IDE) und AWS Cloud Development Kit (AWS CDK) , um eine Infrastruktur mithilfe von zwei AWS CloudFormation Stacks zu definieren: `MonoRepoStack` und `PipelinesStack`. Der `MonoRepoStack`Stack erstellt das Monorepo in AWS CodeCommit und die AWS Lambda Funktion, die die CI/CD-Pipelines initiiert. Der `PipelinesStack`Stack definiert Ihre Pipeline-Infrastruktur.

Wichtig: Der Workflow dieses Musters ist ein Machbarkeitsnachweis (PoC). Wir empfehlen, sie nur in einer Testumgebung zu verwenden. Wenn Sie den Ansatz dieses Musters in einer Produktionsumgebung verwenden möchten, finden Sie weitere Informationen unter Bewährte Methoden für die Sicherheit in IAM in der AWS Identity and Access Management (IAM)-Dokumentation und nehmen Sie die erforderlichen Änderungen an Ihren IAM-Rollen und vor AWS-Services.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS Konto.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI in der - AWS CLI Dokumentation.
- Python 3 und `pip`, installiert auf Ihrem lokalen Computer. Weitere Informationen finden Sie in der Python-Dokumentation.
- AWS CDK, installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte mit in AWS CDK der - AWS CDK Dokumentation.
- Eine AWS Cloud9 IDE, installiert und konfiguriert. Weitere Informationen finden Sie unter Einrichten von AWS Cloud9 in der - AWS Cloud9 Dokumentation.
- Das Multi- GitHub AWS CodeCommit Pipeline-Auslöser-Repository für Monorepo, das auf Ihrem lokalen Computer geklont ist.
- Ein vorhandenes Verzeichnis mit Anwendungscode, das Sie mit erstellen und bereitstellen möchten CodePipeline.
- Vertrautheit und Erfahrung mit DevOps bewährten Methoden in der AWS Cloud. Um Ihre Vertrautheit mit zu erhöhen DevOps, können Sie das Muster Erstellen einer lose gekoppelten Architektur mit Microservices mithilfe von - DevOps Methoden und AWS Cloud9 auf der Website AWS Prescriptive Guidance verwenden.

Architektur

Das folgende Diagramm zeigt, wie Sie mit eine Infrastruktur mit zwei AWS CloudFormation Stacks AWS CDK definieren: `MonoRepoStack` und `PipelinesStack`.

Das Diagramm zeigt den folgenden Workflow:

1. Der Bootstrap-Prozess verwendet die AWS CDK , um die AWS CloudFormation Stacks `MonoRepoStack` und zu erstellen`PipelinesStack`.
2. Der `MonoRepoStack`Stack erstellt das CodeCommit Repository für Ihre Anwendung und die `monorepo-event-handler` Lambda-Funktion, die nach jedem Commit initiiert wird.
3. Der `PipelinesStack`Stack erstellt die Pipelines in CodePipeline , die von der Lambda-Funktion initiiert werden. Jeder Microservice muss über eine definierte Infrastruktur-Pipeline verfügen.
4. Die Pipeline für `microservice-n` wird von der Lambda-Funktion initiiert und startet ihre isolierten CI/CD-Phasen, die auf dem Quellcode in basieren CodeCommit.
5. Die Pipeline für `microservice-1` wird von der Lambda-Funktion initiiert und startet ihre isolierten CI/CD-Phasen, die auf dem Quellcode in basieren CodeCommit.

Das folgende Diagramm zeigt die Bereitstellung der AWS CloudFormation Stacks `MonoRepoStack` und `PipelinesStack` in einem Konto.

1. Ein Benutzer ändert Code in einem der Microservices der Anwendung.
2. Der Benutzer überträgt die Änderungen aus einem lokalen Repository in ein CodeCommit Repository.
3. Die Push-Aktivität initiiert die Lambda-Funktion, die alle Pushs in das CodeCommit Repository empfängt.
4. Die Lambda-Funktion liest einen Parameter in Parameter Store, einer Funktion von AWS Systems Manager, um die neueste Commit-ID abzurufen. Der Parameter hat das Namensformat: `/MonoRepoTrigger/{repository}/{branch_name}/LastCommit`. Wenn der Parameter nicht gefunden wird, liest die Lambda-Funktion die letzte Commit-ID aus dem CodeCommit Repository und speichert den zurückgegebenen Wert im Parameter Store.
5. Nachdem die Commit-ID und die geänderten Dateien identifiziert wurden, identifiziert die Lambda-Funktion die Pipelines für jedes Microservice-Verzeichnis und initiiert die erforderliche CodePipeline Pipeline.

Tools

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework für die Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS CloudFormation.
- Python ist eine Programmiersprache, mit der Sie schneller arbeiten und Systeme effektiver integrieren können.

Code

Der Quellcode und die Vorlagen für dieses Muster sind im Multi- GitHub AWS CodeCommit Pipeline-Auslöser-Repository von Monorepo verfügbar.

Bewährte Methoden

- Diese Beispielarchitektur enthält keine Überwachungslösung für die bereitgestellte Infrastruktur. Wenn Sie diese Lösung in einer Produktionsumgebung bereitstellen möchten, empfehlen wir Ihnen, die Überwachung zu aktivieren. Weitere Informationen finden Sie unter Überwachen Ihrer Serverless-Anwendungen mit CloudWatch Application Insights in der AWS Serverless Application Model (AWS SAM)-Dokumentation.
- Wenn Sie den von diesem Muster bereitgestellten Beispielcode bearbeiten, befolgen Sie die bewährten Methoden für die Entwicklung und Bereitstellung der Cloud-Infrastruktur in der - AWS CDK Dokumentation.
- Wenn Sie Ihre Microservice-Pipelines definieren, lesen Sie die bewährten Sicherheitsmethoden in der - AWS CodePipeline Dokumentation.
- Sie können Ihren AWS CDK Code auch mithilfe des Hilfsprogramms cdk-nag auf bewährte Methoden überprüfen. Dieses Tool verwendet eine Reihe von Regeln, gruppiert nach Paketen, um Ihren Code auszuwerten. Die verfügbaren Pakete sind:
  - AWS -Lösungsbibliothek
  - Sicherheit im Health Insurance Portability and Accountability Act (HIPAA)
  - National Institute of Standards and Technology (NIST) 800–53, Version 4
  - NIST 800-53, Version 5
  - Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Polen

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle Python-Umgebung.	Erstellen Sie in Ihrer AWS Cloud9 IDE eine virtuelle Python-Umgebung und installieren Sie die erforderl ichen Abhängigkeiten, indem Sie den folgenden Befehl ausführen: `make install`	Developer
Bootstrappen Sie die AWS-Konto und AWS-Region für die AWS CDK.	Führen Sie den folgenden Befehl aus, um das erforderl iche AWS-Konto und die Region zu booten: `make bootstrap account-id=<your-AWS-account-ID> region=<required-region>`	Developer

Hinzufügen einer neuen Pipeline für einen Microservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Ihren Beispielcode zu Ihrem Anwendungsverzeich nis hinzu.	Fügen Sie das Verzeichnis, das Ihren Beispielanwendungs code enthält, dem `monorepo-sample` Verzeichnis im geklonten Multi- GitHub AWS CodeCommit Pipeline-	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Auslöser-Repository für Monorepo hinzu.	
Bearbeiten Sie die `monorepo-main.json` -Datei.	Fügen Sie den Verzeichnisnamen des Codes Ihrer Anwendung und den Namen der Pipeline zur `monorepo-main.json` Datei im geklonten Repository hinzu.	Developer
Erstellen Sie die Pipeline.	Fügen Sie im `Pipelines` Verzeichnis für das Repository die Pipeline `class` für Ihre Anwendung hinzu. Das Verzeichnis enthält zwei Beispieldateien, `pipeline_hotsite.py` und `pipeline_demo.py` . Jede Datei besteht aus drei Phasen: Quelle, Build und Bereitstellung. Sie können eine der Dateien kopieren und entsprechend den Anforderungen Ihrer Anwendung Änderungen daran vornehmen.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bearbeiten Sie die `monorepo_config.py` -Datei.	Fügen Sie in den Verzeichnisnamen für Ihre Anwendung und die Klasse `service_map` hinzu, die Sie für die Pipeline erstellt haben.
	
	Der folgende Code zeigt beispielsweise eine Pipeline-Definition im `Pipelines` Verzeichnis , die eine Datei mit dem Namen `pipeline_mysample.py` mit einer `MySamplePipeline` Klasse verwendet:
	
	`...`
	`# Pipeline definition imports`
	`from pipelines.pipeline_demo import DemoPipeline`
	`from pipelines.pipeline_hotsite import HotsitePipeline`
	`from pipelines.pipeline_mysample import MySamplePipeline`
	
	`### Add your pipeline configuration here`
	`service_map: Dict[str, ServicePipeline] = {`
	`# folder-name -> pipeline-class`
	`'demo': DemoPipeline(),`
	`'hotsite': HotsitePipeline(),`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`'mysample': MySamplePipeline() }`	

Bereitstellen des MonoRepoStack Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS CloudFormation Stack bereit.	Stellen Sie den AWS CloudFormation `MonoRepoStack` Stack mit Standardparameterwerten im Stammverzeichnis des geklonten Repositorys bereit, indem Sie den `make deploy-core` Befehl ausführen. Sie können den Namen des Repositorys ändern, indem Sie den `make deploy-core monorepo-name=<repo_name>` Befehl ausführen. Hinweis: Sie können beide Pipelines gleichzeitig bereitstellen, indem Sie den `make deploy monorepo-name=<repo_name>` Befehl verwenden.	Developer
Validieren Sie das CodeCommit Repository.	Überprüfen Sie, ob Ihre Ressourcen erstellt wurden, indem Sie den `aws codecommit get-repository --repository-`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`name <repo_name>` Befehl ausführen. Wichtig: Da der AWS CloudFormation Stack das CodeCommit Repository erstellt, in dem das Monorepo gespeichert ist, führen Sie den `cdk destroy MonoRepoStack` Befehl nicht aus, wenn Sie mit dem Übertragen von Änderungen in das Stack begonnen haben.	
Validieren Sie die AWS CloudFormation Stack-Ergebnisse.	Überprüfen Sie, ob der AWS CloudFormation `MonoRepoStack` Stack korrekt erstellt und konfiguriert wurde, indem Sie den folgenden Befehl ausführen: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE --query 'StackSummaries[?StackName == 'MonoRepoStack']'`	Developer

Bereitstellen des PipelinesStack Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS CloudFormation Stack bereit.	Der AWS CloudFormation `PipelinesStack` Stack muss bereitgestellt werden,	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nachdem Sie den `MonoRepoStack` Stack bereitgestellt haben. Der Stack nimmt zu, wenn der Codebasis des Monorepo neue Microservices hinzugefügt werden, und wird erneut bereitgestellt, wenn ein neuer Microservice integriert wird. Stellen Sie den Pipelines Stack Stack bereit, indem Sie den `make deploy-pipelines` Befehl ausführen. Hinweis: Sie können auch beide Pipelines gleichzeitig bereitstellen, indem Sie den `make deploy monorepo-name=<repo_name>` Befehl ausführen. Die folgende Beispielausgabe zeigt, wie die `Pipelines Stacks` Bereitstellung die URLs für die Microservices am Ende der Implementierung druckt: `Outputs: PipelinesStack.dem ourl = .cloudfront.net PipelinesStack.hotsi teurl = .cloudfro nt.net`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die AWS CloudFormation Stack-Ergebnisse.	Überprüfen Sie, ob der AWS CloudFormation `Pipelines Stacks` Stack korrekt erstellt und konfiguriert wurde, indem Sie den folgenden Befehl ausführen: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE UPDATE_COMPLETE --query 'StackSummaries[?StackName == 'PipelinesStack']'`	Developer

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie Ihre AWS CloudFormation Stacks.	Führen Sie den Befehl `make destroy` aus.	Developer
Löschen Sie die S3-Buckets für Ihre Pipelines.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Simple Storage Service (Amazon S3)-Konsole. 2. Löschen Sie die S3-Buckets, die Ihren Pipelines zugeordnet sind, und verwenden Sie den folgenden Namen: `pipelinesstack-codepipeline*`	Developer

Fehlerbehebung

Problem	Lösung
Ich habe AWS CDK Probleme festgestellt.	Weitere Informationen finden Sie unter Fehlerbehebung bei häufigen AWS CDK Problemen in der AWS-CDK-Dokumentation.
Ich habe meinen Microservice-Code übertragen, aber die Microservice-Pipeline wurde nicht ausgeführt.	Setup-Validierung Überprüfen Sie die Zweigkonfiguration: • Stellen Sie sicher, dass Sie Ihren Code an die richtige Verzweigung übertragen. Diese Pipeline ist so konfiguriert, dass sie nur ausgeführt wird, wenn Änderungen an der `main` Verzweigung vorgenommen werden. Pushs an andere Zweige initiieren die Pipeline nur, wenn sie speziell konfiguriert sind. • Nachdem Sie Ihren Code übertragen haben, überprüfen Sie, ob der Commit in sichtbar ist, AWS CodeCommit um sicherzustellen, dass der Push erfolgreich war und dass die Verbindung zwischen Ihrer lokalen Umgebung und dem Repository intakt ist. Aktualisieren Sie Ihre Anmeldeinformationen, wenn Probleme beim Pushen von Code auftreten. Validieren von Konfigurationsdateien: • Vergewissern Sie sich, dass die `service_map` Variable in die aktuelle Verzeichnisstruktur Ihrer Microservices `monorepo_config.py` genau widerspiegelt. Diese Variable spielt eine entscheidende Rolle

Problem	Lösung
	bei der Zuordnung Ihres Code-Pushs zur jeweiligen Pipeline. • Stellen Sie sicher, dass aktualisiert `monorepo-main.json` wird, um das neue Mapping für Ihren Microservice aufzunehmen. Diese Datei ist wichtig, damit die Pipeline Änderungen an Ihrem Microservice erkennt und korrekt verarbeitet. Fehlerbehebung in der Konsole AWS CodePipeline -Prüfungen: • Vergewissern Sie sich in der AWS Management Console, dass Sie sich in der befinden AWS-Region , in der Ihre Pipeline gehostet wird. Öffnen Sie die -CodePipeline Konsole und überprüfen Sie, ob die Pipeline, die Ihrem Microservice entspricht, initiiert wurde. Fehleranalyse: Wenn die Pipeline initiiert wurde, aber fehlgeschlagen ist, überprüfen Sie alle von bereitgestellten Fehlermeldungen oder Protokolle, CodePipeline um zu verstehen, was schief gelaufen ist. AWS Lambda Fehlerbehebung: • Öffnen Sie in der AWS Lambda -Konsole die `monorepo-event-handler` Lambda-Funktion. Stellen Sie sicher, dass die Funktion als Reaktion auf den Code-Push initiiert wurde.

Problem	Lösung
	Protokollanalyse: Überprüfen Sie die Protokolle der Lambda-Funktion auf Probleme. Die Protokolle können detaillierte Einblicke in die Geschehnisse bei der Ausführung der Funktion geben und helfen festzustellen, ob die Funktion das Ereignis wie erwartet verarbeitet hat.

Problem	Lösung
Ich muss alle meine Microservices erneut bereitstellen.	Es gibt zwei Ansätze, um die erneute Bereitstellung aller Microservices zu erzwingen. Wählen Sie die Option aus, die Ihren Anforderungen entspricht. Ansatz 1: Löschen eines Parameters im Parameter Store Diese Methode beinhaltet das Löschen eines bestimmten Parameters in Systems Manager Parameter Store, der die letzte Commit-ID verfolgt, die für die Bereitstellung verwendet wurde. Wenn Sie diesen Parameter entfernen, ist das System gezwungen, alle Microservices beim nächsten Auslöser erneut bereitzustellen, da es ihn als neuen Zustand wahrnimmt. Schritte: 1. Suchen Sie den spezifischen Parameter Store-Eintrag, der die Commit-ID oder eine zugehörige Bereitstellungsmarkierung für Ihr Monorepo enthält. Der Parametername hat folgendes Format: `"/MonoRepoTrigger/{repository}/{branch_name}/LastCommit"` 2. Erwägen Sie, den Parameterwert zu sichern, wenn er wichtig ist oder wenn Sie eine Aufzeichnung des Bereitstellungsstatus führen möchten, bevor Sie ihn zurücksetzen. 3. Verwenden Sie die AWS Management Console AWS CLI, oder SDKs, um den identifizierten Parameter zu löschen. Diese Aktion setzt die Bereitstellungsmarkierung zurück.

Problem	Lösung
	4. Nach dem Löschen sollte der nächste Push in das Repository dazu führen, dass das System alle Microservices bereitstellt, da es nach dem letzten Commit sucht, der für die Bereitstellung in Betracht gezogen werden soll. Vorteile: • Einfache und schnelle Implementierung in nur wenigen Schritten. • Es ist nicht erforderlich, beliebige Codeänder ungen vorzunehmen, um Bereitstellungen zu initiieren. Vorteile: • Weniger detaillierte Kontrolle über den Bereitstellungsprozess. • Potenziell riskant, wenn der Parameter Store für die Verwaltung anderer kritischer Konfigurationen verwendet wird. Ansatz 2: Übertragen eines Commit in jeden Monorepo-Unterordner Bei dieser Methode wird eine geringfüg ige Änderung vorgenommen und in jeden Microservice-Unterordner innerhalb des Monorepo verschoben, um ihre einzelnen Pipelines zu initiieren. Schritte:

Problem	Lösung
	1. Listen Sie alle Microservices innerhalb des Monorepo auf, die erneut bereitgestellt werden müssen. 2. Nehmen Sie für jeden Microservice eine minimale, nicht sinnvolle Änderung am Unterordner vor. Dies kann das Aktualisieren einer `README` Datei, das Hinzufügen eines Kommentars in einer Konfigurationsdatei oder jede Änderung sein, die sich nicht auf die Funktionalität des Services auswirkt. 3. Übernehmen Sie diese Änderungen mit einer Klarmeldung (z. B. „Neubereitstellung von Microservices initiieren“) und übertragen Sie sie in das Repository. Stellen Sie sicher, dass Sie die Änderungen an den Zweig übertragen, der die Bereitstellung initiiert. 4. Überwachen Sie die Pipelines für jeden Microservice, um zu bestätigen, dass sie initiiert und erfolgreich abgeschlossen wurden. Vorteile: • Bietet eine detaillierte Kontrolle darüber, welche Microservices erneut bereitgestellt werden. • Sicherer, da dies nicht das Löschen von Konfigurationsparametern beinhaltet, die für andere Zwecke verwendet werden könnten. Vorteile: • Zeitaufwändiger, insbesondere bei einer großen Anzahl von Microservices.

Problem	Lösung
	• Erfordert unnötige Codeänderungen, die den Commit-Verlauf überladen könnten.

Zugehörige Ressourcen

- Kontinuierliche Integration und Bereitstellung (CI/CD) mithilfe von CDK Pipelines (AWS CDK Dokumentation)
- Modul aws-cdk/pipelines (AWS CDK API-Referenz)

Integrieren eines Bitbucket-Repositorys mit AWS Amplify mithilfe von AWS CloudFormation

Erstellt von Alwin Abraham (AWS)

Umgebung: Produktion	Technologien: DevOps	AWS-Services: AWS Amplify; AWS CloudFormation

Übersicht

AWS Amplify hilft Ihnen, statische Websites schnell bereitzustellen und zu testen, ohne die Infrastruktur einrichten zu müssen, die normalerweise erforderlich ist. Sie können den Ansatz dieses Musters einsetzen, wenn Ihre Organisation Bitbucket für die Quellkontrolle verwenden möchte, unabhängig davon, ob Sie vorhandenen Anwendungscode migrieren oder eine neue Anwendung erstellen möchten. Indem Sie AWS verwenden, CloudFormation um Amplify automatisch einzurichten, bieten Sie Einblicke in die Konfigurationen, die Sie verwenden.

Dieses Muster beschreibt, wie Sie eine Pipeline und Bereitstellungsumgebung für kontinuierliche Frontend-Integration und kontinuierliche Bereitstellung (CI/CD) erstellen, indem Sie AWS verwenden CloudFormation , um ein Bitbucket-Repository in AWS Amplify zu integrieren. Der Ansatz des Musters bedeutet, dass Sie eine Amplify-Frontend-Pipeline für wiederholbare Bereitstellungen erstellen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto
- Ein aktives Bitbucket-Konto mit Administratorzugriff
- Zugriff auf ein Terminal, das cURL oder die Postman-Anwendung verwendet
- Vertrautheit mit Amplify
- Vertrautheit mit AWS CloudFormation
- Vertrautheit mit Dateien im YAML-Format

Architektur

Technologie-Stack

- Amplify
- AWS CloudFormation
- Bitbucket

Tools

- AWS Amplify – Amplify hilft Entwicklern bei der Entwicklung und Bereitstellung von cloudbasierten mobilen und Web-Apps.
- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt, sodass Sie weniger Zeit für die Verwaltung dieser Ressourcen aufwenden müssen und sich stattdessen mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden.
- Bitbucket – Bitbucket ist eine Git-Repository-Verwaltungslösung, die für Geschäftsteams entwickelt wurde. Es bietet Ihnen einen zentralen Ort, an dem Sie Git-Repositorys verwalten, an Ihrem Quellcode zusammenarbeiten und Sie durch den Entwicklungsablauf führen können.

Code

Die `bitbucket-amplify.yml` Datei (angefügt) enthält die AWS- CloudFormation Vorlage für dieses Muster.

Polen

Konfigurieren des Bitbucket-Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erstellen Sie ein Bitbucket-Repository.	1. Melden Sie sich bei Ihrem Bitbucket-Konto an und erstellen Sie ein neues	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repository. Weitere Informationen dazu finden Sie unter Erstellen eines Git-Repositorys in der Bitbucket-Dokumentation. 2. Notieren Sie sich den Namen des Workspace. Hinweis: Sie können auch ein vorhandenes Bitbucket-Repository verwenden.	
Öffnen Sie die Workspace-Einstellungen.	1. Öffnen Sie den Workspace und wählen Sie die Registerkarte Repository aus. 2. Wählen Sie das Repository aus, das Sie in Amplify integrieren möchten. 3. Wählen Sie den Namen des Workspace aus, der über dem Namen des Repositorys liegt. 4. Wählen Sie in der Seitenleiste Einstellungen aus.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen OAuth-Verbraucher.	1. Wählen Sie im Abschnitt Apps und Features die Option OAuth-Konsumenten und dann Konsument hinzufügen aus. 2. Geben Sie einen Namen für Ihren Verbraucher ein, z. B. `Amplify Integration` . 3. Geben Sie eine Rückruf-URL ein. Obwohl dieses Feld eine erforderliche Eingabe ist, wird es nicht verwendet, um die Integration abzuschließen, sodass der Wert sein könnte `http://localhost:3000` 4. Aktivieren Sie das Kontrollkästchen für Dies ist ein privater Verbraucher . 5. Wählen Sie die folgenden Berechtigungen aus: • Projekt – `Read` • Repositorys – `Admin` • Pull-Anforderungen – `Read` • Webhooks – `Read`und `Write` 6. Behalten Sie die Standardoptionen für alle anderen Felder bei und wählen Sie Senden aus.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Notieren Sie den Schlüssel und das Geheimnis, die generiert werden.	
OAuth-Zugriffstoken abrufen.	1. Öffnen Sie ein Terminalf enster und führen Sie den folgenden Befehl aus: `curl -X POST -u "KEY:SECRET" https://bitbucket.org/site/oauth2/access_token -d grant_type=client_credentials` Wichtig: Ersetzen Sie `KEY` und `SECRET` durch den Schlüssel und das Secret, die Sie zuvor aufgezeichnet haben. 2. Notieren Sie das Zugriffst oken, ohne die Anführung szeichen zu verwenden. Das Token ist nur für einen begrenzten Zeitraum gültig und die Standardzeit beträgt zwei Stunden. Sie müssen die AWS- CloudFormation Vorlage in diesem Zeitrahmen ausführen.	DevOps Techniker

Erstellen und Bereitstellen des AWS- CloudFormation Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die AWS-CloudFormation Vorlage herunter.	Laden Sie die `bitbucket-amplify.yml` AWS-CloudFormation Vorlage (angefügt) herunter. Diese Vorlage erstellt die CI/CD-Pipeline in Amplify, zusätzlich zum Amplify-Projekt und der Verzweigung.	
Erstellen Sie den AWS-CloudFormation Stack und stellen Sie ihn bereit.	1. Melden Sie sich bei der AWS-Managementkonsole in der AWS-Region an, in der Sie bereitstellen möchten, und öffnen Sie die AWS- CloudFormation Konsole. 2. Wählen Sie Stack erstellen (mit neuen Ressourcen) und dann Vorlagendatei hochladen aus. 3. Hochladen der `bitbucket-amplify.yml` -Datei 4. Wählen Sie Weiter, geben Sie einen Stack-Namen ein und geben Sie dann die folgenden Parameter ein: • Zugriffstoken: Fügen Sie das zuvor erstellte OAuth-Zugriffstoken ein. • Repository-URL: Fügen Sie die URL des Bitbucket-Projekt-	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repositorys hinzu. Die URL hat normalerw eise das folgende Format: `https://b itbucket.org/ <WORKSPACE_NAME>/ <REPO_NAME>` • Branch name : Dieser muss mit dem Namen einer Verzweigung in Ihrem Bitbucket-Reposito ry übereinstimmen. Dieser Zweig muss nicht vorhanden sein, wenn Sie den AWS- CloudForm ation Stack ausführen, ist aber für die Bereitste llung von Code in der Umgebung erforderlich. • Projektname: Dies ist der Name, der dem Amplify-P rojekt zugeordnet werden soll. 5. Wählen Sie Weiter und dann Stack erstellen aus.	

Testen der CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Code in der Verzweigung in Ihrem Repository bereit.	1. Klonen Sie Ihr Bitbucket-Repository, indem Sie den folgenden Befehl ausführen: `git clone https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` 2. Sehen Sie sich den Branch-Namen an, der beim Ausführen des AWS-CloudFormation Skripts verwendet wurde. Um einen neuen Zweig zu erstellen und auszuchecken, führen Sie den `git checkout -b <BRANCH_NAME>` Befehl aus. Führen Sie den `git checkout <BRANCH_NAME>` Befehl aus, um eine vorhandene Verzweigung auszuchecken. 3. Übergeben Sie den Code in den Zweig und übertragen Sie ihn an den Remote-Zweig, indem Sie die `git push` Befehle `git commit` und ausführen. 4. Amplify erstellt und stellt dann die Anwendung bereit.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen dazu finden Sie unter Grundlegende Git-Befehle in der Bitbucket-Dokumentation.	

Zugehörige Ressourcen

Authentifizierungsmethoden (Atlassische Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Starten eines CodeBuild Projekts über AWS-Konten hinweg mithilfe von Step Functions und einer Lambda-Proxy-Funktion

Erstellt von Richard Milner-Watts (AWS) und Amit Anjarlekar (AWS)

Code-Repository: Kontoüber greifender CodeBuild Proxy	Umgebung: Produktion	Technologien: DevOps; Management und Governanc e; Betrieb; Serverless
AWS-Services: AWS CodeBuild; AWS Lambda ; AWS Step Functions ; AWS X-Ray ; AWS CloudFormation		

Übersicht

Dieses Muster zeigt, wie ein AWS- CodeBuild Projekt asynchron über mehrere AWS-Konten hinweg gestartet wird, indem AWS Step Functions und eine AWS Lambda-Proxy-Funktion verwendet werden. Sie können den Step Functions-Zustandsautomaten des Musters verwenden, um den Erfolg Ihres CodeBuild Projekts zu testen.

CodeBuild hilft Ihnen, operative Aufgaben mit der AWS Command Line Interface (AWS CLI) aus einer vollständig verwalteten Laufzeitumgebung zu starten. Sie können das Verhalten Ihres CodeBuild Projekts zur Laufzeit ändern, indem Sie Umgebungsvariablen überschreiben. Darüber hinaus können Sie verwenden, CodeBuild um Workflows zu verwalten. Weitere Informationen finden Sie unter Service Catalog Tools auf der AWS Workshop-Website und Planen von Aufträgen in Amazon RDS for PostgreSQL mit AWS CodeBuild und Amazon EventBridge im AWS Database Blog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten: ein Quellkonto für den Aufruf einer Lambda-Proxy-Funktion mit Step Functions und ein Zielkonto für die Erstellung eines Remote- CodeBuild Beispielprojekts

Einschränkungen

- Dieses Muster kann nicht verwendet werden, um Artefakte zwischen Konten zu kopieren.

Architektur

Das folgende Diagramm zeigt die Architektur, die dieses Muster erstellt.

Das Diagramm zeigt den folgenden Workflow:

1. Der Step-Functions-Zustandsautomat analysiert die bereitgestellte Eingabezuordnung und ruft die Lambda-Proxy-Funktion (`codebuild-proxy-lambda`) für jedes Konto, jede Region und jedes Projekt auf, das Sie definiert haben.
2. Die Lambda-Proxy-Funktion verwendet AWS Security Token Service (AWS STS), um eine IAM-Proxy-Rolle (`codebuild-proxy-role`) anzunehmen, die einer IAM-Richtlinie (`codebuild-proxy-policy`) im Zielkonto zugeordnet ist.
3. Mit der angenommenen Rolle startet die Lambda-Funktion das CodeBuild Projekt und gibt die CodeBuild Auftrags-ID zurück. Der Step-Functions-Zustandsautomat führt Schleifen durch und fragt den CodeBuild Auftrag ab, bis er einen Erfolgs- oder Fehlerstatus erhält.

Die Logik des Zustandsautomaten ist in der folgenden Abbildung dargestellt.

Technologie-Stack

- AWS CloudFormation
- CodeBuild
- IAM
- Lambda
- Step Functions
- X-Ray

Tools

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS CloudFormation Designer bietet einen integrierten JSON- und YAML-Editor, mit dem Sie CloudFormation Vorlagen anzeigen und bearbeiten können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- AWS X-Ray hilft Ihnen, Daten über die Anfragen zu sammeln, die Ihre Anwendung verarbeitet, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren.

Code

Der Beispielcode für dieses Muster ist im GitHubCross-Account- CodeBuild Proxy-Repository verfügbar. Dieses Muster verwendet die AWS Lambda Powertools for Python-Bibliothek, um Protokollierungs- und Ablaufverfolgungsfunktionen bereitzustellen. Weitere Informationen zu dieser Bibliothek und ihren Dienstprogrammen finden Sie unter Powertools für AWS Lambda (Python).

Bewährte Methoden

1. Passen Sie die Wartezeitwerte im Step-Function-Zustandsautomaten an, um Abfrageanforderungen für den Auftragsstatus zu minimieren. Verwenden Sie die erwartete Ausführungszeit für das CodeBuild Projekt.
2. Passen Sie die `MaxConcurrency` Eigenschaft der Karte in Step Functions an, um zu steuern, wie viele CodeBuild Projekte parallel ausgeführt werden können.

3. Überprüfen Sie bei Bedarf den Beispielcode auf Produktionsbereitschaft. Überlegen Sie, welche Daten möglicherweise von der Lösung protokolliert werden und ob die standardmäßige Amazon-CloudWatch Verschlüsselung ausreicht.

Polen

Erstellen der Lambda-Proxy-Funktion und der zugehörigen IAM-Rolle im Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie die AWS-Konto-IDs .	AWS-Konto-IDs sind erforderlich, um den kontenübergreifenden Zugriff einzurichten. Notieren Sie die AWS-Konto-ID für Ihre Quell- und Zielkonten. Weitere Informationen finden Sie unter Suchen Ihrer AWS-Konto-ID in der IAM-Dokumentation.	AWS DevOps
Laden Sie die AWS-CloudFormation Vorlagen herunter.	1. Laden Sie die `sample_target_codebuild_template.yaml` AWS-CloudFormation Vorlage aus dem GitHub Repository für dieses Muster herunter. 2. Laden Sie die`codebuild_lambda_proxy_template.yaml` AWS-CloudFormation Vorlage aus dem GitHub Repository für dieses Muster herunter.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: In den AWS-CloudFormation Vorlagen `<SourceAccountId>` ist die AWS-Konto-ID für das Quellkonto und `<TargetAccountId>` die AWS-Konto-ID für das Zielkonto.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS-CloudFormation Stack und stellen Sie ihn bereit.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Quellkonto an, öffnen Sie die AWS- CloudFormation Konsole und wählen Sie dann Stacks aus. 2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie unter Templete source (Vorlagenquelle) den Wert Upload a template file (Vorlagendatei hochladen) aus. 4. Wählen Sie unter Vorlagendatei hochladen die Option Datei und dann Ihre heruntergeladene `codebuild_lambda_proxy_template.yaml` Datei aus. Wählen Sie Weiter aus. 5. Geben Sie für Stack-Name einen Namen für den Stack ein (z. B. `codebuild-lambda-proxy`). 6. Ersetzen Sie den `crossAccountTargetRoleArn` Parameter durch Ihre `<TargetAccountId>` (z. B. `<arn:aws:iam::123456789012:role/prox`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	y-lambda-codebuild -role>). Hinweis: Sie müssen den Standardw ert für dentargetCod eBuildProject Parameter nicht aktualisi eren. 7. Wählen Sie Weiter, akzeptieren Sie die Standardoptionen für die Stack-Erstellung und wählen Sie dann Weiter aus. 8. Aktivieren Sie das Kontrollk ästchen Ich bestätige, dass AWS IAM-Ressourcen mit benutzerdefinierten Namen erstellen CloudFormation kann, und wählen Sie dann Stack erstellen aus. Hinweis: Sie müssen den AWS- CloudFormation Stack für die Proxy-Lambda-Funkt ion erstellen, bevor Sie Ressourcen in Zielkonten erstellen können. Wenn Sie eine Vertrauensrichtlinie in einem Zielkonto erstellen, wird die IAM-Rolle vom Rollennam en in eine interne Kennung übersetzt. Aus diesem Grund muss die IAM-Rolle bereits vorhanden sein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Erstellung der Proxy-Funktion und des Zustandsautomaten.	1. Warten Sie, bis der AWS-CloudFormation Stack den Status CREATE_COMPLETE erreicht hat. Dies sollte weniger als eine Minute dauern. 2. Öffnen Sie die AWS Lambda-Konsole , wählen Sie Funktionen und suchen Sie dann die `lambda-proxy-ProxyLambda-<GUID>` Funktion . 3. Öffnen Sie die AWS Step Functions-Konsole, wählen Sie Zustandsautomaten aus und suchen Sie dann den `sample-crossaccount-codebuild-state-machine` Zustandsautomaten.	AWS DevOps

Erstellen einer IAM-Rolle im Zielkonto und Starten eines CodeBuild Beispielprojekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS-CloudFormation Stack und stellen Sie ihn bereit.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Zielkonto an, öffnen Sie die AWS- CloudFormation Konsole und wählen Sie dann Stacks aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie unter Templete source (Vorlagenquelle) den Wert Upload a template file (Vorlagendatei hochladen) aus. 4. Wählen Sie unter Vorlagendatei hochladen die Option Datei auswählen und dann die `sample_target_codebuild_template.yaml` Datei aus. Wählen Sie Weiter aus. 5. Geben Sie für Stack-Name einen Namen für den Stack ein (z. B.: `sample-codebuild-stack`). 6. Ersetzen Sie den `crossAccountSourceRoleArn` Parameter durch Ihre <SourceAccountId> (z. B. <arn:aws:iam::123456789012:role/codebuild-proxy-lambda-role>). 7. Wählen Sie Weiter, akzeptieren Sie die Standardoptionen für die Stack-Erstellung und wählen Sie dann Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Aktivieren Sie das Kontrollkästchen Ich bestätige, dass AWS möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen CloudFormation erstellt, und wählen Sie dann Stack erstellen aus.	
Überprüfen Sie die Erstellung des CodeBuild Beispielprojekts.	1. Warten Sie, bis der AWS-CloudFormation Stack den Status CREATE_COMPLETE erreicht. Dies sollte weniger als eine Minute dauern. 2. Öffnen Sie die AWS-CodeBuild Konsole und suchen Sie dann das `sample-codebuild-project` Projekt.	AWS DevOps

Testen der kontoübergreifenden Lambda-Proxy-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Zustandsautomaten.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Quellkonto an, öffnen Sie die AWS Step Functions-Konsole und wählen Sie dann Zustandsautomaten aus. 2. Wählen Sie den `sample-crossaccount-`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`codebuild-state-machine` Zustandsa utomaten und dann Ausführung starten aus. 3. Geben Sie im Eingabe-Editor den folgenden JSON-Code ein und ersetzen Sie durch `<TargetAccountID>` die AWS-Konto -ID des Kontos, das das CodeBuild Projekt enthält. `{ "crossAccountTargetRoleArns": [ { "arn": "arn:aws:iam::<TargetAccountID>:role/proxy-lambda-codebuild-role", "region": "eu-west-1", "codeBuildProject": "sample-codebuild-project", "SampleValue1": "Value1", "SampleValue2": "Value2" } ] }` Hinweis: Die Schlüssel-Wert-Paare werden als Umgebungsvariablen von der Funktion im Quellkont	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	o an das CodeBuild Projekt im Zielkonto übergeben. 4. Wählen Sie Start execution (Ausführung starten) aus. 5. Überprüfen Sie auf der Registerkarte Details der Seite Zustandsautomat, ob der Ausführungsstatus auf Erfolgreich gesetzt ist. Dadurch wird bestätigt, dass Ihr Zustandsautomat ausgeführt wird. Hinweis: Es kann etwa 30 Sekunden dauern, bis der Zustandsa utomat den Status Erfolgrei ch erreicht. 6. Um die Ausgabe und Eingabe eines Schritts im Zustandsautomaten anzuzeigen, erweitern Sie diesen Schritt im Abschnitt Ausführungsereignisverlauf. Erweitern Sie beispiels weise den Schritt Lambda - CodeBuild Proxy – Start. Die Ausgabe enthält Details zu den überschriebenen Umgebungsvariablen, der ursprünglichen Nutzlast und der CodeBuild Auftrags-ID.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Umgebungsvariablen.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Zielkonto an. 2. Öffnen Sie die AWS-CodeBuild Konsole , erweitern Sie Erstellen und wählen Sie dann Projekte erstellen aus. 3. Wählen Sie das `sample-codebuild-project` Projekt und dann Details anzeigen aus. 4. Wählen Sie auf der Registerkarte Build-Verlauf den neuesten Build des Projekts und dann Protokolle anzeigen aus. 5. Überprüfen Sie in der Protokollausgabe, ob die in STDOUT gedruckten Umgebungsvariablen mit den Umgebungsvariablen aus dem Step-Functions-Beispielzustandsautomaten übereinstimmen.	AWS DevOps

Fehlerbehebung

Problem	Lösung
Die Ausführung von Step Functions dauert länger als erwartet.	Passen Sie die -`MaxConcurrency` Eigenschaft der Karte im Step Function-Zustandsautomaten an, um zu steuern, wie viele

Problem	Lösung
	CodeBuild Projekte parallel ausgeführt werden können.
Die Ausführung der CodeBuild Aufträge dauert länger als erwartet.	1. Passen Sie die Wartezeitwerte im Step-Functions-Zustandsautomaten an, um Abfragean forderungen für den Auftragsstatus zu minimieren. Verwenden Sie die erwartete Ausführungszeit für das CodeBuild Projekt. 2. Überlegen Sie, ob CodeBuild das geeignete Tool ist. Beispielsweise kann die zum Initialisieren eines CodeBuild Auftrags erforderliche Zeit deutlich länger sein als AWS Lambda . Wenn ein hoher Durchsatz und schnelle Abschlusszeiten erforderlich sind, sollten Sie die Geschäftslogik auf AWS Lambda migrieren und eine Fan-Out-Architektur verwenden.

Verwalten Sie Blau/Grün-Bereitstellungen von Microservices für mehrere Konten und Regionen mithilfe von AWS-Codeservices und AWS KMS-Schlüsseln für mehrere Regionen

Erstellt von Balaji Vedagiri (AWS), Ashish Kumar (AWS), Faisal Shahdad (AWS), Anand Krishna Varanasi (AWS), Vanitha Dontireddy (AWS) und Vivek Thangamuthu (AWS)

Code-Repository: ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Container und Microservices
AWS-Services: AWS CloudFormation; AWS CodeBuild; AWS CodeDeploy; AWS CodePipeline; Amazon ECS		

Übersicht

Dieses Muster beschreibt, wie eine globale Microservices-Anwendung von einem zentralen AWS-Konto aus in mehreren Workload-Konten und -Regionen gemäß einer Blau/Grün-Bereitstellungsstrategie bereitgestellt wird. Das Muster unterstützt Folgendes:

- Software wird in einem zentralen Konto entwickelt, wohingegen Workloads und Anwendungen auf mehrere Konten und AWS-Regionen verteilt sind.
- Ein einzelner AWS Key Management System (AWS KMS) multiregionaler Schlüssel wird für die Verschlüsselung und Entschlüsselung verwendet, um die Notfallwiederherstellung abzudecken.
- Der KMS-Schlüssel ist regionsspezifisch und muss in drei verschiedenen Regionen für Pipeline-Artefakte verwaltet oder erstellt werden. Ein multiregionaler KMS-Schlüssel trägt dazu bei, dieselbe Schlüssel-ID regionsübergreifend beizubehalten.
- Das Git-Workflow-Verzweigungsmodell wird mit zwei Verzweigungen (Entwicklung und Haupt) implementiert und Code wird mithilfe von Pull-Anforderungen (PRs) zusammengeführt.
  Die AWS Lambda-Funktion, die von diesem Stack bereitgestellt wird, erstellt eine PR vom Entwicklungszweig zum Hauptzweig. Die PR-Zusammenführung mit dem Hauptzweig initiiert

eine AWS- CodePipeline Pipeline, die den CI/CD-Flow (Continuous Integration and Continuous Delivery) orchestriert und die Stacks kontenübergreifend bereitstellt.

Dieses Muster bietet ein Beispiel für die Einrichtung von Infrastructure as Code (IaC) über AWS-CloudFormation Stacks, um diesen Anwendungsfall zu demonstrieren. Die Blau/Grün-Bereitstellung von Microservices wird mithilfe von AWS implementiert CodeDeploy.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Vier aktive AWS-Konten:
  - Ein Tools-Konto zur Verwaltung der Code-Pipeline und zur Verwaltung des AWS- CodeCommit Repositorys.
  - Drei Workload-Konten (Test) für die Bereitstellung des Microservices-Workloads.
- Dieses Muster verwendet die folgenden Regionen. Wenn Sie andere Regionen verwenden möchten, müssen Sie die entsprechenden Änderungen an den AWS- CodeDeploy und AWS KMS-Stacks für mehrere Regionen vornehmen.
  - Tools (AWS CodeCommit)-Konto:`ap-south-1`
  - Workload-Konto (Test) 1:`ap-south-1`
  - Workload-Konto (Test) 2:`eu-central-1`
  - Workload-Konto (Test) 3:`us-east-1`
- Drei Amazon Simple Storage Service (Amazon S3)-Buckets für die Bereitstellungsregionen in jedem Workload-Konto. (Diese werden als `S3BUCKETNAMETESTACCOUNT1` `S3BUCKETNAMETESTACCOUNT2` und `S3BUCKETNAMETESTACCOUNT3` später in diesem Muster bezeichnet.)

  Sie können diese Buckets beispielsweise in bestimmten Konten und Regionen wie folgt mit eindeutigen Bucket-Namen erstellen (ersetzen Siexxxx durch eine Zufallszahl):

```
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-xxxx-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-xxxx-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-xxxx-us-east-1 --region us-east-1
```

```
#Example
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-18903-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-18903-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-18903-us-east-1 --region us-east-1
```

Einschränkungen

Das Muster verwendet AWS CodeBuild und andere Konfigurationsdateien, um einen Beispiel-Microservice bereitzustellen. Wenn Sie einen anderen Workload-Typ haben (z. B. Serverless), müssen Sie alle relevanten Konfigurationen aktualisieren.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CodeCommit
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Zielarchitektur

Automatisierung und Skalierung

Die Einrichtung wird mithilfe von AWS- CloudFormation Stack-Vorlagen (IaC) automatisiert. Es kann einfach für mehrere Umgebungen und Konten skaliert werden.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen in Amazon Elastic Compute Cloud (Amazon EC2) oder On-Premises-Instances, AWS Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS)-Services.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Zusätzliche Tools

- Git ist ein verteiltes Open-Source-Versionsverwaltungssystem, das mit dem AWS- CodeCommit Repository funktioniert.
- Docker ist eine Reihe von Platform as a Service (PaaS)-Produkten, die Virtualisierung auf Betriebssystemebene verwenden, um Software in Containern bereitzustellen. Dieses Muster verwendet Docker, um Container-Images lokal zu erstellen und zu testen.
- cfn-lint und cfn-nag sind Open-Source-Tools, mit denen Sie CloudFormation Stacks auf Fehler und Sicherheitsprobleme überprüfen können.

Code-Repository

Der Code für dieses Muster ist in den GitHub globalen Blau/Grün-Bereitstellungen in mehreren Regionen und Konten-Repository verfügbar.

Sekunden

Einrichten von Umgebungsvariablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Umgebungsvariablen für die CloudFormation Stack-Bereitstellung.	Definieren Sie Umgebungsvariablen, die später in diesem Muster als Eingabe für die CloudFormation Stacks verwendet werden.
	1. Aktualisieren Sie die Bucket-Namen, die Sie in den drei Konten und Regionen erstellt haben, wie zuvor im Abschnitt Voraussetzungen erläutert:
	`export S3BUCKETNAMETESTACCOUNT1=<S3BUCKETACCOUNT1>`
	`export S3BUCKETNAMETESTACCOUNT2=<S3BUCKETACCOUNT2>`
	`export S3BUCKETNAMETESTACCOUNT3=<S3BUCKETACCOUNT3>`
	2. Definieren Sie eine zufällige Zeichenfolge, um Artefakt-Buckets zu erstellen, da Bucket-Namen global eindeutig sein müssen:
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`export BUCKETSTARTNAME=ecs-codepipeline-artifacts-19992`
	3. Definieren und exportieren Sie die Konto-IDs und Regionen:
	`export TOOLSACCOUNT=<TOOLSACCOUNT>`
	`export CODECOMMITACCOUNT=<CODECOMMITACCOUNT>`
	`export CODECOMMITREGION=ap-south-1`
	`export CODECOMMITREPONAME=Poc`
	`export TESTACCOUNT1=<TESTACCOUNT1>`
	`export TESTACCOUNT2=<TESTACCOUNT2>`
	`export TESTACCOUNT3=<TESTACCOUNT3>`
	`export TESTACCOUNT1REGION=ap-south-1`
	`export TESTACCOUNT2REGION=eu-central-1`
	`export TESTACCOUNT3REGION=us-east-1`
	`export TOOLSACCOUNTREGION=ap-south-1`
	`export ECRREPOSITORYNAME=web`	

Verpacken und Bereitstellen der CloudFormation Stacks für die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	Klonen Sie das Beispiel-Repository in ein neues Repository an Ihrem Speicherort:
	`##In work location`
	`git clone https://github.com/aws-samples/ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline.git`
		AWS DevOps

Verpacken Sie die Cloudformation-Ressourcen.	In diesem Schritt verpacken Sie die lokalen Artefakte, auf die die CloudFormation Vorlagen verweisen, um die Infrastrukturressourcen zu erstellen, die für Services wie Amazon Virtual Private Cloud (Amazon VPC) und Application Load Balancer erforderlich sind.
	Die Vorlagen sind im `Infra` Ordner des Code-Repositorys verfügbar.
	`##In TestAccount1##`
	`aws cloudformation package \`
	`--template-file mainInfraStack.yaml \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	--s3-bucket $S3BUCKETNAMETESTACCOUNT1 \ --s3-prefix infraStack \ --region $TESTACCOUNT1REGION \ --output-template-file infrastructure_${TESTACCOUNT1}.template ##In TestAccount2## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT2 \ --s3-prefix infraStack \ --region $TESTACCOUNT2REGION \ --output-template-file infrastructure_${TESTACCOUNT2}.template ##In TestAccount3## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT3 \ --s3-prefix infraStack \	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--region $TESTACCOUNT3REGION \` `--output-template-file infrastructure_${TESTACCOUNT3}.template`	

Validieren Sie die Paketvorlagen.	Validieren Sie die Paketvorlagen:
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT1}.template`
	
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT2}.template`
	
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT3}.template`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Paketdateien in den Workload-Konten bereit.	1. Aktualisieren Sie die Platzhalterwerte und Kontonamen im `infraParameters.json` -Skript basierend auf Ihrer Einrichtung.
	2. Stellen Sie die Paketvorlagen in Ihren drei Workload-Konten bereit.
	
	`##In TestAccount1##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT1}.template \`
	`--stack-name mainInfrastack \`
	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT1REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount2##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT2}.template \`
	`--stack-name mainInfrastack \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	--parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT2REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM ##In TestAccount3## aws cloudformation deploy \ --template-file infrastructure_${TESTACCOUNT3}.template \ --stack-name mainInfrastack \ --parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT3REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM	

Übertragen eines Beispielbilds und Skalieren von Amazon ECS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie ein Beispiel-Image in das Amazon-ECR-Repository.	Verschieben Sie ein Beispiel-Image (NGINX) in das Amazon Elastic Container Registry (Amazon ECR)-Repository mit dem Namen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`web` (wie in den Parametern festgelegt). Sie können das Image nach Bedarf anpassen.
	
	Um sich anzumelden und die Anmeldeinformationen für das Pushen eines Images an Amazon ECR festzulegen, folgen Sie den Anweisungen in der Amazon-ECR-Dokumentation.
	
	Die Befehle sind:
	
	`docker pull nginx`
	`docker images`
	`docker tag <imageid> aws_account_id.dkr.ecr.region.amazonaws.com/<web>:latest`
	`docker push <aws_account_id>.dkr.ecr.<region>.amazonaws.com/<web>:tag`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Skalieren Sie Amazon ECS und überprüfen Sie den Zugriff.	1. Skalieren Sie Amazon ECS, um zwei Replikate zu erstellen: `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 2` wobei sich auf Ihre Beispielanwendung `Poc-Service` bezieht. 2. Stellen Sie sicher, dass die Services vom Application Load Balancer aus zugänglich sind, indem Sie einen vollqualifizierten Domainnamen (FQDN) oder DNS von einem Browser oder mit dem Befehl curl verwenden.	AWS DevOps

Einrichten von Code-Services und -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository im -Tools-Konto.	Erstellen Sie ein CodeCommit Repository im Tools-Konto, indem Sie die `codecommit.yaml` Vorlage verwenden, die sich im `code` Ordner des GitHub Repositorys befindet. Sie dürfen dieses Repositor	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	y nur in der einzelnen Region erstellen, in der Sie den Code entwickeln möchten. `aws cloudformation deploy --stack-name codecommitrepoStack --parameter-overrides CodeCommitReponame=$CODECOMMITREPONAME \ ToolsAccount=$TOOLSACCOUNT --template-file codecommit.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket zum Verwalten von Artefakten, die von generiert wurden CodePipeline.	Erstellen Sie einen S3-Bucket zum Verwalten von Artefakten, die CodePipeline mit der `pre-reqs-bucket.yaml` Vorlage generiert wurden, die sich im `code` Ordner des GitHub Repositorys befindet. Die Stacks müssen in allen drei Workload- (Test-) und Tools-Konten und -Regionen bereitgestellt werden. `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen multiregionalen KMS-Schlüssel ein.	1. Erstellen Sie einen multiregionalen KMS-Schlüssel mit Primär- und Replikatschlüsseln, die verwenden CodePipeline wird. In unserem Beispiel `ToolsAccount1region - ap-south-1` wird die primäre Region sein. `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Legen Sie die CMKARN-Variablen fest, die an CodeBuild Projekte übergeben werden sollen. Die Werte sind in der Ausgabe des ecs-codepipeline-pre-reqs-KMS-Vorlagen-Stacks verfügbar (die Schlüssel-ID ist in	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	allen Regionen gleich und beginnt mit `mrk-`). Oder Sie können die CMKARN-We rte aus dem Tools-Konto abrufen. Exportieren Sie sie in allen Kontositzungen: `export CMKARN1=a rn:aws:kms:ap-sout h-1:<TOOLSACCOUNTI D>:key/mrk-xxx export CMKARN2=a rn:aws:kms:eu-cent ral-1:<TOOLSACCOUN TID>:key/mrk-xxx export CMKARN3=a rn:aws:kms:us-east -1:<TOOLSACCOUNTID >:key/mrk-xxx export CMARNTOOL S=arn:aws:kms:ap-s outh-1:<TOOLSACCOU NTID>:key/mrk-xxx`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das CodeBuild Projekt im -Tools-Konto ein.	1. Verwenden Sie die `codebuild_IAM.yaml` Vorlage aus dem `code` Ordner des GitHub Repositorys, um AWS Identity and Access Management (IAM) für AWS CodeBuild in einer einzigen Region im Tools-Konto einzurichten:
	`#In ToolsAccount aws cloudformation deploy --stack-name ecs-codebuild-iam \ --template-file codebuild_IAM.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`
	2. Verwenden Sie die `codebuild.yaml` Vorlage, um CodeBuild für Ihr Build-Projekt einzurichten. Stellen Sie diese Vorlage in allen drei Regionen wie folgt bereit:
	`aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOLSACCOUNT \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT1 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN1 \ --template-file codebuild.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOL SACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN2 \ --template-file codebuild.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws cloudformation deploy --stack-name ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT3 \ CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN3 \ --template-file codebuild.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie CodeDeploy in Workload-Konten ein.	Verwenden Sie die `codedeploy.yaml` Vorlage im `code` Ordner des GitHub Repositorys, um CodeDeploy in allen drei Workload-Konten einzurichten. Die Ausgabe von `mainInfraStack` enthält die Amazon-Ressourcenn amen (ARNs) des Amazon-ECS-Clusters und Application Load Balancer-Listeners.
	
	Hinweis: Die Werte aus den Infrastruktur-Stacks werden bereits exportiert, daher werden sie von den CodeDeploy Stack-Vorlagen importiert.
	
	`##WorkloadAccount1##`
	`aws cloudformation deploy --stack-name ecscodedeploystack \`
	`--parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \`
	`--template-file codedeploy.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`
	
	`##WorkloadAccount2##`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \ --template-file codedeploy.yaml --region $TESTACCOUNT2REGION --capabilities CAPABILITY_NAMED_IAM`
	
	`##WorkloadAccount3## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \ --template-file codedeploy.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM`	

Einrichten CodePipeline im -Tools-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Code-Pipeline im -Tools-Konto.	Führen Sie im Tools-Konto den Befehl aus:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws cloudformation deploy --stack-name ecscodepipelinestack --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount1Region=$TESTACCOUNT1REGION \ TestAccount2=$TESTACCOUNT2 TestAccount2Region=$TESTACCOUNT2REGION \ TestAccount3=$TESTACCOUNT3 TestAccount3Region=$TESTACCOUNT3REGION \ CMKARNTools=$CMKTROOLSARN CMKARN1=$CMKARN1 CMKARN2=$CMKARN2 CMKARN3=$CMKARN3 \ CodeCommitRepoName=$CODECOMMITREPONAME BucketStartName=$BUCKETSTARTNAME \ --template-file codepipeline.yaml --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff für - CodePipeline und - CodeBuild Rollen in der AWS KMS-Schlüsselrichtlinie und der S3-Bucket-Richtlinie.	1. Gewähren Sie Zugriff für - CodePipeline und - CodeBuild Rollen in der AWS KMS-Schlüsselrichtlinie: `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ CodeBuildCondition=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Aktualisieren Sie die S3-Bucket-Richtlinie, um den Zugriff für - CodePipeline und - CodeDeploy Rollen zu ermöglichen: `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rtName=$BUCKETSTAR TNAME \ PutS3BucketPolic y=true TestAccou nt1=$TESTACCOUNT1 TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ PutS3BucketPolic y=true TestAccou nt1=$TESTACCOUNT1 TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Aufrufen und Testen der Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie Änderungen in das CodeCommit Repository.	1. Klonen Sie das CodeCommit Repository, das in der erstellt wurde, `codecommitrepoStack` mithilfe des `git clone` Befehls , wie in der AWS-CodeCommit Dokumentation beschrieben. 2. Aktualisieren Sie die Eingabeartefakte mit den erforderlichen Details: • JSON-Datei: Aktualisieren Sie `AccountID` die Datei an drei Stellen dieser Datei. Benennen Sie die drei Dateien so um, dass sie die Konto-IDs enthalten. • YAML-Dateien: Aktualisieren Sie den ARN und die Version der Aufgabendefinition. Benennen Sie die drei	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Dateien so um, dass sie die Konto-IDs enthalten.
	3. Ändern Sie die `index.html` Datei, um einige kleinere Änderungen an der -Startseite vorzunehmen.
	4. Kopieren Sie die folgenden Dateien in das Repository und führen Sie ein Commit durch:
	`index.html`
	`Dockerfile`
	`buildspec.yaml`
	`appspec_<accountid>.yaml (3 files - one per account )`
	`taskdef<accountid>.json (3 files - one per account)`
	5. Starten oder starten Sie die Pipeline neu und überprüfen Sie die Ergebnisse.
	6. Greifen Sie über einen FQDN oder DNS auf den Service vom Application Load Balancer aus zu und überprüfen Sie, ob die Updates bereitgestellt wurden.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen Sie alle bereitgestellten Ressourcen.	1. Skalieren Sie Amazon ECS auf null Instances herunter:
	`aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 0`
	2. Löschen Sie die CloudFormation Stacks in jedem Konto und jeder Region:
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name ecscodepipelinestack --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT1REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT2REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT3REGION`
	`aws cloudformation delete-stack --stack-name ecs-codepipeline-pre-reqs-K`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	MS --region $TOOLSACC OUNTREGION aws cloudformation delete-stack -- stack-name codecommi trepoStack --region $TOOLSACCOUNTREGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT1REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT2REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT3REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TOOLSACC OUNTREGION aws cloudformation delete-stack -- stack-name ecs-codeb uild-iam --region $TOOLSACCOUNTREGION ##NOTE: Artifact buckets will not get deleted if there are artifacts so it has to be emptied	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	manually before deleting.##	
	##In Workload / Test Accounts## ##Account:1## aws cloudformation delete-stack --stack-name ecscodedeploystack --region $TESTACCOUNT1REGION aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT1REGION ##Account:2## aws cloudformation delete-stack --stack-name ecscodedeploystack --region $TESTACCOUNT2REGION aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT2REGION ##Account:3## aws cloudformation delete-stack --stack-name ecscodedeploystack --region $TESTACCOUNT3REGION aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT3REGION ##NOTE: Amazon ECR (web) will not get deleted if	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`the registry still includes images. It can be manually cleaned up if not required.`	

Fehlerbehebung

Problem	Lösung
Änderungen, die Sie an das Repository übergeben haben, werden nicht bereitgestellt.	• Überprüfen Sie die CodeBuild Protokolle in der Docker-Build-Aktion auf Fehler. Weitere Informationen finden Sie in der CodeBuild - Dokumentation. • Überprüfen Sie die CodeDeploy Bereitstellung auf Probleme mit der Amazon-ECS-Bereitstellung.

Zugehörige Ressourcen

- Pushen eines Docker-Images (Amazon-ECR-Dokumentation)
- Herstellen einer Verbindung mit einem AWS- CodeCommit Repository (AWS- CodeCommit Dokumentation)
- Fehlerbehebung bei AWS CodeBuild (AWS- CodeBuild Dokumentation)

Überwachen von Amazon ECR-Repositorys auf Platzhalterberechtigungen mit AWS CloudFormation und AWS Config

Erstellt von Vit Telkar (AWS), Sajid Momin (AWS) und Wassim Benhallam (AWS)

Umgebung: Produktion	Technologien: DevOps; Container und Microservices	AWS-Services: AWS CloudFormation; AWS Config ; Amazon ECR; Amazon SNS ; AWS Lambda

Übersicht

In der Amazon Web Services (AWS) Cloud ist Amazon Elastic Container Registry (Amazon ECR) ein verwalteter Container-Image-Registry-Service, der private Repositorys mit ressourcenbasierten Berechtigungen unter Verwendung von AWS Identity and Access Management (IAM) unterstützt.

IAM unterstützt den Platzhalter „*“ sowohl in den Ressourcen- als auch in den Aktionsattributen, was die automatische Auswahl mehrerer übereinstimmender Elemente erleichtert. In Ihrer Testumgebung können Sie allen authentifizierten AWS-Benutzern den Zugriff auf ein Amazon ECR-Repository erlauben, indem Sie die `ecr:*` Platzhalterberechtigung in einem Prinzipalelement für Ihre Repository-Richtlinienanweisung verwenden. Die `ecr:*` Platzhalterberechtigung kann nützlich sein, wenn Sie Entwicklungskonten entwickeln und testen, die nicht auf Ihre Produktionsdaten zugreifen können.

Sie müssen jedoch sicherstellen, dass die `ecr:*` Platzhalterberechtigung in Ihren Produktionsumgebungen nicht verwendet wird, da sie zu schwerwiegenden Sicherheitsschwachstellen führen kann. Der Ansatz dieses Musters hilft Ihnen, Amazon-ECR-Repositorys zu identifizieren, die die `ecr:*` Platzhalterberechtigung in Repository-Richtlinienanweisungen enthalten. Das Muster enthält Schritte und eine AWS- CloudFormation Vorlage zum Erstellen einer benutzerdefinierten Regel in AWS Config . Eine AWS Lambda-Funktion überwacht dann Ihre Amazon ECR-Repository-Richtlinienanweisungen auf `ecr:*` Platzhalterberechtigungen. Wenn nicht konforme Repository-Richtlinienanweisungen gefunden werden, benachrichtigt Lambda AWS Config, um ein Ereignis an Amazon zu senden, EventBridge und initiiert EventBridge dann ein Amazon Simple Notification Service (Amazon SNS)-

Thema. Das SNS-Thema benachrichtigt Sie per E-Mail über die nicht konformen Repository-Richtlinienanweisungen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI in der AWS CLI-Dokumentation.
- Ein vorhandenes Amazon-ECR-Repository mit einer angehängten Richtlinienanweisung, das in Ihrer Testumgebung installiert und konfiguriert ist. Weitere Informationen dazu finden Sie unter Erstellen eines privaten Repositorys und Festlegen einer Repository-Richtlinienanweisung in der Amazon-ECR-Dokumentation.
- AWS Config , konfiguriert in Ihrer bevorzugten AWS-Region. Weitere Informationen dazu finden Sie unter Erste Schritte mit AWS Config in der AWS Config-Dokumentation.
- Die `aws-config-cloudformation.template` Datei (angefügt), die auf Ihren lokalen Computer heruntergeladen wurde.

Einschränkungen

- Die Lösung dieses Musters ist regional und Ihre Ressourcen müssen in derselben Region erstellt werden.

Architektur

Das folgende Diagramm zeigt, wie AWS Config Amazon ECR-Repository-Richtlinienanweisungen auswertet.

Das Diagramm zeigt den folgenden Workflow:

1. AWS Config initiiert eine benutzerdefinierte Regel.

2. Die benutzerdefinierte Regel ruft eine Lambda-Funktion auf, um die Compliance der Amazon-ECR-Repository-Richtlinienanweisungen zu bewerten. Die Lambda-Funktion identifiziert dann nicht konforme Repository-Richtlinienanweisungen.
3. Die Lambda-Funktion sendet den Status der Nichtkonformität an AWS Config .
4. AWS Config sendet ein Ereignis an EventBridge.
5. EventBridge veröffentlicht die Benachrichtigungen über Compliance-Nichtkonformität in einem SNS-Thema.
6. Amazon SNS sendet eine E-Mail-Warnung an Sie oder einen autorisierten Benutzer.

Automatisierung und Skalierung

Die Lösung dieses Musters kann eine beliebige Anzahl von Amazon-ECR-Repository-Richtlinienanweisungen überwachen, aber alle Ressourcen, die Sie auswerten möchten, müssen in derselben Region erstellt werden.

Tools

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.
- AWS Config – AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.
- Amazon ECR – Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. Amazon ECR unterstützt private Container-Image-Repositories mit ressourcenbasierten Berechtigungen unter Verwendung von IAM.
- Amazon EventBridge – Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren Anwendungen, Software-as-a-Service (SaaS)-Anwendungen und AWS-Services für Ziele wie AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen Konten bereit.

- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Der Code für dieses Muster ist in der `aws-config-cloudformation.template` Datei verfügbar (angefügt).

Polen

Erstellen des AWS- CloudFormation Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS-CloudFormation Stack.	Erstellen Sie einen AWS-CloudFormation Stack, indem Sie den folgenden Befehl in AWS CLI ausführen: `$ aws cloudformation create-stack --stack-name=AWSConfigECR \ --template-body file://aws-config-cloudformation.template \ --parameters ParameterKey=<email>,ParameterValue=<myemail@example.com> \`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--capabilities CAPABILITY_NAMED_IAM`	

Testen der benutzerdefinierten AWS Config-Regel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die benutzerd efinierte AWS Config-Regel.	1. Melden Sie sich bei der AWS-Managementkons ole an, öffnen Sie die AWS Config-Konsole und wählen Sie dann Ressourcen aus. 2. Auf der Seite Ressource nbestand können Sie nach Ressourcenkategori e, Ressourcentyp und Compliance-Status filtern. 3. Ein Amazon-ECR-Reposit ory, das enthält, `ecr:*` ist `NON-COMPLIANT?` und ein Amazon-ECR-Reposit ory, das nicht enthält, `ecr:*` ist `COMPLIANT` . 4. Die E-Mail-Adresse, die das SNS-Thema abonniert hat, erhält Benachrichtigungen , wenn ein Amazon ECR-Repository nicht konforme Richtlinienanweisungen enthält.	AWS DevOps

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Führen Sie benutzerdefinierte Aktionen aus CodeCommit AWS-Ereignissen durch

Erstellt von Abdullahi Olaoye (AWS)

Umgebung: PoC oder Pilot	Technologien: DevOps; Management und Unternehmensführung	AWS-Dienste: AWS CodeCommit; Amazon SNS

Übersicht

Wenn Sie ein CodeCommit AWS-Repository zum Speichern von Code verwenden, möchten Sie möglicherweise das Repository überwachen und bei bestimmten Ereignissen einen Aktionsablauf einleiten. Beispielsweise möchten Sie möglicherweise eine E-Mail-Benachrichtigung senden, wenn ein Benutzer eine Codezeile in einem Commit kommentiert, oder eine AWS-Lambda-Funktion initiieren, um nach einem Commit Sicherheitsscans der Repository-Inhalte durchzuführen. Dieses Muster beschreibt die Schritte zur Konfiguration eines CodeCommit Repositorys für benutzerdefinierte Aktionen. Das Muster verwendet CodeCommit AWS-Benachrichtigungsregeln, um die relevanten Ereignisse zu erfassen, und sendet diese Ereignisse dann an ein konfiguriertes Ziel.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vertrautheit mit Git-Befehlen.
- AWS CodeCommit, eingerichtet. Anweisungen finden Sie unter Einrichtung für AWS CodeCommit.
- (Empfohlen) AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Anweisungen finden Sie unter Erste Schritte mit der AWS-CLI.

Architektur

Tools

AWS-Services

- AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet. Es erleichtert Teams die Zusammenarbeit an Code in einem sicheren und hoch skalierbaren Ökosystem. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen
- Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen. Amazon SNS bietet Themen (Kommunikationskanäle) für Push-basiertes Messaging mit hohem Durchsatz. many-to-many Mithilfe von Amazon SNS SNS-Themen können Herausgeber Nachrichten zur parallel Verarbeitung an eine große Anzahl von Abonnenten verteilen, einschließlich Amazon Simple Queue Service (Amazon SQS) -Warteschlangen, AWS Lambda Lambda-Funktionen und HTTP/S-Webhooks. Sie können Amazon SNS auch verwenden, um Benachrichtigungen per Push, SMS und E-Mail an Endbenutzer zu senden.

Epen

Richten Sie ein Repository ein CodeCommit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Verwenden Sie die CodeCommit Konsole oder die AWS-CLI, um ein CodeCommi t Repository zu erstellen. Anweisungen finden Sie unter Erstellen eines CodeCommit Repositorys.	DevOps Ingenieur
Inhalte in das CodeCommit Repository übertragen.	Nachdem Sie ein Repositor y erstellt haben, fügen Sie ihm mithilfe von Git-Befeh len Inhalte hinzu. Sie können den Inhalt eines vorhandenen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Git-Repositorys oder lokale, unversionierte Inhalte von Ihrem Computer migrieren. Anweisungen finden Sie unter Dateien zu Ihrem Repository hinzufügen oder Zu AWS migrieren CodeCommit.	

Einrichten von Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Dieses SNS-Thema erhält die Ereignisse von CodeCommit. Anweisungen finden Sie unter Erstellen eines Amazon SNS SNS-Themas.	Cloud-Architekt, Ingenieur DevOps
Erstellen Sie eine Ressource für eine benutzerdefinierte Aktion.	Damit die benutzerdefinierte Aktion ausgeführt werden kann, müssen Sie die entsprechende Ressource erstellen. Wenn Ihre benutzerdefinierte Aktion beispielsweise darin besteht, Lambda-Code auszuführen und Nachrichten an eine SQS-Warteschlange zu senden, müssen Sie die Lambda-Funktion und die SQS-Warteschlange erstellen. Aktionen wie E-Mail- und SMS-Benachrichtigungen benötigen keine Ressourcen. Weitere Informationen finden Sie in der AWS-Dokum	Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	entation für den Ressource ntyp, den Sie erstellen.	
Abonnieren Sie die Ressource für benutzerdefinierte Aktionen zum SNS-Thema.	Abhängig von der benutzerd efinierten Aktion erstellen Sie ein Abonnement für das entsprechende Protokoll. Sie abonnieren beispielsweise eine E-Mail-Adresse für E-Mail-Benachrichtigungen, eine Lambda-Funktion zum Ausführen von benutzerd efiniertem Code oder eine SQS-Warteschlange, um Ereignisse an Amazon SQS zu senden. Bei Abonnemen tprotokollen wie E-Mail und SMS müssen Sie das Abonnement über den Link bestätigen, der an die E-Mail bzw. Telefonnummer gesendet wird. Anweisungen finden Sie unter Amazon SNS abonnieren.	Cloud-Architekt, Ingenieur DevOps

Benachrichtigungsregeln konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Benachric htigungsregel für das CodeCommit Repository.	Wenn Sie die Benachric htigungsregel erstellen, wählen Sie die Git-Ereignisse aus, die die Benachrichtigung auslösen sollen, wählen Sie das SNS-Thema als Zieltyp	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus und wählen dann das SNS-Thema aus, das Sie zuvor erstellt haben. Sie können auch mehrere Ziele für das Repository konfigurieren. Anweisungen finden Sie unter Eine Benachrichtigungsregel erstellen.	
Testen Sie benutzerdefinierte Aktionen.	Führen Sie eines der Ereignisse aus, die für die Initiierung der Benachrichtigung konfiguriert wurden. Erstellen Sie beispielsweise eine Pull-Anfrage, wenn Sie dieses Ereignis als Auslöser ausgewählt haben. Sie sollten sehen, dass Ihre benutzerdefinierte Aktion ausgeführt wird. Wenn Sie beispielsweise eine E-Mail-Adresse für das SNS-Thema abonniert haben, sollten Sie eine E-Mail-Benachrichtigung erhalten.	DevOps Ingenieur

Zugehörige Ressourcen

- CodeCommit AWS-Dokumentation
- Amazon SNS SNS-Dokumentation
- Git-Dokumentation

Veröffentlichen von Amazon- CloudWatch Metriken in einer CSV-Datei

Erstellt von Abdullahi Olaoye (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps	AWS-Services: Amazon CloudWatch

Übersicht

Dieses Muster verwendet ein Python-Skript, um Amazon- CloudWatch Metriken abzurufen und die Metrikinformationen zur besseren Lesbarkeit in eine CSV-Datei (durch Kommas getrennte Werte) zu konvertieren. Das Skript verwendet den AWS-Service, dessen Metriken abgerufen werden sollen, als erforderliches Argument. Sie können die AWS-Region und das AWS-Anmeldeinformationsprofil als optionale Argumente angeben. Wenn Sie diese Argumente nicht angeben, verwendet das Skript die Standardregion und das Profil, die für die Workstation konfiguriert sind, auf der das Skript ausgeführt wird. Nachdem das Skript ausgeführt wurde, wird eine CSV-Datei generiert und im selben Verzeichnis gespeichert.

Im Abschnitt Anhänge finden Sie das Skript und die zugehörigen Dateien, die mit diesem Muster bereitgestellt werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Python 3.x
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)

Einschränkungen

Das Skript unterstützt derzeit die folgenden AWS-Services:

- AWS Lambda
- Amazon Elastic Compute Cloud (Amazon EC2)

  - Standardmäßig erfasst das Skript keine Volume-Metriken von Amazon Elastic Block Store (Amazon EBS). Um Amazon-EBS-Metriken zu erfassen, müssen Sie die angehängte `metrics.yaml` Datei ändern.
- Amazon Relational Database Service (Amazon RDS)
  - Das Skript unterstützt jedoch nicht Amazon Aurora.
- Application Load Balancer
- Network Load Balancer
- Amazon API Gateway

Tools

- Amazon CloudWatch ist ein Überwachungsservice, der für DevOps Techniker entwickelt wurde. Entwickler, Site Reliability Engineers (SREs), und IT-Manager. CloudWatch bietet Daten und verwertbare Erkenntnisse, die Sie bei der Überwachung Ihrer Anwendungen unterstützen. auf systemweite Leistungsänderungen reagieren, Optimieren der Ressourcenauslastung, und erhalten einen einheitlichen Überblick über den Betriebsstatus. CloudWatch erfasst Überwachungs- und Betriebsdaten in Form von Protokollen, -Metriken, - und -Ereignisse, und bietet eine einheitliche Ansicht der AWS-Ressourcen. -Anwendungen, und Services, die auf AWS und On-Premises-Servern ausgeführt werden.

Polen

Installieren und Konfigurieren der Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Vorausset zungen.	Führen Sie den folgenden Befehl aus: `$ pip3 install -r requirements.txt`	Developer
Konfigurieren Sie die AWS CLI.	Führen Sie den folgenden Befehl aus:	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ aws configure`	

Konfigurieren des Python-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie das Skript.	Um die Standardkonfiguration des Skripts zu ändern, öffnen Sie `metrics.yaml` .	Developer
Legen Sie den Zeitraum für das Skript fest.	Dies ist der abzurufende Zeitraum. Der Standardz eitraum beträgt 5 Minuten (300 Sekunden). Sie können den Zeitraum ändern, beachten Sie jedoch die folgenden Einschränkungen: • Wenn der von Ihnen angegebene Stundenwert zwischen 3 Stunden und 15 Tagen liegt, verwenden Sie ein Vielfaches von 60 Sekunden (1 Minute) für den Zeitraum. • Wenn der von Ihnen angegebene Stundenwert zwischen 15 Stunden und 63 Tagen liegt, verwenden Sie ein Vielfaches von 300 Sekunden (5 Minuten) für den Zeitraum. • Wenn der von Ihnen angegebene Stundenwert	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	vor mehr als 63 Tagen liegt, verwenden Sie ein Vielfache s von 3 600 Sekunden (1 Stunde) für den Zeitraum. Andernfalls gibt die API-Operation keine Datenpunkte zurück.	
Legen Sie die Stunden für das Skript fest.	Dieser Wert gibt an, wie viele Stunden an Metriken Sie abrufen möchten. Die Standardeinstellung ist 1 Stunde. Um Metriken für mehrere Tage abzurufen , geben Sie den Wert in Stunden an. Geben Sie beispielsweise für 2 Tage 48 an.	Developer
Ändern Sie die Statistikwerte für das Skript.	(Optional) Der globale Statistikwert ist `Average`, der beim Abrufen von Metriken verwendet wird, denen kein bestimmter Statistikwert zugewiesen ist. Das Skript unterstützt die Statistikwerte `Maximum`, `SampleCount` und `Sum`.	Developer

Ausführen des Python-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie das Skript aus.	Verwenden Sie den folgenden Befehl:
	`$ python3 cwreport.py <service>`
	Führen Sie den folgenden Befehl aus, um eine Liste der Servicewerte und der optionalen `profile` Parameter `region` und anzuzeigen:
	`$ python3 cwreport.py -h`
	Weitere Informationen zu den optionalen Parametern finden Sie im Abschnitt Zusätzliche Informationen.
		Developer

Zugehörige Ressourcen

- Konfigurieren der AWS CLI
- Verwenden von Amazon- CloudWatch Metriken
- Amazon- CloudWatch Dokumentation
- EC2 CloudWatch -Metriken
- AWS Lambda-Metriken
- Amazon-RDS-Metriken
- Application Load Balancer-Metriken
- Network Load Balancer-Metriken

- Amazon API Gateway-Metriken

Zusätzliche Informationen

Skriptnutzung

```
$ python3 cwreport.py -h
```

Beispielsyntax

```
python3 cwreport.py <service> <--region=Optional Region> <--profile=Optional credential
 profile>
```

Parameter

- service (erforderlich) Der Service, für den Sie das Skript ausführen möchten. Das Skript unterstützt derzeit die folgenden Services: AWS Lambda ,Amazon EC2, Amazon RDS, Application Load Balancer, Network Load Balancer und API Gateway.
- region (optional) Die AWS-Region, aus der Metriken abgerufen werden sollen. Die Standardregion ist `ap-southeast-1`.
- profile (optional) Das zu verwendende benannte AWS CLI-Profil. Wenn dieser Parameter nicht angegeben ist, wird das standardmäßig konfigurierte Anmeldeinformationsprofil verwendet.

Beispiele

- So verwenden Sie die Standardregion `ap-southeast-1` und die standardmäßig konfigurierten Anmeldeinformationen zum Abrufen von Amazon EC2Metriken: `$ python3 cwreport.py ec2`
- So geben Sie eine Region an und rufen API Gateway-Metriken ab: `$ python3 cwreport.py apigateway --region us-east-1`
- So geben Sie ein AWS-Profil an und rufen Amazon EC2-Metriken ab: `$ python3 cwreport.py ec2 --profile testprofile`
- So geben Sie sowohl die Region als auch das Profil an, um Amazon EC2Metriken abzurufen: `$ python3 cwreport.py ec2 --region us-east-1 --profile testprofile`

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Führen Sie Komponententests für Python-ETL-Jobs in AWS Glue mithilfe des Pytest-Frameworks aus

Quellcode-Repository: aws-glue-jobs-unit-testing	Umgebung: Produktion	Technologien: DevOps; Große Datenmengen; Softwaree ntwicklung und Testen
AWS-Dienste: AWS CloudFormation CodeBuild ; AWS CodeCommit; AWS CodePipeline; AWS Glue		

Übersicht

Sie können Komponententests für Python-Jobs zum Extrahieren, Transformieren und Laden (ETL) für AWS Glue in einer lokalen Entwicklungsumgebung ausführen, aber die Replikation dieser Tests in einer DevOps Pipeline kann schwierig und zeitaufwändig sein. Unit-Tests können besonders schwierig sein, wenn Sie den Mainframe-ETL-Prozess auf AWS-Technologie-Stacks modernisieren. Dieses Muster zeigt Ihnen, wie Sie Komponententests vereinfachen und gleichzeitig die bestehende Funktionalität beibehalten, Unterbrechungen wichtiger Anwendungsfunktionen bei der Veröffentlichung neuer Funktionen vermeiden und hochwertige Software beibehalten können. Sie können die Schritte und Codebeispiele in diesem Muster verwenden, um Komponententests für Python-ETL-Jobs in AWS Glue auszuführen, indem Sie das Pytest-Framework in AWS CodePipeline verwenden. Sie können dieses Muster auch verwenden, um mehrere AWS Glue Glue-Jobs zu testen und bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon Elastic Container Registry (Amazon ECR) -Image-URI für Ihre AWS Glue Glue-Bibliothek, heruntergeladen von der Amazon ECR Public Gallery
- Bash-Terminal (auf einem beliebigen Betriebssystem) mit einem Profil für das AWS-Zielkonto und die AWS-Region

- Python 3.10 oder höher
- Pytest
- Moto-Python-Bibliothek zum Testen von AWS-Services

Architektur

Technologie-Stack

- Amazon Elastic Container Registry (Amazon ECR)
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- AWS Glue
- Pytest
- Python
- Python-ETL-Bibliothek für AWS Glue

Zielarchitektur

Das folgende Diagramm beschreibt, wie Unit-Tests für AWS Glue ETL-Prozesse, die auf Python basieren, in eine typische DevOps AWS-Pipeline für Unternehmen integriert werden können.

Das Diagramm zeigt den folgenden Workflow:

1. CodePipeline Verwendet in der Quellphase ein CodeCommit Repository für Quellcode, einschließlich eines Python-ETL-Beispieljobs (`sample.py`), einer Unit-Test-Datei (`test_sample.py`) und einer CloudFormation AWS-Vorlage. CodePipeline Überträgt dann den neuesten Code aus dem Hauptzweig zur weiteren Verarbeitung in das CodeBuild Projekt.
2. In der Erstellungs- und Veröffentlichungsphase wird der neueste Code aus der vorherigen Quellphase mithilfe eines öffentlichen Amazon ECR-Images von AWS Glue auf Einheiten getestet. Anschließend wird der Testbericht für CodeBuild Berichtsgruppen veröffentlicht. Das Container-Image im öffentlichen Amazon ECR-Repository für AWS Glue-Bibliotheken enthält alle Binärdateien, die für die lokale Ausführung und auf Unit-Tests PySparkbasierende ETL-Aufgaben

in AWS Glue erforderlich sind. Das öffentliche Container-Repository hat drei Image-Tags, einen für jede von AWS Glue unterstützte Version. Zu Demonstrationszwecken verwendet dieses Muster das `glue_libs_4.0.0_image_01` Image-Tag. Um dieses Container-Image als Runtime-Image zu verwenden CodeBuild, kopieren Sie den Image-URI, der dem Image-Tag entspricht, den Sie verwenden möchten, und aktualisieren Sie dann die `pipeline.yml` Datei im GitHub Repository für die `TestBuild` Ressource.

3. In der Bereitstellungsphase wird das CodeBuild Projekt gestartet und der Code wird in einem Amazon Simple Storage Service (Amazon S3) -Bucket veröffentlicht, wenn alle Tests erfolgreich sind.
4. Der Benutzer stellt die AWS Glue Glue-Aufgabe mithilfe der CloudFormation Vorlage im `deploy` Ordner bereit.

Tools

AWS-Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Glue ist ein vollständig verwalteter ETL-Service. Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.

Andere Tools

- Python ist eine interpretierte Mehrzweck-Programmiersprache auf hohem Niveau.
- Moto ist eine Python-Bibliothek zum Testen von AWS-Services.
- Pytest ist ein Framework zum Schreiben kleiner Komponententests, die skaliert werden können, um komplexe Funktionstests für Anwendungen und Bibliotheken zu unterstützen.

- Die Python-ETL-Bibliothek für AWS Glue ist ein Repository für Python-Bibliotheken, die bei der lokalen Entwicklung von PySpark Batch-Jobs für AWS Glue verwendet werden.

Code

Der Code für dieses Muster ist im Repository GitHub aws-glue-jobs-unit-testing verfügbar. Das Repository umfasst die folgenden Ressourcen:

- Ein Beispiel für einen Python-basierten AWS Glue Glue-Job im Ordner `src`
- Zugeordnete Unit-Testfälle (erstellt mit dem Pytest-Framework) im Ordner `tests`
- Eine CloudFormation Vorlage (in YAML geschrieben) im Ordner `deploy`

Bewährte Methoden

Sicherheit für Ressourcen CodePipeline

Es hat sich bewährt, Verschlüsselung und Authentifizierung für die Quell-Repositorys zu verwenden, die eine Verbindung zu Ihren Pipelines herstellen. CodePipeline Weitere Informationen finden Sie in der Dokumentation unter Bewährte Sicherheitsmethoden. CodePipeline

CodePipeline Ressourcen überwachen und protokollieren

Es hat sich bewährt, mithilfe der AWS-Protokollierungsfunktionen zu ermitteln, welche Aktionen Benutzer in Ihrem Konto ausführen und welche Ressourcen sie verwenden. Die Protokolldateien zeigen Folgendes:

- Uhrzeit und Datum der Aktionen
- Quell-IP-Adresse der Aktionen
- Welche Aktionen sind aufgrund unzureichender Berechtigungen fehlgeschlagen

Protokollierungsfunktionen sind in AWS CloudTrail und Amazon CloudWatch Events verfügbar. Sie können CloudTrail damit AWS-API-Aufrufe und zugehörige Ereignisse protokollieren, die von oder im Namen Ihres AWS-Kontos getätigt wurden. Weitere Informationen finden Sie CloudTrail in der CodePipeline Dokumentation unter Protokollieren von CodePipeline API-Aufrufen mit AWS.

Sie können CloudWatch Events verwenden, um Ihre AWS-Cloud-Ressourcen und -Anwendungen zu überwachen, die auf AWS ausgeführt werden. Sie können auch Benachrichtigungen in CloudWatch

Events erstellen. Weitere Informationen finden Sie in der CodePipeline Dokumentation unter CodePipeline Ereignisse überwachen.

Epen

Stellen Sie den Quellcode bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereiten Sie das Codearchiv für die Bereitstellung vor.	1. Laden Sie es `code.zip` aus dem GitHub aws-glue-jobs-unit-testing Repository herunter, oder erstellen Sie die .zip-Datei selbst mit einem Befehlszeilentool. Sie können die ZIP-Datei beispielsweise unter Linux oder Mac erstellen, indem Sie die folgenden Befehle im Terminal ausführen:
	`git clone https://github.com/aws-samples/aws-glue-jobs-unit-testing.git`
	`cd aws-glue-jobs-unit-testing`
	`git checkout master`
	`zip -r code.zip src/ tests/ deploy/`
	2. Melden Sie sich bei der AWS-Managementkonsole an und wählen Sie die AWS-Region Ihrer Wahl aus.
	3. Erstellen Sie einen S3-Bucket und laden Sie dann das .zip-Paket und die
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`code.zip` Datei (zuvor heruntergeladen) in den von Ihnen erstellten S3-Bucket hoch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CloudFormation Stapel.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 2. Wählen Sie Stack erstellen und anschließend Mit vorhandenen Ressourcen (Ressourcen importieren). 3. Wählen Sie auf der Seite „Stack erstellen“ im Abschnitt „Vorlage angeben“ die Option „Eine Vorlagendatei hochladen“ und dann die Vorlage „pipeline.yml“ (aus dem Repository heruntergeladen) aus. GitHub Wählen Sie anschließend Weiter. 4. Geben Sie als Stack-Name glue-unit-testing-pipeline ein, oder wählen Sie einen Stack-Namen Ihrer Wahl. 5. Verwenden Sie als ApplicationStackName den vorausgefüllten Namen glue-codepipeline-app. Dies ist der Name des CloudFormation Stacks, der von der Pipeline erstellt wird. 6. Verwenden Sie für BranchNameden vorab	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausgefüllten Masternamen. Dies ist der Name des Branches, der im CodeCommit Repository erstellt wurde, um den Code aus der .zip-Datei für den S3-Bucket einzuchecken. 7. Verwenden Sie für den BucketNamebereits ausgefüllten Bucket-Namen aws-glue-artifacts-us-east-1. Dies ist der Name des S3-Buckets, der die ZIP-Datei enthält und von der Pipeline zum Speichern von Codeartefakten verwendet wird. 8. Verwenden Sie für CodeZipFile den vorab ausgefüllten Wert code.zip. Dies ist der Schlüsselname des S3-Beispielcodeobjekts. Das Objekt sollte eine ZIP-Datei sein. 9. Verwenden Sie für den RepositoryNamebereits ausgefüllten Namen aws-glue-unit-testing. Dies ist der Name des CodeCommit Repositorys, das vom Stack erstellt wurde. 10. Verwenden Sie für TestReportGroupNameden vorausgefüllten Namen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	glue-unittest-report. Dies ist der Name der CodeBuild Testberichtsgruppe, die zum Speichern der Unit-Testberichte erstellt wurde. 11. Wählen Sie Weiter und klicken Sie dann auf der Seite Stack-Optionen konfigurieren erneut auf Weiter. 12. Wählen Sie auf der Seite Überprüfen unter Funktionen die Option Ich bestätige, dass CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden. 13. Wählen Sie Absenden aus. Nachdem die Erstellung des Stacks abgeschlossen ist, können Sie die erstellten Ressourcen auf der Registerkarte Ressourcen sehen. Die Erstellung des Stacks dauert ungefähr 5-7 Minuten. Der Stack erstellt automatisch ein CodeCommit Repository mit dem ursprünglichen Code, der aus der ZIP-Datei eingecheckt und in den S3-Bucket hochgeladen wurde. Darüber hinaus	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellt der Stack eine CodePipeline Ansicht, die das CodeCommit Repository als Quelle verwendet. In den obigen Schritten heißt das CodeCommit Repository aws-glue-unit-test und die Pipeline aws-glue-unit-test-pipeline.	
Bereinigen Sie die Ressourcen in Ihrer Umgebung.	Um zusätzliche Infrastrukturkosten zu vermeiden, stellen Sie sicher, dass Sie den Stack löschen, nachdem Sie mit den Beispielen in diesem Muster experimentiert haben. 1. Öffnen Sie die CloudFormation Konsole und wählen Sie dann den Stack aus, den Sie erstellt haben. 2. Wählen Sie Löschen aus. Dadurch werden alle Ressourcen gelöscht, die Ihr Stack erstellt hat, einschließlich CodeCommit Repositorys, AWS Identity and Access Management (IAM) -Rollen oder -Richtlinien und Projekte. CodeBuild	AWS DevOps, DevOps Ingenieur

Führen Sie die Komponententests aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die in der Pipeline befindlichen Komponent entests aus.	1. Um die bereitgestellte Pipeline zu testen, melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodePipeline Konsole. 2. Wählen Sie die Pipeline aus, die durch den CloudFormation Stack erstellt wurde, und wählen Sie dann Release change aus. Die Pipeline wird gestartet (unter Verwendun g des neuesten Codes im CodeCommit Repository). 3. Nachdem die Test_and_ Build-Phase abgeschlo ssen ist, wählen Sie die Registerkarte Details und überprüfen Sie dann die Protokolle. 4. Wählen Sie die Registerk arte Berichte und dann unter Berichtsverlauf den Testbericht aus, um die Ergebnisse der Komponent entests anzuzeigen. 5. Führen Sie nach Abschluss der Bereitstellungspha se den bereitgestellten AWS Glue-Job auf der AWS Glue-Konsole aus	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und überwachen Sie ihn. Weitere Informationen finden Sie unter Überwachung von AWS Glue in der AWS Glue Glue-Dokumentation.	

Fehlerbehebung

Problem	Lösung
Eine Pipeline mit Amazon S3, Amazon ECR oder CodeCommit Quelle wird nicht mehr automatisch gestartet	Wenn Sie Konfigurationseinstellungen für eine Aktion ändern, die Ereignisregeln in Amazon EventBridge oder CloudWatch Ereignisse zur Änderungserkennung verwendet, erkennt die AWS-Managementkonsole möglicher weise keine Änderung, wenn Quellkennungen ähnlich sind und identische Anfangszeichen haben. Da die neue Ereignisregel nicht von der Konsole erstellt wird, wird die Pipeline nicht mehr automatisch gestartet. Das Ändern eines CodeCommit Zweigname ns von `MyTestBranch-1` zu `MyTestBra nch-2` ist beispielsweise eine geringfügige Änderung. Da sich die Änderung am Ende des Zweignamens befindet, aktualisiert oder erstellt die Ereignisregel für die Quellaktion möglicher weise keine Regel für die neuen Quelleins tellungen. Dies gilt für die folgenden Quellaktionen, bei denen Ereignisse in CloudWatch Ereignissen zur Erkennung von Änderungen verwendet werden:

Problem	Lösung
	• Der S3-Bucket-Name und das S3-Objekt , die Schlüsselparameter oder Konsolen-IDs, wenn sich die Quellaktion in Amazon S3 befindet • Der Repository-Name und die Image-Tag-Parameter oder Konsolen-IDs, wenn sich die Quellaktion in Amazon ECR befindet • Der Repository-Name und der Branch-Name oder die Konsolen-Identifikatoren, wenn die Quell-Aktion aktiviert ist CodeCommit Gehen Sie wie folgt vor, um das Problem zu beheben: • Ändern Sie die Konfigurationseinstellungen in Amazon S3, Amazon ECR oder CodeCommit, sodass Änderungen am Startteil des Parameterwerts vorgenommen werden. Ändern Sie beispielsweise Ihren Filialnamen von `release-branch` zu `2nd-release-branch` . Vermeiden Sie eine Änderung am Ende des Namens, z. `release-branch-2` B. • Ändern Sie die Konfigurationseinstellungen in Amazon S3, Amazon ECR oder CodeCommit für jede Pipeline. Ändern Sie beispielsweise Ihren Filialnamen von `myRepo/myBranch` zu `myDeployRepo/myDeployBranch` . Vermeiden Sie eine Änderung am Ende des Namens, z. `myRepo/myBranch2` B. • Anstatt die AWS-Managementkonsole zu verwenden, verwenden Sie die AWS-Befehlszeilenschnittstelle (AWS CLI) oder AWS, CloudFormation um Ihre Regeln für Ereigniss

Problem	Lösung
	e zur Änderungserkennung zu erstellen und zu aktualisieren. Anweisungen zum Erstellen von Ereignisregeln für eine Amazon S3 S3-Quellaktion finden Sie unter Amazon S3 S3-Quellaktionen und CloudWatch Ereignisse. Anweisungen zum Erstellen von Ereignisr egeln für eine Amazon ECR-Aktion finden Sie unter Amazon ECR-Quellaktionen und CloudWatch Ereignisse. Anweisung en zum Erstellen von Ereignisregeln für eine CodeCommit Aktion finden Sie unter CodeCommit Quellaktionen und CloudWatc h Ereignisse. Nachdem Sie Ihre Aktionsko nfiguration in der Konsole bearbeitet haben, akzeptieren Sie die aktualisierten Ressource n zur Änderungserkennung, die von der Konsole erstellt wurden.

Zugehörige Ressourcen

- AWS Glue
- Lokales Entwickeln und Testen von AWS Glue Glue-Jobs
- AWS CloudFormation für AWS Glue

Zusätzliche Informationen

Darüber hinaus können Sie die CloudFormation AWS-Vorlagen mithilfe der AWS-CLI bereitstellen. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Schnelles Bereitstellen von Vorlagen mit Transformationen.

Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Container und Mikroservices; Modernisierung	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon S3		

Übersicht

Dieses Muster hilft Ihnen, Helm v3-Diagramme effizient zu verwalten, indem Sie das Helm v3-Repository in Amazon Simple Storage Service (Amazon S3) in der Amazon Web Services (AWS) Cloud integrieren. Um dieses Muster verwenden zu können, müssen Sie mit Kubernetes und Helm, einem Kubernetes-Paketmanager, vertraut sein. Die Verwendung von Helm-Repositorys zum Speichern von Diagrammen und zur Steuerung von Diagrammversionen kann die mittlere Wiederherstellungszeit (MTTR) bei Ausfällen verbessern.

Dieses Muster verwendet AWS CodeCommit für die Erstellung von Helm-Repositorys und verwendet einen S3-Bucket als Helm-Diagramm-Repository, sodass die Diagramme zentral verwaltet und von Entwicklern im gesamten Unternehmen abgerufen werden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Python-Version 2.7.12 oder höher
- pip
- Eine virtuelle private Cloud (VPC) mit Subnetzen und einer Amazon Elastic Compute Cloud (Amazon EC2) -Instanz
- Git ist auf der EC2-Instance installiert
- Zugriff auf AWS Identity and Access Management (IAM) zur Erstellung des S3-Buckets
- IAM-Zugriff (programmatischer oder Rollenzugriff) auf Amazon S3 vom Client-Computer
- CodeCommit AWS-Repository
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)

Produktversionen

- Helm v3
- Python-Version 2.7.12 oder höher

Architektur

Zieltechnologie-Stack

- Amazon S3
- AWS CodeCommit
- Helm
- Kubectl
- Python und Pip
- Git
- Helm-S3-Plugin

Zielarchitektur

Automatisierung und Skalierung

- Sie können Helm in Ihr bestehendes Automatisierungstool für Continuous Integration/Continuous Delivery (CI/CD) integrieren, um die Paketierung und Versionskontrolle von Helm-Charts zu automatisieren (außerhalb des Geltungsbereichs dieses Musters).
- GitVersion oder Jenkins-Build-Nummern können verwendet werden, um die Versionskontrolle der Charts zu automatisieren.

Tools

- Helm — Helm ist ein Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.

- helm-S3-Plugin — Das helm-S3-Plugin unterstützt die Interaktion mit Amazon S3. Es kann entweder mit Helm v2 oder Helm v3 verwendet werden.

Epen

Installieren und validieren Sie Helm v3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Helm v3-Client.	Führen Sie den folgenden Befehl aus, um den Helm-Client herunterzuladen und auf Ihrem lokalen System zu installieren: `sudo curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash`	Cloud-Administrator, DevOps Ingenieur
Validieren Sie die Helm-Installation.	Führen Sie den folgenden Befehl aus, um den Helm-Client zu validieren: `helm version --short`	Cloud-Administrator, DevOps Ingenieur

Initialisieren Sie einen S3-Bucket als Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für Helm-Charts.	Erstellen Sie einen eindeutigen S3-Bucket. Erstellen Sie im Bucket einen Ordner mit dem Namen `stable/myapp` . Das Beispiel in diesem Muster verwendet `s3://my-helm-charts/stable/myapp` als Zieldiagramm-Repository.	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das Helm-S3-Plugin für Amazon S3.	Führen Sie den folgenden Befehl aus, um das Helm-S3-Plugin auf Ihrem Client-Computer zu installieren: `helm plugin install https://github.com/hypnoglow/helm-s3.git`	Cloud-Administrator, Ingenieur DevOps
Initialisieren Sie das Amazon S3 Helm-Repository.	Verwenden Sie den folgenden Befehl, um den Zielordner als Helm-Repository zu initialisieren: `helm s3 init s3://my-helm-charts/stable/myapp` Der Befehl erstellt eine `index.yaml` Datei im Ziel, um alle Diagramminformationen zu verfolgen, die an diesem Speicherort gespeichert sind.	Cloud-Administrator, DevOps Ingenieur
Überprüfen Sie das neu erstellte Helm-Repository.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die `index.yaml` Datei erstellt wurde: `aws s3 ls s3://my-helm-charts/stable/myapp/`	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Amazon S3 S3-Repository zu Helm auf dem Client-Computer hinzu.	Verwenden Sie den folgenden Befehl, um den Ziel-Repo sitory-Alias zum Helm-Client-Computer hinzuzufügen: `helm repo add stable-myapp s3://my-helm-charts/stable/myapp/`	Cloud-Administrator, DevOps Ingenieur

Verpacken und veröffentlichen Sie Diagramme im Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie Ihre Helm-Charts.	Wenn in Ihrem CodeCommi t Repository keine lokalen Helm-Charts vorhanden sind, klonen Sie sie aus Ihrem GitHub Repo, indem Sie den folgenden Befehl ausführen : `git clone <url_of_your_helm_source_code>.git`	Cloud-Administrator, Ingenieur DevOps
Package Sie die lokale Helm-Karte.	Verwenden Sie den folgenden Befehl, um das Diagramm, das Sie erstellt oder geklont haben, zu verpacken: `helm package ./my-app` Als Beispiel verwendet dieses Muster das `my-app` Diagramm. Der Befehl packt den gesamten Inhalt des `my-app` Diagrammordners in eine Archivdatei, die anhand der	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Versionsnummer benannt wird, die in der `Chart.yaml` Datei angegeben ist.	
Speichern Sie das lokale Paket im Amazon S3 Helm-Repository.	Führen Sie den folgenden Befehl aus, um das lokale Paket in das Helm-Repository in Amazon S3 hochzuladen: `helm s3 push ./my-app-0.1.0.tgz stable-myapp` In dem Befehl `my-app` steht der Name Ihres Diagrammordners, `0.1.0` die unter `Chart.yaml` erwähnte Diagrammversion und der Alias für das Ziel-Repository. `stable-myapp`	Cloud-Administrator, DevOps Ingenieur
Suchen Sie nach dem Helm-Diagramm.	Um zu überprüfen, ob das Diagramm sowohl lokal als auch im Amazon S3 Helm-Repository angezeigt wird, führen Sie den folgenden Befehl aus: `helm search repo stable-myapp`	Cloud-Administrator, DevOps Ingenieur

Aktualisieren Sie Ihr Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern und verpacken Sie das Diagramm.	Legen Sie den `replicaCount` Wert auf fest1, und verpacken Sie dann das	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Diagramm, wobei Sie diesmal die Version in `Chart.yaml` ändern`0.1.1`. `values.yaml` Die Versionskontrolle wird idealerweise durch Automatisierung mithilfe von Tools wie GitVersion oder Jenkins-Build-Nummern in einer CI/CD-Pipeline erreicht. Die Automatisierung der Versionsnummer ist für dieses Muster nicht vorgesehen. Führen Sie den folgenden Befehl aus, um das Diagramm zu verpacken: `helm package ./my-app/`	
Pushen Sie die neue Version in das Helm-Repository in Amazon S3.	Führen Sie den folgenden Befehl aus, um das neue Paket, Version 0.1.1, in das Helm-Repository my-helm-charts in Amazon S3 zu übertragen: `helm s3 push ./my-app-0.1.1.tgz stable-myapp`	Cloud-Administrator, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie das aktualisierte Helm-Diagramm.	Um zu überprüfen, ob das aktualisierte Diagramm sowohl lokal als auch im Amazon S3 Helm-Repository angezeigt wird, führen Sie die folgenden Befehle aus.
	`helm repo update`
	`helm search repo stable-myapp`
		Cloud-Administrator, DevOps Ingenieur

Suchen und installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach allen Versionen des my-app-Diagramms.	Um alle verfügbaren Versionen eines Diagramms anzuzeigen, führen Sie den folgenden Befehl mit der `--versions` Markierung aus: `helm search repo my-app --versions` Ohne die Markierung zeigt Helm standardmäßig die zuletzt hochgeladene Version eines Diagramms an.	DevOps Ingenieur
Installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository.	Eine automatische Installation ist für dieses Muster nicht vorgesehen, aber Sie können die Installation manuell durchführen. Die Suchergebnisse der vorherigen Aufgabe	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zeigen die verschiedenen Versionen des `my-app` Diagramms. Verwenden Sie den folgenden Befehl, um die neue Version (0.1.1) aus dem Amazon S3 Helm-Repo sitory zu installieren: `helm upgrade --install my-app-release stable-myapp/my-app --version 0.1.1 --namespace dev`	

Gehen Sie mithilfe von Helm zu einer früheren Version zurück

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Details für eine bestimmte Revision.	Ein automatisiertes Rollback ist für dieses Muster nicht vorgesehen, aber Sie können manuell zu einer früheren Version zurückkehren. Bevor Sie zu einer funktionierenden Version wechseln oder ein Rollback durchführen und für eine zusätzliche Überprüfungsebene vor der Installation einer Revision, sollten Sie mit dem folgenden Befehl überprüfen, welche Werte an die einzelnen Versionen übergeben wurden: `helm get values --revision=2 my-app-release`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie zurück zu einer früheren Version.	Ein automatisiertes Rollback ist für dieses Muster nicht vorgesehen. Verwenden Sie den folgenden Befehl, um manuell zu einer früheren Version zurückzukehren: `helm rollback my-app-release 1` In diesem Beispiel wird auf Version 1 zurückgesetzt.	DevOps Ingenieur

Zugehörige Ressourcen

- HELM-Dokumentation
- helm-S3-Plugin (MIT-Lizenz)
- Amazon S3

Richten Sie eine CI/CD-Pipeline mithilfe von AWS CodePipeline und AWS CDK ein

Code-Repository: AWS CodePipeline mit CI/CD	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps
Arbeitsaufwand: Open Source	AWS-Dienste: AWS CodePipeline	

Startseite

Die Automatisierung Ihres Software-Build- und Release-Prozesses mit Continuous Integration and Continuous Delivery (CI/CD) unterstützt wiederholbare Builds und die schnelle Bereitstellung neuer Funktionen für Ihre Benutzer. Sie können jede Codeänderung schnell und einfach testen und Fehler catch und beheben, bevor Sie Ihre Software veröffentlichen. Indem Sie jede Änderung Ihrem Staging- und Release-Prozess unterziehen, können Sie die Qualität Ihres Anwendungs- oder Infrastrukturcodes überprüfen. CI/CD verkörpert eine Kultur, eine Reihe von Betriebsprinzipien und eine Sammlung von Praktiken, die Anwendungsentwicklungsteams dabei unterstützen, Codeänderungen häufiger und zuverlässiger vorzunehmen. Die Implementierung wird auch als CI/CD-Pipeline bezeichnet.

Dieses Muster definiert eine wiederverwendbare Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) auf Amazon Web Services (AWS). Die CodePipeline AWS-Pipeline wurde mit dem AWS Cloud Development Kit (AWS CDK) v2 geschrieben.

Mithilfe CodePipeline können Sie die verschiedenen Phasen Ihres Softwareveröffentlichungsprozesses über die AWS-Managementkonsole, die AWS-Befehlszeilenschnittstelle (AWS CLI) CloudFormation, AWS oder die AWS-SDKs modellieren. Dieses Muster demonstriert die Implementierung von CodePipeline und seine Komponenten mithilfe von AWS CDK. Zusätzlich zu den Construct-Bibliotheken enthält AWS CDK ein Toolkit (den CLI-Befehl`cdk`), das wichtigste Tool für die Interaktion mit Ihrer AWS-CDK-App. Das Toolkit bietet unter anderem die Möglichkeit, einen oder mehrere Stacks in CloudFormation Vorlagen zu konvertieren und sie auf einem AWS-Konto bereitzustellen.

Die Pipeline umfasst Tests zur Überprüfung der Sicherheit Ihrer Drittanbieter-Bibliotheken und trägt dazu bei, eine beschleunigte, automatisierte Veröffentlichung in den angegebenen Umgebungen

sicherzustellen. Sie können die Gesamtsicherheit Ihrer Anwendungen erhöhen, indem Sie sie einem Validierungsprozess unterziehen.

Ziel dieses Musters ist es, die Verwendung von CI/CD-Pipelines zur Bereitstellung Ihres Codes zu beschleunigen und gleichzeitig sicherzustellen, dass die von Ihnen bereitgestellten Ressourcen den Best Practices entsprechen DevOps . Nachdem Sie den Beispielcode implementiert haben, verfügen Sie über ein AWS CodePipeline mit Linting-, Test-, Sicherheitscheck-, Bereitstellungs- und Nachbereitstellungsprozessen. Dieses Muster beinhaltet auch Schritte für Makefile. Mithilfe eines Makefiles können Entwickler CI/CD-Schritte lokal reproduzieren und so den Entwicklungsprozess beschleunigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein grundlegendes Verständnis im Folgenden:
  - AWS-CDK
  - AWS CloudFormation
  - AWS CodePipeline
  - TypeScript

Einschränkungen

Dieses Muster verwendet AWS CDK TypeScript nur für. Andere Sprachen, die von AWS CDK unterstützt werden, werden nicht abgedeckt.

Produktversionen

Verwenden Sie die neuesten Versionen der folgenden Tools:

- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- cfn_nag
- git-remote-codecommit
- Node.js

Architektur

Zieltechnologie-Stack

- AWS-CDK
- AWS CloudFormation
- AWS CodeCommit
- AWS CodePipeline

Zielarchitektur

Die Pipeline wird durch eine Änderung im CodeCommit AWS-Repository (`SampleRepository`) ausgelöst. Zu Beginn CodePipeline erstellt es Artefakte, aktualisiert sich selbst und startet den Bereitstellungsprozess. Die daraus resultierende Pipeline stellt eine Lösung für drei unabhängige Umgebungen bereit:

- Dev — Dreistufiger Codecheck in der aktiven Entwicklungsumgebung
- Test — Integrations- und Regressionstestumgebung
- Prod — Produktionsumgebung

Die Entwicklungsphase umfasst drei Schritte: Linting, Sicherheit und Komponententests. Diese Schritte laufen parallel ab, um den Prozess zu beschleunigen. Um sicherzustellen, dass die Pipeline nur funktionierende Artefakte bereitstellt, wird sie beendet, sobald ein Schritt im Prozess fehlschlägt. Nach einer Bereitstellung in der Entwicklungsphase führt die Pipeline Validierungstests durch, um die Ergebnisse zu überprüfen. Im Erfolgsfall stellt die Pipeline die Artefakte dann in der Testumgebung bereit, die die Validierung nach der Bereitstellung beinhaltet. Der letzte Schritt besteht darin, die Artefakte in der Prod-Umgebung bereitzustellen.

Das folgende Diagramm zeigt den Arbeitsablauf vom CodeCommit Repository bis zu den Build- und Aktualisierungsprozessen CodePipeline, die drei Schritte der Entwicklungsumgebung und die anschließende Bereitstellung und Validierung in jeder der drei Umgebungen.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten. In diesem Muster können CloudFormation Vorlagen verwendet werden, um ein CodeCommit Repository und eine CodePipeline CI/CD-Pipeline zu erstellen.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline ist ein CI/CD-Service, der Ihnen hilft, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere Tools

- cfn_nag ist ein Open-Source-Tool, das in CloudFormation Vorlagen nach Mustern sucht, um potenzielle Sicherheitsprobleme zu identifizieren.
- git-remote-codecommit ist ein Hilfsprogramm zum Übertragen und Abrufen von Code aus Repositorys durch Erweiterung von CodeCommit Git.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.

Code

Der Code für dieses Muster ist im GitHub AWS CodePipeline with CI/CD Practices Repository verfügbar.

Bewährte Methoden

Überprüfen Sie Ressourcen wie die Richtlinien von AWS Identity and Access Management (IAM), um sicherzustellen, dass sie mit den bewährten Methoden Ihres Unternehmens übereinstimmen.

Epen

Tools installieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Tools auf macOS oder Linux.	Wenn Sie macOS oder Linux verwenden, können Sie die Tools installieren, indem Sie den folgenden Befehl in Ihrem bevorzugten Terminal ausführen oder Homebrew für Linux verwenden.
	`brew install`
	`brew install git-remote-codecommit`
	`brew install ruby brew-gem`
	`brew-gem install cfn-nag`
		DevOps Ingenieur

Installieren Sie Tools mithilfe von AWS Cloud9.	Wenn Sie AWS Cloud9 verwenden, installieren Sie die Tools, indem Sie den folgenden Befehl ausführen.
	`gem install cfn-nag`
	Hinweis: In AWS Cloud9 sollten Node.js und npm installiert sein. Führen Sie den folgenden Befehl aus, um die Installation oder Version zu überprüfen.
	`node -v`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`npm -v`	
Richten Sie die AWS-CLI ein.	Verwenden Sie die Anweisungen für Ihr Betriebssystem, um AWS CLI einzurichten: • Windows: Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Windows mit dem AWS CLI Credential Helper • Linux, macOS, Unix: Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Linux, macOS oder Unix mit dem AWS CLI Credential Helper	DevOps Ingenieur

Richten Sie die erste Bereitstellung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code herunter oder klonen Sie ihn.	Gehen Sie wie folgt vor, um den Code abzurufen, der von diesem Muster verwendet wird: • Laden Sie den neuesten Quellcode aus den Releases im GitHub Repo herunter und entpacken Sie die heruntergeladene Datei in einen Ordner.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Klonen Sie das Projekt, indem Sie den folgenden Befehl ausführen.
	
	`git clone --depth 1 https://github.com/aws-samples/aws-codepipeline-cicd.git`
	
	Entfernen Sie das `.git` Verzeichnis aus dem geklonten Repository.
	
	`cd ./aws-codepipeline-cicd`
	`rm -rf ./.git`
	
	Später werden Sie ein neu erstelltes CodeCommit AWS-Repository als Remote-Ursprung verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Connect zum AWS-Konto her.	Sie können eine Verbindung herstellen, indem Sie ein temporäres Sicherheitstoken oder eine Landingzone-Authentifizierung verwenden. Führen Sie die folgenden Befehle aus, um zu bestätigen, dass Sie das richtige Konto und die richtige AWS-Region verwenden.
	`AWS_REGION="eu-west-1"`
	`ACCOUNT_NUMBER=$(aws sts get-caller-identity --query Account --output text)`
	`echo "${ACCOUNT_NUMBER}"`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bootstrapping für die Umwelt.	Führen Sie die folgenden Befehle aus, um eine AWS-CDK-Umgebung zu booten.
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Nachdem Sie die Umgebung erfolgreich gebootet haben, sollte die folgende Ausgabe angezeigt werden.
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
	Weitere Informationen zu AWS CDK-Bootstrapping finden Sie in der AWS CDK-Dokumentation.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Synthetisieren Sie eine Vorlage.	Verwenden Sie den Befehl, um eine AWS CDK-App zu synthetisieren. `cdk synth`
	`npm run cdk synth`
	Die Ausgabe sollte folgender maßen aussehen.
	`Successfully synthesized to <path-to-directory>/aws-codepipeline-cicd/cdk.out`
	`Supply a stack id (CodePipeline, Dev-MainStack) to display its template.`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den CodePipeline Stack bereit.	Nachdem Sie die CloudFormation Vorlage nun gebootet und synthetisiert haben, können Sie sie bereitstellen. Bei der Bereitstellung werden die CodePipeline Pipeline und ein CodeCommit Repository erstellt, das als Quelle und Auslöser der Pipeline dient.
	`npm run cdk -- deploy CodePipeline --require-approval never`
	Nachdem Sie den Befehl ausgeführt haben, sollten Sie sehen, dass der CodePipeline Stack erfolgreich bereitgestellt und die Informationen ausgegeben wurden. Das `CodePipeline.RepositoryName` gibt Ihnen den Namen des CodeCommit Repositorys im AWS-Konto.
	`CodePipeline: deploying...`
	`CodePipeline: creating CloudFormation changeset...`
	`# CodePipeline Outputs:`
	`CodePipeline.RepositoryName = SampleRepository`
	`Stack ARN:`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`arn:aws:cloudformation:REGION:ACCOUNT-ID:stack/CodePipeline/STACK-ID`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das CodeCommit Remote-Repository und den Branch ein.	Nach einer erfolgreichen Bereitstellung CodePipeline wird der erste Lauf der Pipeline initiiert, den Sie in der CodePipeline AWS-Konsole finden. Da AWS CDK und CodeCommit kein Standard-Branch initiieren, schlägt dieser erste Pipeline-Lauf fehl und gibt die folgende Fehlermeldung zurück.
	`The action failed because no branch named main was found in the selected AWS CodeCommit repository SampleRepository. Make sure you are using the correct branch name, and then try again. Error: null`
	Um diesen Fehler zu beheben, richten Sie einen Remote-Ursprung als `SampleRepository` ein und erstellen Sie den erforderlichen `main` Branch.
	`RepoName=$(aws cloudformation describe-stacks --stack-name CodePipeline --query "Stacks[0].Outputs[?OutputKey=='RepositoryNam`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`e'].OutputValue" --`
	`output text)`
	`echo "${RepoName}"`
	`#`
	`git init`
	`git branch -m master`
	` main`
	`git remote add origin`
	` codecommit://${Rep`
	`oName}`
	`git add .`
	`git commit -m "Initial`
	` commit"`
	`git push -u origin main`	

Testen Sie die bereitgestellte CodePipeline Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie eine Änderung, um die Pipeline zu aktivieren.	Nach einer erfolgreichen ersten Bereitstellung sollten Sie über eine vollständige CI/CD-Pipeline mit einem `main` Zweig `SampleRepository` als Quellzweig verfügen. Sobald Sie die Änderunge n an der `main` Verzweigung vorgenommen haben, initiiert die Pipeline die folgende Abfolge von Aktionen und führt sie aus: 1. Holen Sie sich Ihren Code aus dem CodeCommit Repository. 2. Erstellen Sie Ihren Code.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Aktualisieren Sie die Pipeline selbst (`UpdatePipeline`). 4. Führen Sie drei parallel Jobs für Linting-, Sicherheits- und Unit-Test-Checks aus. 5. Im Erfolgsfall verteilt die Pipeline den `Main` Stack von der Entwicklungsumgebung in `./lib/main-stack.ts` die Entwicklungsumgebung. 6. Führen Sie nach der Bereitstellung eine Überprüfung der bereitgestellten Ressourcen durch. Sie können alle CodePipeline Schritte und Ergebnisse in der CodePipeline Konsole verfolgen. 7. Im Erfolgsfall wiederholt die Pipeline die Bereitstellung und Validierung für die Test- und Prod-Umgebungen.	

Testen Sie lokal mit einem Makefile

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Entwicklungsprozess mithilfe eines Makefiles aus.	Sie können die gesamte Pipeline lokal ausführen, indem Sie den `make` Befehl verwenden, oder Sie können einen einzelnen Schritt ausführen (z. B.`make linting`). Führen Sie die folgenden Aktionen aus`make`, um die Verwendung zu testen: • Implementieren Sie die lokale Pipeline: `make` • Nur Unit-Tests ausführen: `make unittest` • Auf das Girokonto bereitstellen: `make deploy` • Säubere die Umwelt: `make clean`	App-Entwickler, DevOps Ingenieur

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die AWS-CDK-App-Ressourcen.	Führen Sie den folgenden Befehl aus, um Ihre AWS CDK-App zu bereinigen. `cdk destroy --all`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beachten Sie, dass die Amazon Simple Storage Service (Amazon S3) - Buckets, die beim Bootstrap ping erstellt werden, nicht automatisch gelöscht werden. Sie benötigen eine Aufbewahr ungsrichtlinie, die das Löschen ermöglicht, oder Sie müssen sie manuell in Ihrem AWS-Konto löschen.	

Fehlerbehebung

Problem	Lösung
Die Vorlage funktioniert nicht wie erwartet.	Wenn etwas schief geht und die Vorlage nicht funktioniert, stellen Sie sicher, dass Sie über Folgendes verfügen: • Die richtigen Versionen der Tools. • Zugriff auf das AWS-Zielkonto (Netzwerk konnektivität). • Genügend Berechtigungen für das AWS-Zielkonto.

Zugehörige Ressourcen

- Beginnen Sie mit den häufigsten Aufgaben im IAM Identity Center
- CodePipeline AWS-Dokumentation
- AWS CDK

Einrichten der end-to-end Verschlüsselung für Anwendungen in Amazon EKS mit cert-manager und Let's Encrypt

Erstellt vonendra Siddappa (AWS) und Bolanth Jeyaraj (AWS)

Code-Repository: E-nd-to-end Verschlüsselung auf Amazon EKS	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Container und Microservices; Sicherheit, Identität, Compliance
Workload: Alle anderen Workloads	AWS-Services: Amazon EKS; Amazon Route 53	

Übersicht

Die Implementierung der end-to-end Verschlüsselung kann komplex sein und Sie müssen Zertifikate für jede Komponente in Ihrer Microservices-Architektur verwalten. Obwohl Sie die Transport Layer Security (TLS)-Verbindung am Edge des Amazon Web Services (AWS)-Netzwerks mit einem Network Load Balancer oder Amazon API Gateway end-to-end beenden können, benötigen einige Organisationen eine Verschlüsselung.

Dieses Muster verwendet NGINX Ingress Controller für eingehenden Datenverkehr. Dies liegt daran, dass beim Erstellen eines Kubernetes-Eingangs die Eingangsressource einen Network Load Balancer verwendet. Der Network Load Balancer erlaubt keine Uploads von Clientzertifikaten. Daher können Sie gegenseitiges TLS mit Kubernetes-Eingang nicht erreichen.

Dieses Muster richtet sich an Organisationen, die eine gegenseitige Authentifizierung zwischen allen Microservices in ihren Anwendungen benötigen. Gegenseitiges TLS reduziert den Aufwand für die Verwaltung von Benutzernamen oder Passwörtern und kann auch das schlüsselfertige Sicherheits-Framework verwenden. Der Ansatz dieses Musters ist kompatibel, wenn Ihre Organisation über eine große Anzahl verbundener Geräte verfügt oder strenge Sicherheitsrichtlinien einhalten muss.

Dieses Muster trägt dazu bei, die Sicherheitslage Ihrer Organisation zu erhöhen, indem es end-to-end Verschlüsselung für Anwendungen implementiert, die auf Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden. Dieses Muster bietet eine Beispielanwendung und Code im

GitHub Repository E-nd-to-end Verschlüsselung in Amazon EKS, um zu zeigen, wie ein Microservice mit end-to-end Verschlüsselung in Amazon EKS ausgeführt wird. Der Ansatz des Musters verwendet cert-manager, ein Add-on für Kubernetes, mit Let's Encrypt als Zertifizierungsstelle (CA). Let's Encrypt ist eine kostengünstige Lösung zur Verwaltung von Zertifikaten und stellt kostenlose Zertifikate bereit, die 90 Tage gültig sind. Cert-Manager automatisiert die On-Demand-Bereitstellung und Rotation von Zertifikaten, wenn ein neuer Microservice auf Amazon EKS bereitgestellt wird.

Zielgruppe

Dieses Muster wird für Benutzer empfohlen, die Erfahrung mit Kubernetes, TLS, Amazon Route 53 und Domain Name System (DNS) haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon-EKS-Cluster.
- AWS Command Line Interface (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert unter macOS , Linux oder Windows.
- Das `kubectl` Befehlszeilen-Dienstprogramm, das für den Zugriff auf den Amazon-EKS-Cluster installiert und konfiguriert ist. Weitere Informationen dazu finden Sie unter Installieren von kubectl in der Amazon-EKS-Dokumentation.
- Ein vorhandener DNS-Name zum Testen der Anwendung. Weitere Informationen dazu finden Sie unter Registrieren von Domainnamen mit Amazon Route 53 in der Amazon Route 53-Dokumentation.
- Die neueste Helm-Version, die auf Ihrem lokalen Computer installiert ist. Weitere Informationen dazu finden Sie unter Verwenden von Helm mit Amazon EKS in der Amazon-EKS-Dokumentation und im GitHub Helm-Repository.
- Das GitHub E-nd-to-end Verschlüsselung auf Amazon EKS-Repository, geklont auf Ihrem lokalen Computer.
- Ersetzen Sie die folgenden Werte in den `trustpolicy.json` Dateien `policy.json` und aus dem geklonten GitHub E-nd-to-end Verschlüsselung in Amazon-EKS-Repository:
  - `<account number>` – Ersetzen Sie durch die AWS-Konto-ID für das Konto, in dem Sie die Lösung bereitstellen möchten.
  - `<zone id>` – Ersetzen Sie durch die Route 53-Zonen-ID des Domänennamens.

- `<node_group_role>` – Ersetzen Sie durch den Namen der AWS Identity and Access Management (IAM)-Rolle, die den Amazon EKS-Knoten zugeordnet ist.
- `<namespace>` – Ersetzen Sie durch den Kubernetes-Namespace, in dem Sie den NGINX Ingress Controller und die Beispielanwendung bereitstellen.
- `<application-domain-name>` – Ersetzen Sie durch den DNS-Domänennamen aus Route 53.

Einschränkungen

- Dieses Muster beschreibt nicht, wie Zertifikate rotiert werden, und zeigt nur, wie Zertifikate mit Microservices in Amazon EKS verwendet werden.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Client sendet eine Anforderung für den Zugriff auf die Anwendung an den DNS-Namen.
2. Der Route 53-Datensatz ist ein CNAME für den Network Load Balancer .
3. Der Network Load Balancer leitet die Anforderung an den NGINX Ingress Controller weiter, der mit einem TLS-Listener konfiguriert ist. Die Kommunikation zwischen dem NGINX Ingress Controller und dem Network Load Balancer folgt dem HTTPS-Protokoll.
4. Der NGINX Ingress Controller führt pfadbasiertes Routing basierend auf der Anforderung des Clients an den Anwendungsservice durch.
5. Der Anwendungsservice leitet die Anfrage an den Anwendungs-Pod weiter. Die Anwendung ist so konzipiert, dass sie dasselbe Zertifikat verwendet, indem sie -Secrets aufruft.
6. Pods führen die Beispielanwendung mit den Zertifikaten cert-manager aus. Die Kommunikation zwischen dem NGINX Ingress Controller und den Pods verwendet HTTPS.

Hinweis: Cert-manager wird in einem eigenen Namespace ausgeführt. Es verwendet eine Kubernetes-Clusterrolle, um Zertifikate als Secrets in bestimmten Namespaces bereitzustellen. Sie können diese Namespaces an Anwendungs-Pods und NGINX Ingress Controller anfügen.

Tools

AWS-Services

- Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren, betreiben und warten zu müssen.
- Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, Container und IP-Adressen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Andere Tools

- cert-manager ist ein Add-on für Kubernetes, das Zertifikate anfordert, sie an Kubernetes-Container verteilt und die Zertifikatserneuerung automatisiert.
- NGINX Ingress Controller ist eine Datenverkehrsverwaltungslösung für cloudnative Apps in Kubernetes und containerisierten Umgebungen.

Polen

Erstellen und Konfigurieren einer öffentlich gehosteten Zone mit Route 53

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine öffentlich gehostete Zone in Route 53.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Route 53-Konsole, wählen Sie Gehostete Zonen und dann Gehostete Zone erstellen aus. Erstellen Sie eine öffentlich gehostete Zone und notieren Sie sich die Zonen-ID. Weitere Informationen dazu finden Sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Erstellen einer öffentlich gehosteten Zone in der Amazon Route 53-Dokumentation. Hinweis: ACME DNS01 verwendet den DNS-Anbieter, um eine Aufforderung für cert-manager zur Ausstellung des Zertifikats zu senden. Bei dieser Aufforderung werden Sie aufgefordert, nachzuweisen, dass Sie das DNS für Ihren Domänennamen kontrollieren, indem Sie einen bestimmten Wert in einen TXT-Datensatz unter diesem Domänennamen einfügen. Nachdem Let's Encrypt Ihrem ACME-Client ein Token gegeben hat, erstellt Ihr Client einen TXT-Datensatz, der von diesem Token und Ihrem Kontoschlüssel abgeleitet wird, und legt diesen Datensatz unter `ab_acme-challenge.<YOURDOMAIN>` . Dann fragt Let's Encrypt das DNS für diesen Datensatz ab. Wenn eine Übereinstimmung gefunden wird, können Sie mit der Ausstellung eines Zertifikats fortfahren.	

Konfigurieren einer IAM-Rolle, um cert-manager den Zugriff auf die öffentlich gehostete Zone zu ermöglichen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie für cert-manager.	Eine IAM-Richtlinie ist erforderlich, um cert-manager die Berechtigung zu erteilen, zu überprüfen, ob Sie Eigentümer der Route 53-Domain sind. Die `policy.json` Beispiel-IAM-Richtlinie wird im `1-IAMRole` Verzeichnis im geklonten GitHub E-nd-to-end Verschlüsselung in Amazon-EKS-Repository bereitgestellt. Geben Sie den folgenden Befehl in AWS CLI ein, um die IAM-Richtlinie zu erstellen. `aws iam create-policy \ --policy-name PolicyForCertManager \ --policy-document file://policy.json`	AWS DevOps
Erstellen Sie die IAM-Rolle für cert-manager.	Nachdem Sie die IAM-Richtlinie erstellt haben, müssen Sie eine IAM-Rolle erstellen. Die IAM-`trustpolicy.json` Beispielrolle wird im `1-IAMRole` Verzeichnis bereitgestellt.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Geben Sie den folgenden Befehl in AWS CLI ein, um die IAM-Rolle zu erstellen. `aws iam create-role \ --role-name RoleForCertManager \ --assume-role-policy-document file://trustpolicy.json`	
Fügen Sie der Rolle die -Richtlinie an.	Geben Sie den folgenden Befehl in AWS CLI ein, um die IAM-Richtlinie an die IAM-Rolle anzuhängen. Ersetzen Sie durch `AWS_ACCOUNT_ID` die ID Ihres AWS-Kontos. `aws iam attach-role-policy \ --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/PolicyForCertManager \ --role-name RoleForCertManager`	AWS DevOps

Einrichten des NGINX Ingress Controllers in Amazon EKS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den NGINX Ingress Controller bereit.	Installieren Sie die neueste Version von `nginx-ingress` mit Helm. Sie können die `nginx-ingress` Konfiguration vor der Bereitste	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	llung an Ihre Anforderu ngen anpassen. Dieses Muster verwendet einen mit Anmerkungen versehene n, internen Network Load Balancer, der im `5-Nginx-Ingress-Controller` Verzeichnis verfügbar ist. Installieren Sie den NGINX Ingress Controller, indem Sie den folgenden Helm-Befehl aus dem `5-Nginx-Ingress-Controller` Verzeichnis ausführen. `helm install test-nginx nginx-stable/nginx-ingress -f 5-Nginx-Ingress-Controller/values_internal_nlb.yaml`	
Stellen Sie sicher, dass der NGINX Ingress Controller installiert ist.	Geben Sie den `helm list`-Befehl ein. Die Ausgabe sollte zeigen, dass der NGINX Ingress Controller installiert ist.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Route 53-A-Datensatz.	Der A-Datensatz verweist auf den Network Load Balancer, der vom NGINX Ingress Controller erstellt wurde. 1. Rufen Sie den DNS-Namen des Network Load Balancers ab. Anweisungen finden Sie unter Abrufen des DNS-Namens für einen ELB Load Balancer. 2. Wählen Sie in der Amazon Route 53-Konsole Hosted Zones aus. 3. Wählen Sie die öffentlich gehostete Zone aus, in der Sie den Datensatz erstellen möchten, und wählen Sie dann Datensatz erstellen aus. 4. Geben Sie einen Namen für den Datensatz ein. 5. Wählen Sie unter Datensatz typ A – Leitet den Datenverkehr an IPv4 und einige AWS-Ressourcen weiter. 6. Alias aktivieren. 7. Gehen Sie unter Datenverkehr an weiterleiten wie folgt vor:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	a. Wählen Sie Alias zu Network Load Balancer aus. b. Wählen Sie die AWS-Region aus, in der der Network Load Balancer bereitgestellt wird. c. Geben Sie den DNS-Namen des Network Load Balancers ein. 8. Wählen Sie Create records (Datensätze erstellen).	

Einrichten von NGINX VirtualServer auf Amazon EKS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie NGINX bereit VirtualServer.	Die NGINX- VirtualServer Ressource ist eine Load Balancing-Konfiguration, die eine Alternative zur Ingress-Ressource darstellt. Die Konfiguration zum Erstellen der NGINX- VirtualSe rver Ressource ist in der `nginx_virtualserve r.yaml` Datei im `6-Nginx-Virtual-Server` Verzeichnis verfügbar. Geben Sie den folgenden Befehl in ein`kubectl`, um die NGINX-VirtualServer Ressource zu erstellen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`kubectl apply -f nginx_virtualserver.yaml` Wichtig: Stellen Sie sicher, dass Sie den Anwendungsdomänennamen, das Zertifikatsgeheimnis und den Anwendungsservicenamen in der `nginx_virtualserver.yaml` Datei aktualisieren.	
Stellen Sie sicher, dass NGINX erstellt VirtualServer wurde.	Geben Sie den folgenden Befehl in ein, `kubectl` um zu überprüfen, ob die NGINX-VirtualServer Ressource erfolgreich erstellt wurde. `kubectl get virtualserver` Hinweis: Überprüfen Sie, ob die `Host` Spalte mit dem Domänennamen Ihrer Anwendung übereinstimmt.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den NGINX-Web server mit aktiviertem TLS bereit.	Dieses Muster verwendet einen NGINX-Webserver mit aktiviertem TLS als Anwendung zum Testen der end-to-end Verschlüsselung. Die Konfigurationsdateien, die für die Bereitstellung der Testanwendung erforderlich sind, sind im `demo-webserver` Verzeichnis verfügbar. Geben Sie den folgenden Befehl in ein`kubectl`, um die Testanwendung bereitzustellen. `kubectl apply -f nginx-tls-ap.yaml`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Testanwendungsressourcen erstellt wurden.	Geben Sie die folgenden Befehle in ein, `kubectl` um zu überprüfen, ob die erforderlichen Ressourcen für die Testanwendung erstellt wurden: • `kubectl get deployments` Hinweis: Validieren Sie die `Ready` Spalte und die `Available` Spalte. • `kubectl get pods | grep -i example-deploy` Hinweis: Pods sollten sich im `running` Status befinden. • `kubectl get configmap` • `kubectl get svc`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Anwendung.	1. Geben Sie den folgenden Befehl ein, indem Sie durch `<application-domain-name>` den Route53-DNS-Namen ersetzen, den Sie zuvor erstellt haben. `curl --verbose https://<application-domain-name>` 2. Stellen Sie sicher, dass Sie auf die Anwendung zugreifen können.	AWS DevOps

Zugehörige Ressourcen

AWS-Ressourcen

- Erstellen von Datensätzen mithilfe der Amazon Route 53-Konsole (Amazon Route 53-Dokumentation)
- Verwenden eines Network Load Balancer smit dem NGINX Ingress Controller auf Amazon EKS (AWS-Blogbeitrag)

Sonstige Ressourcen

- Route 53 (cert-manager-Dokumentation)
- Konfigurieren von DNS01 Challenge Provider (cert-manager-Dokumentation)
- Let's Encrypt DNS-Herausforderung (Let's Encrypt-Dokumentation)

Vereinfachen Sie die Bereitstellung von Amazon-EKS-Anwendungen mit mehreren Mandanten mithilfe von Flux

Erstellt von Nadeem Rahaman (AWS), Aditya Ambati (AWS), Aniket Dekate (AWS) und Shrikantpatil (AWS)

Code-Repository: aws-eks-multitenancy-deployment	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Container und Microservices
AWS-Services: AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; Amazon EKS; Amazon VPC		

Übersicht

Viele Unternehmen, die -Produkte und -Services anbieten, sind datenreguläre Branchen, die erforderlich sind, um Datenhindernisse zwischen ihren internen Geschäftsbereichen aufrechtzuerhalten. Dieses Muster beschreibt, wie Sie das Multi-Tenancy-Feature in Amazon Elastic Kubernetes Service (Amazon EKS) verwenden können, um eine Datenplattform zu erstellen, die eine logische und physische Isolierung zwischen Mandanten oder Benutzern erreicht, die einen einzigen Amazon-EKS-Cluster gemeinsam nutzen. Das Muster bietet Isolation durch die folgenden Ansätze:

- Kubernetes-Namespace-Isolation
- Rollenbasierte Zugriffskontrolle (RBAC)
- Netzwerkrichtlinien
- Ressourcenkontingente
- AWS Identity and Access Management (IAM)-Rollen für Servicekonten (IRSA)

Darüber hinaus verwendet diese Lösung Flux, um die Mandantenkonfiguration bei der Bereitstellung von Anwendungen unveränderlich zu halten. Sie können Ihre Tenant-Anwendungen bereitstellen, indem Sie das Tenant-Repository angeben, das die Flux-`kustomization.yaml`Datei in Ihrer Konfiguration enthält.

Dieses Muster implementiert Folgendes:

- Ein AWS CodeCommit -Repository, AWS CodeBuild Projekte und eine - AWS CodePipeline Pipeline, die durch manuelle Bereitstellung von Terraform-Skripten erstellt werden.
- Netzwerk- und Rechenkomponenten, die für das Hosten der Mandanten erforderlich sind. Diese werden über CodePipeline und mithilfe CodeBuild von Terraform erstellt.
- Mandanten-Namespaces, Netzwerkrichtlinien und Ressourcenkontingente, die über ein Helm-Diagramm konfiguriert werden.
- Anwendungen, die zu verschiedenen Mandanten gehören, die mithilfe von Flux bereitgestellt werden.

Wir empfehlen Ihnen, Ihre eigene Architektur für Multi-Tenancy auf der Grundlage Ihrer individuellen Anforderungen und Sicherheitsüberlegungen sorgfältig zu planen und zu erstellen. Dieses Muster bietet einen Ausgangspunkt für Ihre Implementierung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2.11.4 oder höher, installiert und konfiguriert
- Terraform Version 0.12 oder höher ist auf Ihrem lokalen Computer installiert
- Terraform AWS Provider Version 3.0.0 oder höher
- Kubernetes-Anbieter Version 2.10 oder höher
- Helm Provider Version 2.8.0 oder höher
- Kubectl Provider Version 1.14 oder höher

Einschränkungen

- Abhängigkeit von manuellen Terraform-Bereitstellungen: Die Ersteinrichtung des Workflows, einschließlich der Erstellung von CodeCommit Repositorys, CodeBuild Projekten und CodePipeline Pipelines, basiert auf manuellen Terraform-Bereitstellungen. Dies führt zu einer potenziellen Einschränkung in Bezug auf Automatisierung und Skalierbarkeit, da es manuelle Eingriffe für Infrastrukturänderungen erfordert.
- CodeCommit Repository-Abhängigkeit: Der Workflow basiert auf CodeCommit Repositorys als Quellcodeverwaltungslösung und ist eng mit - AWS Services verbunden.

Architektur

Zielarchitekturen

Dieses Muster stellt drei Module bereit, um die Pipeline, das Netzwerk und die Datenverarbeitungsinfrastruktur für eine Datenplattform aufzubauen, wie in den folgenden Diagrammen dargestellt.

Pipeline-Architektur:

Netzwerkarchitektur:

Datenverarbeitungsarchitektur:

Tools

AWS-Services

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommitist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf auszuführen, AWS ohne Ihre eigene Kubernetes-Steuerebene oder -Knoten installieren oder warten zu müssen.
- AWS Transit Gateway ist eine zentraler Hub, der Virtual Private Clouds (VPCs) und On-Premises-Netzwerke verbindet.
- Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- Cilium-Netzwerkrichtlinien unterstützen Kubernetes L3- und L4-Netzwerkrichtlinien. Sie können um L7-Richtlinien erweitert werden, um Sicherheit auf API-Ebene für HTTP, Kafka und gRPC sowie andere ähnliche Protokolle zu gewährleisten.
- Flux ist ein Git-basiertes Tool für kontinuierliche Bereitstellung (CD), das Anwendungsbereitstellungen auf Kubernetes automatisiert.
- Helm ist ein Open-Source-Paketmanager für Kubernetes, mit dem Sie Anwendungen auf Ihrem Kubernetes-Cluster installieren und verwalten können.
- Terraform ist ein Infrastructure as Code (IaC HashiCorp)-Tool von , mit dem Sie Cloud- und On-Premises-Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub EKS Multi-Tenancy Terraform Solution Repository verfügbar.

Bewährte Methoden

Richtlinien und bewährte Methoden für die Verwendung dieser Implementierung finden Sie im Folgenden:

- Bewährte Methoden für Amazon EKS mit mehreren Mandanten
- Flux-Dokumentation

Sekunden

Pipelines für Terraform-Entwicklungs-, Test- und Bereitstellungsphasen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Projekt-Repository.	Klonen Sie das GitHub EKS Multi-Tenancy Terraform Solution-Repository, indem Sie den folgenden Befehl in einem Terminalfenster ausführen:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/aws-eks-multitenancy-deployment.git`	

Bootstrappen Sie den Terraform-S3-Bucket und Amazon DynamoDB .	1. Öffnen Sie im `bootstrap` Ordner die `bootstrap.sh` Datei und aktualisieren Sie die Variablenwerte für den S3-Bucket-Namen, den DynamoDB-Tabellennamen und AWS-Region:
	`S3_BUCKET_NAME="<S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME="<DYNAMODB_NAME>" REGION="<AWS_REGION>"`
	2. Führen Sie das `bootstrap.sh` -Skript aus. Das Skript erfordert die AWS CLI, die Sie als Teil der Voraussetzungen installiert haben.
	`cd bootstrap ./bootstrap.sh`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die `locals.tf` Dateien `run.sh` und .	1. Nachdem der Bootstrap -Prozess erfolgreich abgeschlossen wurde, kopieren Sie den S3-Bucket und den DynamoDB-Tabellennamen aus dem `variables` Abschnitt des `bootstrap.sh` Skripts:
	`# Variables S3_BUCKET_NAME="<S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME="<DYNAMODB_NAME"`
	2. Fügen Sie diese Werte in das `run.sh`Skript ein, das sich im Stammverzeichnis des Projekts befindet:
	`BACKEND_BUCKET_ID="<SAME_NAME_AS_S3_BUCKET_NAME>" DYNAMODB_ID="<SAME_NAME_AS_DYNAMODB_NAME>"`
	3. Laden Sie den Projektcode in ein CodeCommit Repository hoch. Sie können dieses Repository automatisch über Terraform erstellen, indem Sie die folgende Variable `true` in der `demo/pipeline/locals.tf` Datei auf setzen:
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`create_new_repo = true` 4. Aktualisieren Sie die `locals.tf` Datei entsprechend Ihren Anforderungen, um Pipeline-Ressourcen zu erstellen.	

Stellen Sie das Pipeline-Modul bereit.	Um Pipeline-Ressourcen zu erstellen, führen Sie die folgenden Terraform-Befehle manuell aus. Es gibt keine Orchestrierung für die automatische Ausführung dieser Befehle.
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t init`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t plan`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t apply`
		AWS DevOps

Erstellen der Netzwerkinfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Pipeline.	1. Stellen Sie im `templates` Ordner sicher, dass für die `buildspec` Dateien	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die folgende Variable auf festgelegt ist`network`: `TF_MODULE_TO_BUILD: "network"` 2. Starten Sie auf der Seite mit den Pipeline-Details der CodePipeline Konsole die Pipeline, indem Sie Release change auswählen. Nach dieser ersten Ausführung wird die Pipeline automatisch gestartet, wenn Sie eine Änderung am Hauptzweig des CodeCommit Repositorys vornehmen. Die Pipeline umfasst die folgenden Phasen: • `validate` initialisiert Terraform, führt Terraform-Sicherheitsscans mithilfe der Tools checkov und tfsec aus und lädt die Scanberichte in den S3-Bucket hoch. • `plan` zeigt den Terraform-Plan an und lädt den Plan in den S3-Bucket hoch. • `apply` wendet die Terraform-Planausgabe aus dem S3-Bucket an und erstellt AWS Ressourcen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `destroy` entfernt die AWS Ressourcen, die während der `-apply`Phase erstellt wurden. Um diese optionale Phase zu aktivieren, setzen Sie die folgende Variable `true` in der `demo/pipeline/locals.tf` Datei auf : `enable_destroy_stage = true`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die über das Netzwerkmodul erstellten Ressourcen.	Vergewissern Sie sich, dass die folgenden AWS Ressourcen erstellt wurden, nachdem die Pipeline erfolgreich bereitgestellt wurde: • Eine Ausgangs-VPC mit drei öffentlichen und drei privaten Subnetzen, einem Internet-Gateway und einem NAT-Gateway. • Eine Amazon-EKS-VPC mit drei privaten Subnetzen. • Tenant 1- und Tenant 2-VPCs mit jeweils drei privaten Subnetzen. • Ein Transit-Gateway mit allen VPC-Anhängen und Routen zu jedem privaten Subnetz. • Eine statische Transit-Gateway-Route für die Amazon-EKS-Ausgangs-VPC mit dem Ziel-CIDR-Block `0.0.0.0/0` . Dies ist erforderlich, damit alle VPCs ausgehenden Internetzugang über die Amazon-EKS-Ausgangs-VPC haben.	AWS DevOps

Erstellen der Datenverarbeitungsinfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie `locals.tf` , um dem CodeBuild Projekt den Zugriff auf die VPC zu ermöglichen.	Um die Add-Ons für den privaten Amazon-EKS-Cluster bereitzustellen, muss das CodeBuild Projekt an die Amazon-EKS-VPC angehängt werden.
	1. Öffnen Sie im `demo/pipeline` Ordner die `locals.tf` Datei und setzen Sie die `vpc_enabled` Variable auf `true`.
	2. Führen Sie das `run.sh` Skript aus, um die Änderungen auf das Pipeline-Modul anzuwenden:
	`demo/pipeline/locals.tf`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd init`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd plan`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd apply`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die `buildspec` Dateien, um das Rechenmodul zu erstellen.	Legen Sie im `templates` Ordner in allen `buildspec` YAML-Dateien den Wert der `TF_MODULE_TO_BUILD` Variablen von `network` auf fest`compute`: `TF_MODULE_TO_BUILD: "compute"`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die `values` Datei für das Helm-Diagramm für die Mandantenverwaltung.	1. Öffnen Sie die `values.yaml` Datei am folgenden Speicherort:
	`cd cfg-terraform/demo/compute/cfg-tenant-mgmt`
	Die Datei sieht wie folgt aus:
	`---`
	`global:`
	`  clusterRoles:`
	`  operator:`
	`  platform-tenant`
	`  flux: flux-tenant-applier`
	`  flux:`
	`  tenantCloneBaseUrl: ${TEANT_BASE_URL}`
	`  repoSecret:`
	`  ${TENANT_REPO_SECRET}`
	`tenants:`
	`  tenant-1:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 1Gi`
	`  flux:`
	`  path: overlays/tenant-1`
	`  tenant-2:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 2Gi`
	`  flux:`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>path: overlays/
	tenant-2</pre>
	2. Aktualisieren Sie in den `tenants` Abschnitten `global` und die Konfiguration basierend auf Ihren Anforderungen:
	• `tenantCloneBaseUrl` – Pfad zum Repository, das den Code für alle Mandanten hostet (wir verwenden dasselbe Git-Repository für alle Mandanten)
	• `repoSecret` – Kubernetes-Secret, das die SSH-Schlüssel und bekannten Hosts enthält, um sich beim globalen Tenant-Git-Repository zu authentifizieren
	• `quotas` – Kubernetes-Ressourcenkontingente, die Sie für jeden Mandanten anwenden möchten
	• `flux path` – Pfad zu den YAML-Dateien der Tenant-Anwendung im globalen Tenant-Repository	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Rechenres sourcen.	Nachdem Sie die Dateien in den vorherigen Schritten aktualisiert haben, CodePipel ine startet automatisch. Vergewissern Sie sich, dass die folgenden AWS Ressource n für die Datenverarbeitungs infrastruktur erstellt wurden: • Amazon-EKS-Cluster mit privatem Endpunkt • Amazon-EKS-Worker-Knoten • Amazon-EKS-Add-ons: externe Secrets`aws-loadb alancer-controller` , und `metrics-server` • GitOps Modul, Flux Helm chart, Cilium Helm chart und Helm chart für die Mandantenverwaltung	AWS DevOps

Überprüfen der Mandantenverwaltung und anderer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Mandanten verwaltungsressourcen in Kubernetes.	Führen Sie die folgenden Befehle aus, um zu überprüfe n, ob Mandantenverwaltun gsressourcen mithilfe von Helm erfolgreich erstellt wurden.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Tenant-Namespaces wurden erstellt, wie unter angegeben`values.yaml` :
	`kubectl get ns -A`
	2. Kontingente werden jedem Mandanten-Namespac e zugewiesen, wie in angegeben`values.yaml` :
	`kubectl get quota --namespace=<tenant_namespace>`
	3. Details zu Kontingenten sind für jeden Mandanten-Namespace korrekt:
	`kubectl describe quota cpu-memory-resourc e-quota-limit -n <tenant_namespace>`
	4. Auf jeden Mandanten -Namespace wurden Cilium-Netzwerkrichtlinien angewendet:
	`kubectl get CiliumNet workPolicy -A`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellung von Tenant-Anwendungen.	Führen Sie die folgenden Befehle aus, um zu überprüfen, ob die Tenant-Anwendungen bereitgestellt wurden.
	
	1. Flux kann eine Verbindung mit dem im GitOps Modul angegebenen CodeCommit Repository herstellen:
	
	`kubectl get gitrepositories -A`
	
	2. Der Flux-Kustomisierungscontroller hat die YAML-Dateien im CodeCommit Repository bereitgestellt:
	
	`kubectl get kustomizations -A`
	
	3. Alle Anwendungsressourcen werden in ihren Mandanten-Namespaces bereitgestellt:
	
	`kubectl get all -n <tenant_namespace>`
	
	4. Für jeden Mandanten wurde ein Ingress erstellt:
	
	`kubectl get ingress -n <tenant_namespace>`	

Fehlerbehebung

Problem	Lösung

Es wird eine Fehlermeldung ähnlich der folgenden angezeigt:
 	
`Failed to checkout and determine revision: unable to clone unknown error: You have successfully authenticated over SSH. You can use Git to interact with AWS CodeCommit.`
	Gehen Sie wie folgt vor, um das Problem zu beheben:
	
	1. Überprüfen Sie das Tenant-Anwendungs-Repository: Ein leeres oder falsch konfiguri ertes Repository kann den Fehler verursach en. Stellen Sie sicher, dass das Tenant-An wendungs-Repository den erforderlichen Code enthält.
	2. Stellen Sie das `tenant_mgmt` Modul erneut bereit: Suchen Sie in der `tenant_mg mt` Modulkonfigurationsdatei den `app` Block und legen Sie dann den `deploy` Parameter auf fest`0`:
	
	`deploy = 0`
	
	Nachdem Sie den Terraform-`apply`Befehl ausgeführt haben, ändern Sie den `deploy` Parameterwert wieder in `1`:
	
	`deploy = 1`
	
	3. Überprüfen Sie den Status erneut: Nachdem Sie die vorherigen Schritte ausgeführt haben, verwenden Sie den folgenden Befehl, um zu überprüfen, ob das Problem weiterhin besteht:
	
	`kubectl get gitrepositories -A`
	
	Wenn es bestehen bleibt, sollten Sie sich eingehender mit den Flux-Protokollen

Problem	Lösung
	befassen, um weitere Informationen zu erhalten, oder lesen Sie den allgemeinen Leitfaden zur Fehlerbehebung von Flux.

Zugehörige Ressourcen

- Amazon-EKS-Blueprints für Terraform
- Bewährte Methoden für Amazon EKS, Abschnitt „Multi-Tenancy“
- Flux-Website
- Helm-Website

Zusätzliche Informationen

Hier ist ein Beispiel für eine Repository-Struktur für die Bereitstellung von Tenant-Anwendungen:

```
applications
sample_tenant_app
### README.md
### base
#   ### configmap.yaml
#   ### deployment.yaml
#   ### ingress.yaml
#   ### kustomization.yaml
#   ### service.yaml
### overlays
    ### tenant-1
    #   ### configmap.yaml
    #   ### deployment.yaml
    #   ### kustomization.yaml
    ### tenant-2
        ### configmap.yaml
        ### kustomization.yaml
```

Abonnieren mehrerer E-Mail-Endpunkte für ein SNS-Thema mithilfe einer benutzerdefinierten Ressource

Erstellt von Ricardoais (AWS)

Umgebung: Produktion	Technologien: DevOps	AWS-Services: Amazon SNS; AWS CloudFormation; AWS Lambda

Übersicht

Hinweis: August 2022: AWS unterstützt CloudFormation jetzt das Abonnement mehrerer Ressourcen über das AWS::SNS::Topic Objekt und sein Abonnementattribut.

Dieses Muster beschreibt, wie Sie mehrere E-Mail-Adressen abonnieren, um Benachrichtigungen von einem Amazon Simple Notification Service (Amazon SNS)-Thema zu erhalten. Es verwendet eine AWS Lambda-Funktion als benutzerdefinierte Ressource in einer AWS- CloudFormation Vorlage. Die Lambda-Funktion ist einem Eingabeparameter zugeordnet, der die E-Mail-Endpunkte für das SNS-Thema angibt.

Derzeit können Sie die AWS- CloudFormation Vorlagenobjekte AWS::SNS::Topic und verwenden, AWS::SNS::Subscription um einzelne Endpunkte für SNS-Themen zu abonnieren. Um mehrere Endpunkte zu abonnieren, müssen Sie das Objekt mehrmals aufrufen. Durch die Verwendung der Lambda-Funktion als benutzerdefinierte Ressource können Sie mehrere Endpunkte über einen Eingabeparameter abonnieren. Sie können diese Lambda-Funktion als benutzerdefinierte Ressource in jeder AWS- CloudFormation Vorlage verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein AWS-Profil, das in Ihrer lokalen Umgebung mit einem Zugriffsschlüssel und einem geheimen Schlüssel konfiguriert ist. Sie können diesen Code auch von AWS Cloud9 aus ausführen.
- Berechtigungen für Folgendes:
  - AWS Identity and Access Management (IAM)-Rolle und -Richtlinie

- AWS Lambda-Funktion
- Amazon Simple Storage Service (Amazon S3) zum Hochladen der Lambda-Funktion
- Amazon SNS-Thema und -Richtlinie
- AWS- CloudFormation Stacks

Einschränkungen

- Der Code unterstützt Linux- und macOS-Workstations.

Produktversionen

- AWS Command Line Interface (AWS CLI) Version 2 oder höher.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- Amazon SNS
- AWS Lambda

Tools

Tools

- AWS CLI Version 2

Code

Der Anhang enthält die folgenden Dateien:

- Lambda-Funktion: `lambda_function.py`
- AWS- CloudFormation Vorlage: `template.yaml`
- Zwei Parameterdateien zur Bearbeitung mehrerer oder einzelner E-Mail-Endpunktabonnements: `parameters-multiple-values.json` (wird als Standard verwendet) und `parameters-one-value.json`

Um den Stack bereitzustellen, können Sie beide Parameterdateien verwenden. So geben Sie mehrere E-Mail-Endpunkte an:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>
```

So geben Sie einen einzelnen E-Mail-Endpunkt an:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json
```

Polen

Option 1 – Bereitstellen eines SNS-Themas mit einem E-Mail-Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den E-Mail-Endpunkt für SNS-Theme nabonnements.	Bearbeiten Sie die Datei `parameters-one-value.json` (angefügt) und ändern Sie den Wert des `pSNSNotificationsEmail` Parameters so, dass er die E-Mail-Adresse widerspiegelt, die Sie verwenden möchten, z. B. `someone@example.com` .	
Stellen Sie den AWS-CloudFormation Stack bereit, der die Ressourcen und das Abonnement erstellt.	Führen Sie den Befehl deploy.sh mit Ihrem AWS-Profilnamen, Ihrer AWS-Region und der `-parameters-one-value.json` Datei aus. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f`	IAM-Rolle mit den richtigen Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`parameters-one-value.json`	

Option 2 – Bereitstellen eines SNS-Themas mit zwei oder mehr E-Mail-Abonnements

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die E-Mail-Endpunkte für SNS-Theme nabonnements.	Bearbeiten Sie die Datei `parameters-multiple-values.json` (angefügt) und ändern Sie den Wert des `pSNSNotificationsEmail` Parameters so, dass er die E-Mail-Adressen widerspiegelt, die Sie verwenden möchten, getrennt durch Kommas: `someone1@example.com,someone2@example.com` .	
Stellen Sie den AWS-CloudFormation Stack bereit, der die Ressourcen und das Abonnement erstellt.	Führen Sie den Befehl deploy.sh mit Ihrem AWS-Profilnamen und Ihrer AWS-Region aus. Sie müssen die `parameters-multiple-values.json` Datei nicht angeben, da sie standardmäßig verwendet wird. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>`	IAM-Rolle mit den richtigen Berechtigungen

Option 3 – Bereitstellen eines SNS-Themas über eine AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Erstellen Sie ein SNS-Thema über eine AWS-CloudFormation Vorlage, ohne Abonnementendpunkte im `AWS::SNS::Topic` Vorlagenobjekt anzugeben. Sie können `template.yaml` in der Anfügung als Ausgangspunkt verwenden.	IAM-Rolle mit den richtigen Berechtigungen
Erstellen Sie eine SNS-Themenrichtlinie.	Erstellen Sie eine SNS-Themenrichtlinie in der AWS-CloudFormation Vorlage.	IAM-Rolle mit den richtigen Berechtigungen
Abonnieren Sie die Liste der E-Mail-Endpunkte für das SNS-Thema.	Abonnieren Sie auf der Grundlage der Liste der E-Mail-Endpunkte (ein oder mehrere) die Endpunkte für das von Ihnen erstellte SNS-Thema.	IAM-Rolle mit den richtigen Berechtigungen

Zugehörige Ressourcen

Referenzen

- CloudFormation Benutzerdefinierte AWS-Ressourcen (AWS-Dokumentation)
- Erstellung CloudFormation benutzerdefinierter AWS-Ressourcen mit Python, AWS Lambda und crhelper (Blogbeitrag)

Erforderliche Tools

- AWS CLI Version 2

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Verwenden von Serverspec für die testgesteuerte Entwicklung von Infrastrukturcode

Erstellt von Sushant Jagdale (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur; Hybrid Cloud	AWS-Services: Amazon EC2; AWS CodeBuild; AWS CodeDeploy

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Serverspec verwenden, um testgesteuerte Entwicklung (TDD) beim Schreiben von Infrastrukturcode in der Amazon Web Services (AWS) Cloud zu verwenden. Das Muster behandelt auch die Automatisierung mit AWS CodePipeline. TDD konzentriert sich darauf, was der Infrastrukturcode tun muss, und legt eine klare Definition von erledigt fest. Sie können Serverspec verwenden, um die Infrastruktur zu testen HashiCorp, die mit Tools wie AWS CloudFormation, Terraform von und Ansible erstellt wurde.

Serverspec hilft beim Faktorwechsel des Infrastrukturcodes. Mit Serverspec können Sie RSpec-Tests schreiben, um die Installation verschiedener Pakete und Software zu überprüfen, Befehle auszuführen, nach laufenden Prozessen und Ports zu suchen, Dateiberechtigungseinstellungen zu überprüfen usw. Serverspec prüft, ob Ihre Server korrekt konfiguriert sind. Sie installieren nur Ruby auf Ihren Servern. Sie müssen keine Agent-Software installieren.

Testgesteuerte Infrastruktur bietet die folgenden Vorteile:

- Plattformübergreifende Tests
- Validierung der Erwartungen
- Vertrauen in Ihre Automatisierung
- Konsistenz und Stabilität der Infrastruktur
- Frühes Fehlschlagen

Sie können dieses Muster verwenden, um Serverspec-Einheitstests für Apache-Software auszuführen und die Einstellungen für die Dateiberechtigung während der Erstellung von Amazon

Machine Image (AMI) zu überprüfen. Ein AMI wird nur erstellt, wenn alle Testfälle erfolgreich sind. Serverspec führt die folgenden Tests durch:

- Der Apache-Prozess wird ausgeführt.
- Der Apache-Port wird ausgeführt.
- Apache-Konfigurationsdateien und Verzeichnisse existieren an bestimmten Speicherorten usw.
- Dateiberechtigungen sind korrekt konfiguriert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Eine Virtual Private Cloud (VPC) mit einem öffentlichen Subnetz
- Installation von AWS Command Line Interface (AWS CLI) und Git

Produktversionen

- HashiCorp Packer-Version: 1.6.6
- Ruby-Version: 2.5.1 und höher
- AWS CLI-Version: 1.18.185

Architektur

Zielarchitektur

1. Wenn Sie den Code in das CodeCommit Repository übertragen, löst ein Amazon CloudWatch Events-Ereignis die aus CodePipeline. In der ersten Phase der Pipeline wird der Code von abgerufen CodeCommit.

2. In der zweiten Pipeline-Phase wird ausgeführt CodeBuild, wodurch die Packer-Vorlage validiert und erstellt wird.
3. Als Teil des Packer Build Provisioner installiert Packer die Software Apache und Ruby. Dann ruft der Provisioner ein Shell-Skript auf, das Serverspec verwendet, um den Apache-Prozess, den Port, die Dateien und die Verzeichnisse zu testen. Der Packer-Post-Prozessor schreibt eine JSON-Datei (JavaScript Object Notation) mit einer Liste aller Artefakte, die von Packer während einer Ausführung erzeugt wurden
4. Schließlich wird eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance mit der von Packer erstellten AMI-ID erstellt.

Tools

- AWS CLI – Amazon Command Line Interface (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services mithilfe von Befehlen in Ihrer Befehlszeilen-Shell.
- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen near-real-time Stream von Systemereignissen bereit, die Änderungen an Amazon Web Services (AWS)-Ressourcen beschreiben.
- AWS CodeBuild – AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Einheitentests durch und erzeugt Artefakte, die bereitgestellt werden können.
- AWS CodeCommit – AWS CodeCommit ist ein Service zur Versionskontrolle, der von Amazon Web Services gehostet wird. Sie können verwenden CodeCommit , um Komponenten (wie Dokumente, Quellcode und Binärdateien) privat in der Cloud zu speichern und zu verwalten.
- AWS CodePipeline – AWS CodePipeline ist ein kontinuierlicher Bereitstellungsservice, mit dem Sie die Schritte zur Veröffentlichung Ihrer Software modellieren, visualisieren und automatisieren können. Sie können die verschiedenen Phasen eines Prozesses für die Veröffentlichung von Software schnell modellieren und konfigurieren.
- HashiCorp Packer – HashiCorp Packer ist ein Tool zur Automatisierung der Erstellung identischer Computerabbilder aus einer einzigen Quellkonfiguration.
- Serverspec – Serverspec führt RSpec-Tests durch, um die Serverkonfiguration zu überprüfen. Serverspec verwendet Ruby und Sie müssen keine Agent-Software installieren.

Code

Der Code ist angehängt. Der Code verwendet die folgende Struktur mit drei Verzeichnissen und acht Dateien.

```
### amazon-linux_packer-template.json (Packer template)
### buildspec.yaml (CodeBuild .yaml file)
### pipeline.yaml (AWS CloudFormation template to automate CodePipeline)
### rspec_tests (RSpec required files and spec)
#   ### Gem-file
#   ### Rakefile
#   ### spec
#       ### apache_spec.rb
#       ### spec_helper.rb
### scripts
    ### rspec.sh (Installation of Ruby and initiation of RSpec)
```

Polen

Konfigurieren von AWS-Anmeldeinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen IAM-Benutzer.	Erstellen Sie einen AWS Identity and Access Management (IAM)-Benutzer mit programmatischem Zugriff und Konsolenzugriff. Weitere Informationen finden Sie in der AWS-Dokumentation.	Entwickler, Systemadministrator, DevOps Techniker
Konfigurieren Sie AWS-Anmeldeinformationen.	Konfigurieren Sie auf Ihrem lokalen Computer oder in Ihrer Umgebung die AWS-Anmeldeinformationen für den IAM-Benutzer. Anweisungen finden Sie in der AWS-Dokumentation.	Entwickler, Systemadministrator, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihre -Anmeldei nformationen.	Führen Sie den folgenden Befehl aus, um die konfiguri erten Anmeldeinformationen zu validieren. `aws sts get-caller-identity --profile <profile>`	Entwickler, Systemadm inistrator, DevOps Techniker

AWS CodePipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Führen Sie den folgenden Befehl aus, um ein CodeCommit Repository zu erstellen. `aws codecommit create-repository --repository-name "<provide repository-name>" --repository-description "repository to unit test the infrastructure code"`	Entwickler, Systemadm inistrator, DevOps Techniker
Schreiben Sie RSpec-Tests.	Erstellen Sie RSpec-Testfälle für Ihre Infrastruktur. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informati onen.	Entwickler, DevOps Techniker
Push-Code in das CodeCommit Repository.	Führen Sie die folgenden Befehle aus, um den	Entwickler, Systemadm inistrator, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	angehängten Code in das CodeCommit Repository zu übertragen.
	
	`git clone <repository url>`
	`cp -R /tmp/<code folder>/ <repository_folder>/`
	`git add .`
	`git commit -m"initial commit"`
	`git push`	

Erstellen Sie die Pipeline.	Um die Pipeline zu erstellen, führen Sie den AWS CLI-Befehl aus, der sich im Abschnitt Zusätzliche Informationen befindet.	Entwickler, Systemadministrator, DevOps Techniker
Starten Sie die Pipeline.	Übergeben Sie Code in das CodeCommit Repository. Jeder Commit an das Repository initiiert die Pipeline.	Entwickler, Systemadministrator, DevOps Techniker
Testen Sie die Apache-URL.	Verwenden Sie die folgende URL, um die AMI-Installation zu testen. `http://<your instance public ip>/hello.html` Auf der Seite wird die Meldung „Hello from Apache“ angezeigt.	Entwickler, Systemadministrator, DevOps Techniker

Zugehörige Ressourcen

- HashiCorp
- HashiCorp Packer
- Serverspezifikation
- Einführung in ServerSpec: Was ist Serverspec und wie verwenden wir es unter Stelligent? (externer Blogbeitrag)
- Testgesteuerte Entwicklung von Infrastrukturcode (externer Blogbeitrag)
- Erstellen und Testen von Bildern mit HashiCorp Packer und ServerSpec (externer Artikel)

Zusätzliche Informationen

Schreiben von RSpec-Tests

Der RSpec-Test für dieses Muster befindet sich unter `<repository folder>/rspec_tests/spec/apache_spec.rb`.

```
require 'spec_helper'


describe service('httpd') do
  it { should be_enabled }
  it { should be_running }
end


describe port(80) do
  it { should be_listening }
end


describe file('/etc/httpd/conf/httpd.conf') do
  it { should exist }
  it { should be_owned_by 'root' }
  it { should contain 'ServerName www.example.com' }
end


describe file('/etc/httpd/conf/httpd.conf') do
  its(:content) { should match /ServerName www.example.com/ }
```

```
end


describe file('/var/www/html/hello.html') do
  it { should exist }
  it { should be_owned_by 'ec2-user' }
end


describe file('/var/log/httpd') do
  it { should be_directory }
end


describe file('/etc/sudoers') do
  it { should be_mode 440 }
end


describe group('root') do
  it { should have_gid 0 }
end
```

Sie können dem `/spec` Verzeichnis eigene Tests hinzufügen.

Erstellen der Pipeline

```
aws cloudformation create-stack --stack-name myteststack --template-body file://
pipeline.yaml --parameters ParameterKey=RepositoryName,ParameterValue=<provide
 repository-name> ParameterKey=ApplicationName,ParameterValue=<provide
 application-name> ParameterKey=SecurityGroupId,ParameterValue=<provide
 SecurityGroupId> ParameterKey=VpcId,ParameterValue=<provide VpcId>
 ParameterKey=SubnetId,ParameterValue=<provide SubnetId> ParameterKey=Region,ParameterValue=<pr
 AccountId> --capabilities CAPABILITY_NAMED_IAM
```

Parameterdetails

`repository-name` – Der Name des AWS- CodeCommit Repositorys

`application-name` – Der Amazon-Ressourcenname (ARNs) ist mit verknüpft`ApplicationName`; geben Sie einen beliebigen Namen an

`SecurityGroupId` – Jede Sicherheitsgruppen-ID aus Ihrem AWS-Konto, für die Port 80 geöffnet ist

`VpcId` – Die ID Ihrer VPC

`SubnetId` – Die ID eines öffentlichen Subnetzes in Ihrer VPC

`Region` – Die AWS-Region, in der Sie dieses Muster ausführen

`Keypair` – Der Secure Shell (SSH)-Schlüsselname, um sich bei der EC2-Instance anzumelden

`AccountId` – Ihre AWS-Konto-ID

Sie können eine CodePipeline Pipeline auch erstellen, indem Sie die AWS-Managementkonsole verwenden und dieselben Parameter übergeben, die sich in der vorherigen Befehlszeile befinden.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Verwenden Sie Git-Quell-Repositorys von Drittanbietern in AWS CodePipeline

Umgebung: PoC oder Pilotprojekt	Technologien: DevOps	Arbeitsaufwand: Open Source
AWS-Dienste: AWS CodeBuild; AWS CodePipeline; AWS Lambda		

Übersicht

Dieses Muster beschreibt, wie AWS CodePipeline mit Git-Quell-Repositorys von Drittanbietern verwendet wird.

AWS CodePipeline ist ein Continuous Delivery Service, der Aufgaben zum Erstellen, Testen und Bereitstellen Ihrer Software automatisiert. Der Service unterstützt derzeit Git-Repositorys GitHub, die von AWS und Atlassian CodeCommit Bitbucket verwaltet werden. Einige Unternehmen verwenden jedoch Git-Repositorys von Drittanbietern, die in ihren Single Sign-On-Dienst (SSO) und Microsoft Active Directory zur Authentifizierung integriert sind. Sie können diese Git-Repositorys von Drittanbietern als Quellen verwenden, CodePipeline indem Sie benutzerdefinierte Aktionen und Webhooks erstellen.

Ein Webhook ist eine HTTP-Benachrichtigung, die Ereignisse in einem anderen Tool, z. B. einem GitHub Repository, erkennt und diese externen Ereignisse mit einer Pipeline verbindet. Wenn Sie einen Webhook in erstellen CodePipeline, gibt der Service eine URL zurück, die Sie in Ihrem Git-Repository-Webhook verwenden können. Wenn Sie Code in einen bestimmten Branch des Git-Repositorys pushen, initiiert der Git-Webhook den CodePipeline Webhook über diese URL und setzt die Quellphase der Pipeline auf In Bearbeitung. Wenn sich die Pipeline in diesem Status befindet, fragt ein Job-Worker CodePipeline nach dem benutzerdefinierten Job ab, führt den Job aus und sendet einen Erfolgs- oder Fehlerstatus an. CodePipeline Da sich die Pipeline in der Quellphase befindet, ruft der Job-Worker in diesem Fall den Inhalt des Git-Repositorys ab, komprimiert den Inhalt und lädt ihn in den Amazon Simple Storage Service (Amazon S3) -Bucket hoch, in dem Artefakte für die Pipeline gespeichert werden. Dabei wird der Objektschlüssel verwendet, der vom abgefragten Job bereitgestellt wird. Sie können auch einen Übergang für die benutzerdefinierte Aktion mit einem

Ereignis in Amazon CloudWatch verknüpfen und den Job Worker auf der Grundlage des Ereignisses initiieren. Mit diesem Setup können Sie Git-Repositorys von Drittanbietern, die der Dienst nicht nativ unterstützt, als Quellen verwenden. CodePipeline

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Git-Repository, das Webhooks unterstützt und über das Internet eine Verbindung zu einer CodePipeline Webhook-URL herstellen kann
- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde für die Verwendung mit dem AWS-Konto installiert und konfiguriert

Architektur

Das Muster umfasst die folgenden Schritte:

1. Der Benutzer überträgt Code in ein Git-Repository.
2. Der Git-Webhook wird aufgerufen.
3. Der CodePipeline Webhook wird aufgerufen.
4. Die Pipeline ist auf In Bearbeitung gesetzt, und die Quellphase ist auf den Status In Bearbeitung gesetzt.
5. Die Aktion der Quellphase initiiert eine CloudWatch Ereignisregel, die angibt, dass sie gestartet wurde.
6. Das CloudWatch Ereignis initiiert eine Lambda-Funktion.
7. Die Lambda-Funktion ruft die Details des benutzerdefinierten Aktionsjobs ab.
8. Die Lambda-Funktion initiiert AWS CodeBuild und übergibt ihm alle auftragsbezogenen Informationen.
9. CodeBuild ruft den öffentlichen SSH-Schlüssel oder die Benutzeranmeldeinformationen für den HTTPS-Git-Zugriff von Secrets Manager ab.
10. CodeBuild klont das Git-Repository für einen bestimmten Branch.
11. CodeBuild komprimiert das Archiv und lädt es in den S3-Bucket hoch, der CodePipeline als Artefaktspeicher dient.

Tools

- AWS CodePipeline — AWS CodePipeline ist ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses für jede Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells. Auf diese Weise können Sie Funktionen und Updates schnell und zuverlässig bereitstellen. Sie können AWS CodePipeline in Dienste von Drittanbietern wie GitHub oder mit Ihrem eigenen benutzerdefinierten Plugin integrieren.
- AWS Lambda — Mit AWS Lambda können Sie Code ausführen, ohne Server bereitzustellen oder zu verwalten. Mit Lambda können Sie Code für praktisch jede Art von Anwendung oder Backend-Service ausführen, ohne dass eine Verwaltung erforderlich ist. Sie laden Ihren Code hoch und Lambda kümmert sich um alles, was für die Ausführung und Skalierung Ihres Codes mit hoher Verfügbarkeit erforderlich ist. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS-Services aus initiiert wird, oder ihn direkt von einer beliebigen Web- oder mobilen App aus aufrufen.
- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Continuous Integration Service, der Quellcode kompiliert, Tests durchführt und Softwarepakete produziert, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen.
- AWS Secrets Manager — AWS Secrets Manager hilft Ihnen beim Schutz von Geheimnissen, die Sie für den Zugriff auf Ihre Anwendungen, Services und IT-Ressourcen benötigen. Mit diesem Service können Sie Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus rotieren, verwalten und abrufen. Benutzer und Anwendungen rufen Geheimnisse ab, indem sie Secrets Manager Manager-APIs aufrufen, ohne sensible Informationen im Klartext fest codieren zu müssen. Secrets Manager bietet geheime Rotation mit integrierter Integration für Amazon Relational Database Service (Amazon RDS), Amazon Redshift und Amazon DocumentDB. Der Service kann erweitert werden, um andere Arten von Geheimnissen zu unterstützen, darunter API-Schlüssel und OAuth-Token. Darüber hinaus können Sie mit Secrets Manager den Zugriff auf geheime Daten mithilfe detaillierter Berechtigungen kontrollieren

und die Rotation von Geheimnissen zentral für Ressourcen in der AWS-Cloud, in Diensten von Drittanbietern und in lokalen Umgebungen überprüfen.

- Amazon CloudWatch — Amazon CloudWatch ist ein Überwachungs- und Beobachtungsdienst für DevOps Ingenieure, Entwickler, Site Reliability Engineers (SREs) und IT-Manager. CloudWatch bietet Ihnen Daten und umsetzbare Erkenntnisse, um Ihre Anwendungen zu überwachen, auf systemweite Leistungsänderungen zu reagieren, die Ressourcennutzung zu optimieren und einen einheitlichen Überblick über den Betriebsstatus zu erhalten. CloudWatch sammelt Überwachungs- und Betriebsdaten in Form von Protokollen, Metriken und Ereignissen und bietet Ihnen so einen einheitlichen Überblick über AWS-Ressourcen, -Anwendungen und -Services, die auf AWS- und lokalen Servern ausgeführt werden. Sie können CloudWatch damit anomales Verhalten in Ihren Umgebungen erkennen, Alarme einrichten, Protokolle und Metriken nebeneinander visualisieren, automatisierte Maßnahmen ergreifen, Probleme beheben und Erkenntnisse gewinnen, damit Ihre Anwendungen reibungslos funktionieren.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, mit dem Sie beliebige Datenmengen für eine Reihe von Anwendungsfällen speichern und schützen können, z. B. für Websites, mobile Anwendungen, Sicherung und Wiederherstellung, Archivierung, Unternehmensanwendungen, IoT-Geräte und Big-Data-Analysen. Amazon S3 bietet easy-to-use Verwaltungsfunktionen, mit denen Sie Ihre Daten organisieren und fein abgestimmte Zugriffskontrollen konfigurieren können, um Ihre spezifischen Geschäfts-, Organisations- und Compliance-Anforderungen zu erfüllen.

Epen

Erstellen Sie eine benutzerdefinierte Aktion in CodePipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine benutzerdefinierte Aktion mit AWS CLI oder AWS CloudFormation.	Dieser Schritt beinhaltet die Erstellung einer benutzerdefinierten Quellaktion, die in der Quellphase einer Pipeline in Ihrem AWS-Konto in einer bestimmten Region verwendet werden kann. Sie müssen AWS CLI oder AWS CloudFormation (nicht die	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole) verwenden, um die benutzerdefinierte Quellaktion zu erstellen. Weitere Informationen zu den in diesem und anderen Epen beschriebenen Befehlen und Schritten finden Sie im Abschnitt „Verwandte Ressourcen“ am Ende dieses Musters. Verwenden Sie in AWS CLI den create-custom-action-type Befehl. Verwenden Sie --configuration-properties, um alle Parameter bereitzustellen, die der Job-Worker verarbeiten muss, wenn er einen Job abfragt. CodePipeline Notieren Sie sich unbedingt die für die Optionen --provider und --action-version bereitgestellten Werte, damit Sie dieselben Werte verwenden können, wenn Sie die Pipeline mit diesem benutzerdefinierten Quellschritt erstellen. Sie können die benutzerdefinierte Quellaktion auch in AWS CloudFormation mithilfe des Ressourcentyps AWS::CodePipeline::CustomActionType erstellen.	

Authentifizierung einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SSH-Schlü sselpaar.	Erstellen Sie ein Secure Shell (SSH) -Schlüsselpaar. Anweisungen finden Sie in der GitHub Dokumentation.	Systeme/ Ingenieur DevOps
Erstellen Sie ein Geheimnis in AWS Secrets Manager.	Kopieren Sie den Inhalt des privaten Schlüssels aus dem SSH-Schlüsselpaar und erstellen Sie ein Geheimnis in AWS Secrets Manager. Dieses Geheimnis wird für die Authentifizierung beim Zugriff auf das Git-Repository verwendet.	Allgemeines AWS
Fügen Sie den öffentlichen Schlüssel zum Git-Repository hinzu.	Fügen Sie den öffentlichen Schlüssel aus dem SSH-Schlü sselpaar zu den Kontoeins tellungen des Git-Repos itorys hinzu, um sich anhand des privaten Schlüssels zu authentifizieren.	Systeme/ Ingenieur DevOps

Erstellen Sie eine Pipeline und einen Webhook

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline, die die benutzerdefinierte Quellaktion enthält.	Erstellen Sie eine Pipeline in CodePipeline. Wenn Sie die Quellstufe konfigurieren, wählen Sie die benutzerd efinierte Quellaktion aus, die Sie zuvor erstellt haben. Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können dies in der CodePipeline AWS-Konsole oder in der AWS-CLI tun. CodePipeline fordert Sie zur Eingabe der Konfigurationseigenschaften auf, die Sie für die benutzerdefinierte Aktion festgelegt haben. Diese Informationen sind erforderlich, damit der Job-Worker den Job für die benutzerdefinierte Aktion bearbeiten kann. Folgen Sie dem Assistenten und erstellen Sie die nächste Phase für die Pipeline.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CodePipeline Webhook.	Erstellen Sie einen Webhook für die Pipeline, die Sie mit der benutzerdefinierten Quellaktion erstellt haben. Sie müssen AWS CLI oder AWS CloudFormation (nicht die Konsole) verwenden, um den Webhook zu erstellen. Führen Sie in der AWS-CLI den Befehl put-webhook aus und geben Sie die entsprechenden Werte für die Webhook-Optionen an. Notieren Sie sich die Webhook-URL, die der Befehl zurückgibt. Wenn Sie AWS verwenden CloudFormation , um den Webhook zu erstellen, verwenden Sie den Ressourcentyp AWS::CodePipeline::Webhook. Stellen Sie sicher, dass Sie die Webhook-URL aus der erstellten Ressource ausgeben, und notieren Sie sich diese.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion und ein CodeBuild Lambda-Projekt.	In diesem Schritt verwenden Sie Lambda und CodeBuild erstellen einen Jobworker, der Jobanfragen CodePipeline für die benutzerdefinierte Aktion abfragt, den Job ausführt und das Statusergebnis CodePipeline zurückgibt. Erstellen Sie eine Lambda-Funktion, die durch eine Amazon CloudWatch Events-Regel initiiert wird, wenn die benutzerdefinierte Quellaktionsphase der Pipeline zu „In Bearbeitung“ übergeht. Wenn die Lambda-Funktion initiiert wird, sollte sie die Auftragsdetails der benutzerdefinierten Aktion abrufen, indem sie nach Jobs abfragt. Sie können die PollForJobs API verwenden, um diese Informationen zurückzugeben. Nachdem die abgefragten Auftragsinformationen abgerufen wurden, sollte die Lambda-Funktion eine Bestätigung zurückgeben und die Informationen dann mit den Daten verarbeiten, die sie aus den Konfigurationseigenschaften für die benutzerdefinierte Aktion erhält. Wenn der Worker bereit	Allgemein AWS, Code-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist, mit dem Git-Repository zu kommunizieren, können Sie ein CodeBuild Projekt initiiere n, da es praktisch ist, Git-Aufgaben mithilfe des SSH-Clients zu erledigen.	

Erstellen Sie ein Ereignis in CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudWatch Ereignisregel.	Erstellen Sie eine CloudWatch Ereignisregel, die die Lambda-Funktion als Ziel initiiert, wenn die benutzerdefinierte Aktionsphase der Pipeline zu „In Bearbeitung“ übergeht.	Allgemeines AWS

Zugehörige Ressourcen

Erstellen einer benutzerdefinierten Aktion in CodePipeline

- Erstellen Sie eine benutzerdefinierte Aktion und fügen Sie sie hinzu in CodePipeline
- AWS::CodePipeline::CustomActionGeben Sie Ressource ein

Authentifizierung einrichten

- Secrets mit AWS Secrets Manager erstellen und verwalten

Eine Pipeline und einen Webhook erstellen

- Erstellen Sie eine Pipeline in CodePipeline
- Put-Webhook-Befehlsreferenz

- AWS::CodePipeline::Webhook Ressource
- PollForJobs API-Referenz
- Erstellen und fügen Sie eine benutzerdefinierte Aktion hinzu in CodePipeline
- Erstellen Sie ein Build-Projekt in AWS CodeBuild

Ein Ereignis erstellen

- Mit Amazon CloudWatch Events können Sie Änderungen im Pipeline-Status erkennen und darauf reagieren

Zusätzliche Referenzen

- Arbeiten mit Pipelines in CodePipeline
- AWS Lambda Lambda-Entwicklerhandbuch

Erstellen einer CI/CD-Pipeline zur Validierung von Terraform-Konfigurationen mithilfe von AWS CodePipeline

Erstellt vonl Raj Jayarajan (AWS) und Vijesh Vijayakumaran Nair (AWS)

Code-Repository: aws-codepipeline-terraform-cicd-samples	Umgebung: PoC oder Pilotprojekt	Technologien: DevOps
Workload: Alle anderen Workloads	AWS-Services: AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; Amazon S3; AWS Identity and Access Management	

Übersicht

Dieses Muster zeigt, wie HashiCorp Terraform-Konfigurationen mithilfe einer Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) getestet werden, die von AWS bereitgestellt wird CodePipeline.

Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können. Die in diesem Muster bereitgestellte Lösung erstellt eine CI/CD-Pipeline, mit der Sie die Integrität Ihrer Terraform-Konfigurationen überprüfen können, indem Sie fünf CodePipeline Phasen ausführen:

1. `“checkout”` ruft die Terraform-Konfiguration, die Sie testen, aus einem AWS- CodeCommit Repository ab.
2. `“validate”` führt infrastructure-as-cod (IaC)-Validierungstools aus, einschließlich tfsec ,TFLint und Checkov. Die -Phase führt auch die folgenden TerraformIaCValidierungsbefehle aus: `terraform validate` und `terraform fmt`.
3. `“plan”` zeigt, welche Änderungen auf die Infrastruktur angewendet werden, wenn die Terraform-Konfiguration angewendet wird.
4. `“apply”` verwendet den generierten Plan, um die erforderliche Infrastruktur in einer Testumgebung bereitzustellen.
5. `“destroy”` entfernt die Testinfrastruktur, die während der -`“apply”`Phase erstellt wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Git , auf Ihrem lokalen Computer installiert und konfiguriert
- Terraform , auf Ihrem lokalen Computer installiert und konfiguriert

Einschränkungen

- Der Ansatz dieses Musters stellt AWS nur CodePipeline in einem AWS-Konto und einer AWS-Region bereit. Konfigurationsänderungen sind für Bereitstellungen mit mehreren Konten und Regionen erforderlich.
- Die AWS Identity and Access Management (IAM)-Rolle, die dieses Muster bereitstellt (codepipeline_iam_role), folgt dem Prinzip der geringsten Berechtigung. Die Berechtigungen dieser IAM-Rolle müssen basierend auf den spezifischen Ressourcen aktualisiert werden, die Ihre Pipeline erstellen muss.

Produktversionen

- AWS CLI Version 2.9.15 oder höher
- Terraform Version 1.3.7 oder höher

Architektur

Zieltechnologie-Stack

- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- AWS IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS)

- Terraform

Zielarchitektur

Das folgende Diagramm zeigt ein Beispiel für einen CI/CD-Pipeline-Workflow zum Testen von Terraform-Konfigurationen in CodePipeline.

Das Diagramm zeigt den folgenden Workflow:

1. In initiiert ein AWS-Benutzer die in einem Terraform-Plan vorgeschlagenen Aktionen CodePipeline, indem er den `terraform apply` Befehl in der AWS CLI ausführt.
2. AWS CodePipeline übernimmt eine IAM-Servicerolle, die die für den Zugriff auf CodeCommit, CodeBuild, AWS KMS und Amazon S3 erforderlichen Richtlinien enthält.
3. CodePipeline führt die `“checkout”` Pipeline-Stufe aus, um die Terraform-Konfiguration zum Testen aus einem AWS- CodeCommit Repository abzurufen.
4. CodePipeline führt die -`“validate”`Stufe aus, um die Terraform-Konfiguration zu testen, indem IaC-Validierungstools und Terraform-IaC-Validierungsbefehle in einem CodeBuild Projekt ausgeführt werden.
5. CodePipeline führt die `“plan”` Stufe aus, um einen Plan im CodeBuild Projekt basierend auf der Terraform-Konfiguration zu erstellen. Der AWS-Benutzer kann diesen Plan überprüfen, bevor die Änderungen auf die Testumgebung angewendet werden.
6. Code Pipeline führt die -`“apply”`Phase aus, um den Plan zu implementieren, indem es das - CodeBuild Projekt verwendet, um die erforderliche Infrastruktur in der Testumgebung bereitzustellen.
7. CodePipeline führt die -`“destroy”`Phase aus, die verwendet, CodeBuild um die Testinfrastruktur zu entfernen, die während der -`“apply”`Phase erstellt wurde.
8. Ein Amazon S3-Bucket speichert Pipeline-Artefakte, die mit einem vom Kunden verwalteten AWS KMS-Schlüssel verschlüsselt und entschlüsselt werden.

Tools

Tools

AWS-Services

- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere -Services

- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.

Code

Der Code für dieses Muster ist im GitHub aws-codepipeline-terraform-cicdsamplesRepository verfügbar. Das Repository enthält die Terraform-Konfigurationen, die zum Erstellen der in diesem Muster beschriebenen Zielarchitektur erforderlich sind.

Polen

Bereitstellen der Lösungskomponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das GitHubaws-codepipeline-terraform-cicdsamplesRepository, indem Sie den folgenden Befehl	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/aws-codepipeline-terraform-cicd-samples.git` Weitere Informationen finden Sie unter Klonen eines Repositorys in der - GitHub Dokumentation.	
Erstellen Sie eine Terraform-Variablendefinitionsdatei.	Erstellen Sie eine `-terraform.tfvars` Datei basierend auf Ihren Anwendungsfallanforderungen. Sie können die Variablen in der `examples/terraform.tfvars` Datei aktualisieren, die sich im geklonten Repository befindet. Weitere Informationen finden Sie unter Zuweisen von Werten zu Root-Modulvariablen in der Terraform-Dokumentation. Hinweis: Die `Readme.md` Datei des Repositorys enthält weitere Informationen zu den erforderlichen Variablen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS als Terraform-Anbieter.	1. Öffnen Sie in einem Code-Editor die `main.tf` Datei des geklonten Repositorys. 2. Fügen Sie die erforderl ichen Konfigurationen zum Herstellen einer Verbindung zum AWS-Zielkonto hinzu. Weitere Informationen finden Sie unter AWS-Anbieter in der Terraform-Dokumentation.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Terraform-Anbieterkonfiguration zum Erstellen des Amazon S3-Replikations-Buckets.	1. Öffnen Sie das `S3` Verzeichnis des Repositorys, indem Sie den folgenden Befehl ausführen: `cd ./modules/s3` 2. Aktualisieren Sie die Terraform-Anbieterkonfiguration zum Erstellen des Amazon S3-Replikations-Buckets, indem Sie den `region` Wert in der `tf` Datei aktualisieren. Stellen Sie sicher, dass Sie die Region eingeben, in die Amazon S3 Objekte replizieren soll. 3. (Optional) Standardmäßig verwendet Terraform lokale Statusdateien für die Statusverwaltung. Wenn Sie Amazon S3 als Remote-Backend hinzufügen möchten, müssen Sie die Terraform-Konfiguration aktualisieren. Weitere Informationen finden Sie unter Backend-Konfiguration in der Terraform-Dokumentation. Hinweis: Die Replikation aktiviert automatisches,	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	asynchrones Kopieren von Objekten über Amazon S3-Buckets hinweg.	
Initialisieren Sie die Terraform-Konfiguration.	Um Ihr Arbeitsverzeichnis zu initialisieren, das die Terraform -Konfigurationsdateien enthält, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform init`	DevOps Techniker
Erstellen Sie den Terraform-Plan.	Um einen Terraform-Plan zu erstellen, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform plan --var-file=terraform.tfvars -out=tfplan` Hinweis: Terraform wertet die Konfigurationsdateien aus, um den Zielstatus für die deklarierten Ressourcen zu bestimmen. Anschließend wird der Zielstatus mit dem aktuellen Status verglichen und ein Plan erstellt.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Terraform -Plan.	Überprüfen Sie den Terraform -Plan und bestätigen Sie, dass er die erforderliche Architekt ur in Ihrem AWS-Zielkonto konfiguriert.	DevOps Techniker
Stellen Sie die Lösung bereit.	1. Um den Terraform-Plan anzuwenden, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform apply "tfplan"` 2. Geben Sie Ja ein, um zu bestätigen, dass Sie die Ressourcen bereitstellen möchten. Hinweis: Terraform erstellt, aktualisiert oder zerstört Infrastrukturen, um den in den Konfigurationsdateien deklarierten Zielstatus zu erreichen.	DevOps Techniker

Validieren von Terraform-Konfigurationen durch Ausführen der Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Quellcode-Repository ein.	1. Rufen Sie aus der Terraform-Ausgabe die Quell-Repository-Details für das Repository ab, das die	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Terraform-Konfigurationen enthält, die Sie validieren möchten. 2. Melden Sie sich bei der AWS-Managementkonsole an. Öffnen Sie dann die CodeCommit Konsole . 3. Erstellen Sie eine neue Verzweigung im Quell-Repository mit dem Namen `main`. Anweisungen finden Sie unter Erstellen einer Verzweigung in AWS CodeCommit in der - CodeCommit Dokumentation. 4. Klonen Sie den `main` Zweig des Quell-Repositorys auf Ihre lokale Workstation. Anweisungen finden Sie unter Einrichtungsschritte für HTTPS-Verbindungen zu AWS CodeCommit -Repositorys unter Windows mit dem AWS CLI Credential Helper in der - CodeCommit Dokumentation. 5. Kopieren Sie den `templates` Ordner aus dem GitHubaws-codepipeline-terraform-cicdsamplesRepository, indem Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den folgenden Befehl ausführen: `cp -r templates $YOUR_CODECOMMIT_REPO_ROOT` Hinweis: Der `templates` Ordner enthält die Build-Spezifikationsdateien und das Validierungsskript für das Stammverzeichnis des Quell-Repositorys. 6. Fügen Sie Ihre erforderlichen Terraform-IaC-Konfigurationen zum Stammordner des Quell-Repositorys hinzu. 7. Fügen Sie die Details für das Remote-Backend in der Terraform-Konfiguration Ihres Projekts hinzu. Weitere Informationen finden Sie unter S3 in der Terraform-Dokumentation. 8. (Optional) Aktualisieren Sie die Variablen im `templates` Ordner , um die vorkonfigurierten Scans, Versionen von Tooländerungen und Ihr Verzeichnis in benutzerdefinierten Skriptdateien zu aktivieren oder zu deaktivieren. Weitere Informationen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie im Abschnitt Zusätzliche Informationen dieses Musters. 9. Übertragen Sie die Änderungen in den `main` Zweig des Quell-Rep ositorys .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Pipeline-Phasen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CodePipeline -Konsole. 2. Suchen Sie in der Ausgabe, die mit dem `terraform apply "tfplan"` Befehl im vorherigen Epic-Abschnitt generiert wurde, den Namen des generierten CodePipeline. 3. Öffnen Sie die Pipeline in der - CodePipeline Konsole und wählen Sie Release change aus. 4. Überprüfen Sie jede Pipeline-Phase und bestätigen Sie, dass sie wie erwartet funktioniert. Weitere Informationen finden Sie unter Anzeigen von Pipeline-Details und -Verlauf (Konsole) im AWS- CodePipeline Benutzerhandbuch. Wichtig: Wenn eine Änderung an den Hauptzweig des Quell-Repositorys übergeben wird, wird die Testpipeline automatisch aktiviert.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Berichtsausgabe.	1. Wählen Sie im linken Navigationsbereich der CodePipeline Konsole die Option Erstellen aus. Wählen Sie dann Berichtsverlauf aus. 2. Überprüfen Sie die tfsec- und Checkov-Scan-Berichte, die die Pipeline generiert. Diese Berichte können Ihnen helfen, Probleme durch Visualisierungen und grafische Darstellungen zu identifizieren. Hinweis: Das `<project_name>-validate` CodeBuild Projekt generiert während der -“`validate`” Phase Schwachstellenberichte für Ihren Code.	DevOps Techniker

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Pipeline und die zugehörigen Ressourcen.	Um die Testressourcen aus Ihrem AWS-Konto zu löschen, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus:	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform destroy --var-file=terraform.tfvars`	

Fehlerbehebung

Problem	Lösung
Sie erhalten während der -`"apply"`Phase eine AccessDenied Fehlermeldung.	1. Überprüfen Sie die Ausführungsprotokolle des CodeBuild Projekts, das der `"apply"` Stufe zugeordnet ist, um fehlende IAM-Berechtigungen zu identifizieren. Weitere Informationen finden Sie unter Anzeigen von Build-Details in AWS CodeBuild im AWS-CodeBuild Benutzerhandbuch. 2. Öffnen Sie in einem Code-Editor den `modules` Ordner des geklonten Repositorys. Navigieren Sie dann zum `iam-role` Ordner und öffnen Sie die `main.tf` Datei, die sich in diesem Ordner befindet. 3. Fügen Sie der `codepipeline_policy` Anweisung die IAM-Richtlinien hinzu, die für die Bereitstellung von Ressourcen in Ihrem AWS-Konto erforderlich sind.

Zugehörige Ressourcen

- Modulblöcke (Terraform-Dokumentation)
- So verwenden Sie CI/CD zum Bereitstellen und Konfigurieren von AWS-Sicherheitsservices mit Terraform (AWS-Blogbeitrag)
- Verwenden von serviceverknüpften Rollen (IAM-Dokumentation)
- create-pipeline (AWS-CLI-Dokumentation)

- Konfigurieren der serverseitigen Verschlüsselung für Artefakte, die in Amazon S3 für gespeichert CodePipeline sind (AWS- CodePipeline Dokumentation)
- Kontingente für AWS CodeBuild (AWS- CodeBuild Dokumentation)
- Datenschutz in AWS CodePipeline (AWS- CodePipeline Dokumentation)

Zusätzliche Informationen

Benutzerdefinierte Terraform-Module

Im Folgenden finden Sie eine Liste von benutzerdefinierten Terraform-Modulen, die in diesem Muster verwendet werden:

- `codebuild_terraform` erstellt die CodeBuild Projekte, die jede Phase der Pipeline bilden.
- `codecommit_infrastructure_source_repo` erfasst und erstellt das Quell- CodeCommit Repository.
- `codepipeline_iam_role` erstellt die erforderlichen IAM-Rollen für die Pipeline.
- `codepipeline_kms` erstellt den erforderlichen AWS KMS-Schlüssel für die Verschlüsselung und Entschlüsselung von Amazon S3-Objekten.
- `codepipeline_terraform` erstellt die Testpipeline für das Quell- CodeCommit Repository.
- `s3_artifacts_bucket` erstellt einen Amazon S3-Bucket zum Verwalten von Pipeline-Artefakten.

Build-Spezifikationsdateien

Im Folgenden finden Sie eine Liste von Build-Spezifikationsdateien (buildspec), die dieses Muster verwendet, um jede Pipeline-Phase auszuführen:

- `buildspec_validate.yml` führt die -`“validate”`Stufe aus.
- `buildspec_plan.yml` führt die -`“plan”`Stufe aus.
- `buildspec_apply.yml` führt die -`“apply”`Stufe aus.
- `buildspec_destroy.yml` führt die -`“destroy”`Stufe aus.

Dateivariablen der Build-Spezifikation

Jede buildspec-Datei verwendet die folgenden Variablen, um verschiedene buildspezifische Einstellungen zu aktivieren:

Variable	Standardwert	Beschreibung
CODE_SRC_DIR	"."	Definiert das CodeCommit Quellverzeichnis
TF_VERSION	„1.3.7“	Definiert die Terraform-Version für die Build-Umgebung

Die buildspec_validate.yml Datei unterstützt auch die folgenden Variablen, um verschiedene Build-spezifische Einstellungen zu aktivieren:

Variable	Standardwert	Beschreibung
SCRIPT_DIR	„./templates/scripts“	Definiert das Skriptverzeichnis
ENVIRONMENT	„Entwicklung“	Definiert den Umgebungs namen
SKIPVALIDATIONFAIL URE	„Y“	Überspringt die Validierung bei Fehlern
ENABLE_TFVALIDATE	„Y“	Aktiviert die Terraform-Validier ung
ENABLE_TFFORMAT	„Y“	Aktiviert das Terraform-Format
ENABLE_TFCHECKOV	„Y“	Aktiviert den Checkov-Scan
ENABLE_TFSEC	„Y“	Aktiviert den tfsec-Scan
TFSEC_VERSION	„v1.28.1“	Definiert die tfsec-Version

Mehr Muster

- ???
- Zuordnen eines AWS- CodeCommit Repositorys in einem AWS-Konto zu SageMaker Studio in einem anderen Konto
- Automatisieren des Hinzufügens oder Aktualisierens von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie das Training und die Bereitstellung von Amazon Lookout for Vision zur Erkennung von Anomalien
- Automatisieren von Backups für Amazon RDS for PostgreSQL-DB-Instances mithilfe von AWS Batch
- Automatisieren der Bereitstellung verschachtelter Anwendungen mit AWS SAM
- Automatisieren der Bereitstellung des Node Termination Handler in Amazon EKS mithilfe einer CI/CD-Pipeline
- ???
- Automatisieren der Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation
- Automatisieren der Replikation von Amazon RDS-Instances über AWS-Konten hinweg
- Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisches Generieren eines PynamoDB-Modells und von CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung
- Automatische Validierung und Bereitstellung von IAM-Richtlinien und -Rollen in einem AWS-Konto mithilfe von CodePipeline, IAM Access Analyzer und AWS- CloudFormation Makros
- Sichern von SunSpeedRC-Servern im Stromasys Charon-SSP-Emulator in der AWS Cloud
- Erstellen einer Datenpipeline zur Aufnahme, Transformation und Analyse von Google Analytics-Daten mit dem AWS DataOps Development Kit
- Erstellen Sie einen Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Erstellen einer Pipeline für gehärtete Container-Images mit EC2 Image Builder und Terraform
- Erstellen Sie einen MLOps-Workflow mithilfe von Amazon SageMaker und Azure DevOps
- ???
- Verketten von AWS-Services mithilfe eines Serverless-Ansatzes

- Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog
- Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit
- Erstellen Sie ein benutzerdefiniertes Docker-Container-Image für SageMaker und verwenden Sie es für Modelltrainings in AWS Step Functions
- Erstellen einer Pipeline in AWS-Regionen, die AWS nicht unterstützen CodePipeline
- Erstellen von Alarmen für benutzerdefinierte Metriken mithilfe der Amazon CloudWatch - Anomalieerkennung
- Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme in mehreren Codeergebnissen gleichzeitig erkennt
- Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden
- Stellen Sie Kubernetes-Ressourcen und -Pakete mithilfe von Amazon EKS und einem Helm-Chart-Repository in Amazon S3 bereit
- Bereitstellen von Multi-Stack-Anwendungen mit AWS CDK mit TypeScript
- Stellen Sie die Lösung Security Automations für AWS WAF mithilfe von Terraform bereit
- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct
- ???
- Generieren Sie personalisierte und neu eingestufte Empfehlungen mit Amazon Personalize
- Amazon SNS-Benachrichtigungen abrufen, wenn sich der Schlüsselstatus eines AWS KMS-Schlüssels ändert
- Verbessern Sie die betriebliche Leistung, indem Sie Amazon DevOps Guru über mehrere AWS-Regionen, Konten und OUs hinweg mit dem AWS-CDK aktivieren
- Installieren des SSM-Agenten auf Amazon-EKS-Worker-Knoten mithilfe von Kubernetes DaemonSet
- Integrieren Sie Stonebranch Universal Controller in AWS Mainframe Modernization
- Mainframe-Modernisierung: DevOps auf AWS mit Micro Focus
- Verwalten von AWS IAM Identity Center-Berechtigungssätzen als Code mithilfe von AWS CodePipeline
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten

- Migrieren Sie DNS-Datensätze in großen Mengen in eine privat gehostete Zone von Amazon Route 53
- Migrieren von ML Build, Training und Bereitstellung von Workloads zu Amazon SageMaker mithilfe von AWS-Entwicklertools
- Überwachen der Verwendung eines freigegebenen Amazon Machine Image über mehrere AWS-Konten hinweg
- Von AWS App2Container generierte Docker-Images optimieren
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- Aufbewahren von routbarem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze, die keine Workload sind
- Bereitstellen eines Terraform-Produkts in AWS Service Catalog mithilfe eines Code-Repositorys
- ???
- Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern
- Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus
- Einrichten einer CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere mithilfe von AWS CDK und GitLab
- Einrichten einer Multi-AZ-Infrastruktur für eine SQL Server Always On FCI mithilfe von Amazon FSx
- Automatisches Einrichten von UiPath Bol-Bots auf Amazon EC2 mithilfe von AWS CloudFormation
- Mandanten-Onboarding in SaaS-Architektur für das Silomodell mit C# und AWS CDK
- Verwenden von Terraform zum automatischen Aktivieren von Amazon GuardDuty für eine Organisation
- Lokales Validieren des Codes Account Factory für Terraform (AFT)
- ???

Datenverarbeitung für Endbenutzer

Themen

Automatisieren der Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation

Erstellt von Ram Kandaswamy (AWS) und Dzung Nguyen (AWS)

Umgebung: Produktion	Technologien: Endbenutzer-Computing; Cloudnativ; Kostenmanagement DevOps; SaaS	Workload: Microsoft
AWS-Services: Amazon AppStream 2.0; AWS CloudFormation		

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zur Automatisierung der Erstellung von Amazon AppStream 2.0-Ressourcen in der Amazon Web Services (AWS) Cloud mithilfe einer AWS-CloudFormation Vorlage. Das Muster zeigt Ihnen, wie Sie einen AWS- CloudFormation Stack verwenden, um die Erstellung Ihrer AppStream 2.0-Anwendungsressourcen zu automatisieren, einschließlich Image Builder, Image, Flotten-Instance und Stack. Sie können Ihre AppStream 2.0-Anwendung an Endbenutzer in einem HTML5-compliant Browser streamen, indem Sie entweder den Desktop- oder den Anwendungsbereitstellungsmodus verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Annahme der Allgemeinen Geschäftsbedingungen von AppStream 2.0
- Grundlegendes Wissen über - AppStream Ressourcen wie Stacks, Flotten und Image Builder

Einschränkungen

- Sie können die AWS Identity and Access Management (IAM)-Rolle, die einer AppStream 2.0-Instance zugeordnet ist, nicht ändern, nachdem diese Instance erstellt wurde.

- Sie können Eigenschaften (z. B. das Subnetz oder die Sicherheitsgruppe) auf der AppStream 2.0-Image-Builder-Instance nicht ändern, nachdem dieser Image Builder erstellt wurde.

Architektur

Das folgende Diagramm zeigt Ihnen, wie Sie die Erstellung von AppStream 2.0-Ressourcen mithilfe einer AWS- CloudFormation Vorlage automatisieren können.

Das Diagramm zeigt den folgenden Workflow:

1. Sie erstellen eine AWS- CloudFormation Vorlage basierend auf dem YAML-Code im Abschnitt Zusätzliche Informationen dieses Musters.
2. Die AWS- CloudFormation Vorlage erstellt einen AWS- CloudFormation Test-Stack.
   a. (Optional) Sie erstellen eine Image Builder-Instance mit AppStream 2.0.
   b. (Optional) Sie erstellen ein Windows-Image mit Ihrer benutzerdefinierten Software.
3. Der AWS- CloudFormation Stack erstellt eine AppStream 2.0-Flotten-Instance und einen Stack.
4. Sie stellen Ihre AppStream 2.0-Ressourcen für Endbenutzer in einem HTML5-compliant Browser bereit.

Technologie-Stack

- Amazon AppStream 2.0
- AWS CloudFormation

Tools

- Amazon AppStream 2.0 – Amazon AppStream 2.0 ist ein vollständig verwalteter Anwendungs-Streaming-Service, der Ihnen sofortigen Zugriff auf Ihre Desktop-Anwendungen von überall aus ermöglicht. AppStream 2.0 verwaltet die AWS-Ressourcen, die zum Hosten und Ausführen Ihrer Anwendungen erforderlich sind, skaliert automatisch und bietet Ihren Benutzern On-Demand-Zugriff.
- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre

Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.

Polen

(Optional) Erstellen eines AppStream 2.0-Images

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie benutzerdefinierte Software und erstellen Sie ein Image.	1. Installieren Sie die AppStream 2.0-Anwendung, die Sie für Ihre Benutzer bereitstellen möchten. 2. Verwenden Sie den -Foton-Create-Image-Agenten oder ein PowerShell Skript, um ein neues Windows-Image für Ihre benutzerdefinierte Software zu erstellen. Hinweis: Erwägen Sie, das Windows- AppLocker Feature zu verwenden, um das Image weiter zu sperren.	AWS DevOps, Cloud-Architekt

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die AWS-CloudFormation Vorlage.	1. Speichern Sie den Code im Abschnitt Zusätzliche Informationen dieses Musters als YAML-Datei.	AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, Allgemeine AWS, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Aktualisieren Sie die YAML-Datei mit den erforderlichen Werten für die Parameter in Ihrer Umgebung.	
Erstellen Sie einen AWS-CloudFormation Stack mithilfe der Vorlage.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-CloudFormation Konsole . 2. Wählen Sie im Navigationsbereich Stacks aus. 3. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 4. Wählen Sie im Abschnitt Voraussetzung – Vorlage vorbereiten die Option Vorlage ist bereit aus. 5. Wählen Sie im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen aus. 6. Wählen Sie Datei auswählen und dann Ihre aktualisierte AWS-CloudFormation Vorlage aus. 7. Führen Sie die restlichen Schritte im Assistenten aus, um Ihren Stack zu erstellen.	App-Eigentümer, AWS-Systemadministrator, Windows-Techniker

Zugehörige Ressourcen

Referenzen

- Erste Schritte mit Amazon AppStream 2.0: Einrichten mit Beispielanwendungen
- Erstellen einer AppStream 2.0-Flotte und eines Stacks

Tutorials und Videos

- Amazon- AppStream 2.0-Benutzer-Workflow
- So migrieren Sie eine Legacy-Windows-Format-App zu Amazon AppStream 2.0
- AWS re:Invent 2018: Sichere Bereitstellung von Desktop-Anwendungen mit Amazon AppStream 2.0 (BAP201)

Zusätzliche Informationen

Der folgende Code ist ein Beispiel für eine AWS- CloudFormation Vorlage, mit der Sie automatisch AppStream 2.0-Ressourcen erstellen können.

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  SubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
  testSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup::Id'
  ImageName:
    Type: String
Resources:

  AppStreamFleet:
    Type: 'AWS::AppStream::Fleet'
    Properties:
      ComputeCapacity:
        DesiredInstances: 5
      InstanceType: stream.standard.medium
      Name: appstream-test-fleet
      DisconnectTimeoutInSeconds: 1200
      FleetType: ON_DEMAND
      IdleDisconnectTimeoutInSeconds: 1200
      ImageName: !Ref ImageName
```

```
      MaxUserDurationInSeconds: 345600
      VpcConfig:
        SecurityGroupIds:
          - !Ref testSecurityGroup
        SubnetIds: !Ref SubnetIds
  AppStreamStack:
    Type: 'AWS::AppStream::Stack'
    Properties:
      Description: AppStream stack for test
      DisplayName: AppStream test Stack
      Name: appstream-test-stack
      StorageConnectors:
        - ConnectorType: HOMEFOLDERS
      UserSettings:
        - Action: CLIPBOARD_COPY_FROM_LOCAL_DEVICE
          Permission: ENABLED
        - Action: CLIPBOARD_COPY_TO_LOCAL_DEVICE
          Permission: ENABLED
        - Action: FILE_DOWNLOAD
          Permission: ENABLED
        - Action: PRINTING_TO_LOCAL_DEVICE
          Permission: ENABLED
  AppStreamFleetAssociation:
    Type: 'AWS::AppStream::StackFleetAssociation'
    Properties:
      FleetName: appstream-test-fleet
      StackName: appstream-test-stack
    DependsOn:
      - AppStreamFleet
      - AppStreamStack
```

Mehr Muster

- Herstellen einer Verbindung mit einer Amazon EC2-Instance mithilfe von Session Manager
- Verbessern Sie die Anrufqualität auf den Workstations von Kundendienstmitarbeitern in Amazon Connect-Kontaktzentren
- Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus

Datenverarbeitung in Hochleistung

Themen

Einrichten eines Grafana-Überwachungs-Dashboards für AWS ParallelCluster

Erstellt von Dario La Porta (AWS) und Bol Lu (AWS)

Code-Repository: parallelcluster-monitoring-dashboard	Umgebung: PoC oder Pilotprojekt	Technologien: Hochleistungs-Computing; Analytik; Management und Governance
Workload: Open-Source	AWS-Services: AWS ParallelCluster	

Übersicht

AWS ParallelCluster unterstützt Sie bei der Bereitstellung und Verwaltung von High Performance Computing (HPC)-Clustern. Es unterstützt AWS Batch- und Slurm-Open-Source-Auftragsplaner. Obwohl AWS CloudWatch für die Protokollierung und Metriken in Amazon integriert ParallelCluster ist, bietet es kein Überwachungs-Dashboard für den Workload.

Das Grafana-Dashboard für AWS ParallelCluster (GitHub) ist ein Überwachungs-Dashboard für AWS ParallelCluster. Es bietet Einblicke in den Auftrags-Scheduler und detaillierte Überwachungsmetriken auf Betriebssystemebene (OS). Weitere Informationen zu den in dieser Lösung enthaltenen Dashboards finden Sie unter Beispiel-Dashboards im GitHub -Repository. Diese Metriken helfen Ihnen, den HPC-Workload und seine Leistung besser zu verstehen. Der Dashboard-Code wird jedoch nicht für die neuesten Versionen von AWS ParallelCluster oder die Open-Source-Pakete aktualisiert, die in der Lösung verwendet werden. Dieses Muster verbessert die Lösung, um die folgenden Vorteile zu bieten:

- Unterstützt AWS ParallelCluster v3
- Verwendet die neueste Version von Open-Source-Paketen, einschließlich Prometheus, Grafana, Prometheus Slurm Exporter und NVIDIA DC-Exporter
- Erhöht die Anzahl der CPU-Kerne und GPUs, die die Slurm-Aufträge verwenden
- Fügt ein Dashboard zur Auftragsüberwachung hinzu
- Verbessert das Dashboard zur Überwachung von GPU-Knoten für Knoten mit 4 oder 8 Grafikverarbeitungseinheiten (GPUs)

Diese Version der erweiterten Lösung wurde in der HPC-Produktionsumgebung eines AWS-Kunden implementiert und verifiziert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS ParallelCluster CLI , installiert und konfiguriert.
- Eine unterstützte Netzwerkkonfiguration für AWS ParallelCluster. Dieses Muster verwendet die AWS- ParallelCluster Konfiguration mit zwei Subnetzen, die ein öffentliches Subnetz, ein privates Subnetz, ein Internet-Gateway und ein NAT-Gateway erfordert.
- Alle AWS ParallelCluster -Cluster-Knoten müssen über Internetzugang verfügen. Dies ist erforderlich, damit die Installationsskripts die Open-Source-Software und Docker-Images herunterladen können.
- Ein Schlüsselpaar in Amazon Elastic Compute Cloud (Amazon EC2). Ressourcen mit diesem Schlüsselpaar haben Secure Shell (SSH)-Zugriff auf den Hauptknoten.

Einschränkungen

- Dieses Muster wurde für die Unterstützung von Ubuntu 20.04 LTS entwickelt. Wenn Sie eine andere Version von Ubuntu verwenden oder Amazon Linux oder CentOS verwenden, müssen Sie die mit dieser Lösung bereitgestellten Skripts ändern. Diese Änderungen sind nicht in diesem Muster enthalten.

Produktversionen

- Ubuntu 20.04 LTS
- ParallelCluster 3.X

Überlegungen zu Fakturierung und Kosten

- Die in diesem Muster bereitgestellte Lösung wird nicht vom kostenlosen Kontingent abgedeckt. Für Amazon EC2, Amazon FSx for Lustre, das NAT-Gateway in Amazon VPC und Amazon Route 53 fallen Gebühren an.

Architektur

Zielarchitektur

Das folgende Diagramm zeigt, wie ein Benutzer auf das Überwachungs-Dashboard für AWS ParallelCluster auf dem Hauptknoten zugreifen kann. Auf dem Hauptknoten werden NICE DCV, Prometheus, Grafana, Prometheus Slurm Exporter, Prometheus Node Exporter und NGINX Open Source ausgeführt. Auf den Datenverarbeitungsknoten wird der Prometheus Node Exporter und auch NVIDIA DC-Exporter ausgeführt, wenn der Knoten GPUs enthält. Der Hauptknoten ruft Informationen von den Datenverarbeitungsknoten ab und zeigt diese Daten im Grafana-Dashboard an.

In den meisten Fällen ist der Hauptknoten nicht stark ausgelastet, da der Auftrags-Scheduler keine erhebliche Menge an CPU oder Arbeitsspeicher benötigt. Benutzer greifen über SSL auf Port 443 auf das Dashboard auf dem Hauptknoten zu.

Alle autorisierten Viewer können die Überwachungs-Dashboards anonym anzeigen. Nur der Grafana-Administrator kann Dashboards ändern. Sie konfigurieren ein Passwort für den Grafana-Administrator in der `-aws-parallelcluster-monitoring/docker-compose/docker-compose.head.yml`Datei.

Tools

AWS-Services

- NICE DCV ist ein leistungsstarkes Remote-Anzeigeprotokoll, mit dem Sie Remote-Desktops und Anwendungs-Streaming von jeder Cloud oder jedem Rechenzentrum an jedes Gerät unter unterschiedlichen Netzwerkbedingungen bereitstellen können.
- AWS ParallelCluster unterstützt Sie bei der Bereitstellung und Verwaltung von High Performance Computing (HPC)-Clustern. Es unterstützt AWS Batch- und Slurm-Open-Source-Auftragsplaner.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.

Andere Tools

- Docker ist eine Reihe von Platform as a Service (PaaS)-Produkten, die Virtualisierung auf Betriebssystemebene verwenden, um Software in Containern bereitzustellen.
- Grafana ist eine Open-Source-Software, mit der Sie Metriken, Protokolle und Ablaufverfolgungen abfragen, visualisieren, warnen und untersuchen können.
- NGINX Open Source ist ein Open-Source-Webserver und Reverse-Proxy.
- NVIDIA Data Center GPU Manager (DCSpeed) ist eine Suite von Tools zur Verwaltung und Überwachung von NVIDIA-Rechenzentrum-Grafikverarbeitungseinheiten (GPUs) in Cluster-Umgebungen. In diesem Muster verwenden Sie DC-Exporter, mit dem Sie GPU-Metriken aus Prometheus exportieren können.
- Prometheus ist ein Open-Source-Toolkit zur Systemüberwachung, das seine Metriken als Zeitreihendaten mit zugehörigen Schlüssel-Wert-Paaren sammelt und speichert, die als Labels bezeichnet werden. In diesem Muster verwenden Sie auch Prometheus Slurm Exporter, um Metriken zu sammeln und zu exportieren, und Sie verwenden Prometheus Node Exporter, um Metriken aus den Datenverarbeitungsknoten zu exportieren.
- Ubuntu ist ein Open-Source-Linux-basiertes Betriebssystem, das für Unternehmensserver, Desktops, Cloud-Umgebungen und IoT entwickelt wurde.

Code-Repository

Der Code für dieses Muster ist im GitHub pcluster-monitoring-dashboardRepository verfügbar.

Polen

Erstellen der erforderlichen Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen Amazon-S3-Bucket. Sie verwenden diesen Bucket, um die Konfigurationsskripts zu speichern. Anweisungen finden Sie unter Erstellen eines Buckets in der Amazon S3-Dokumentation.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das GitHub pcluster-monitoring-dashboard Repo, indem Sie den folgenden Befehl ausführen. `git clone https://github.com/aws-samples/parallelcluster-monitoring-dashboard.git`	DevOps Techniker
Erstellen Sie ein Administratorpasswort.	1. Wählen Sie den `aws-parallelcluster-monitoring` Ordner aus, wählen Sie den `docker-compose` Ordner aus und öffnen Sie dann die Datei docker-compose.head.yml. 2. Ersetzen Sie in der `GF_SECURITY_ADMIN_PASSWORD` Variablen durch `Grafana4PC!` ein Passwort Ihrer Wahl. Dies ist das Administratorpasswort, mit dem Sie das Grafana-Konto verwalten. 3. Speichern und schließen Sie die Datei docker-compose.head.yml.	Linux-Shell-Skriptsprache

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die erforderlichen Dateien in den S3-Bucket.	Kopieren Sie das Skript post_install.sh und den aws-parallelcluster-monitoring Ordner in den von Ihnen erstellten S3-Bucket. Anweisungen finden Sie unter Hochladen von Objekten in der Amazon S3-Dokumentation.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine zusätzliche Sicherheitsgruppe für den Hauptknoten.	1. Erstellen Sie eine Sicherheitsgruppe für den Hauptknoten. Diese Sicherheitsgruppe erlaubt eingehenden Datenverkehr zu den Überwachungs-Dashboards auf dem Hauptknoten. Anweisungen finden Sie unter Erstellen einer Sicherheitsgruppe in der Amazon-VPC-Dokumentation. 2. Fügen Sie der Sicherheitsgruppe eine Regel für eingehenden Datenverkehr hinzu. Anweisungen finden Sie unter Hinzufügen von Regeln zu einer Sicherheitsgruppe in der Amazon-VPC-Dokumentation. Verwenden Sie die folgenden Parameter für die Regel: • Typ – HTTPS • Protokoll – TCP • Portbereich – 443 • Quelle – Geben Sie Ihre IP-Adresse ein • Beschreibung – Benutzern den Zugriff auf das Überwachungs-Dashboard erlauben	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine IAM-Richtlinie für den Hauptknoten.	Erstellen Sie eine identitätsbasierte Richtlinie für den Hauptknoten. Diese Richtlinie ermöglicht es dem Knoten, Metrikdaten von Amazon CloudWatch abzurufen. Das GitHub Repo enthält ein Beispiel für eine Richtlinie. Anweisungen finden Sie unter Erstellen von IAM-Richtlinien in der AWS Identity and Access Management (IAM)-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine IAM-Richtlinie für die Datenverarbeitungsknoten.	Erstellen Sie eine identitätsbasierte Richtlinie für die Datenverarbeitungsknoten. Diese Richtlinie ermöglicht es dem Knoten, die Tags zu erstellen, die die Auftrags-ID und den Auftragseigentümer enthalten. Das GitHub Repo enthält ein Beispiel für eine Richtlinie . Anweisungen finden Sie unter Erstellen von IAM-Richtlinien in der IAM-Dokumentation. Wenn Sie die bereitgestellte Beispieldatei verwenden, ersetzen Sie die folgenden Werte: • <REGION> – Die AWS-Region, in der der Cluster gehostet wird • <ACCOUNT_ID> – Die AWS-Konto-ID	AWS-Administrator

Den Cluster erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die bereitgestellte Cluster-Vorlagendatei.	Erstellen Sie den AWS-ParallelCluster Cluster. Verwenden Sie die bereitgestellte cluster.yaml-AWS-CloudFormation Vorlagendatei	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als Ausgangspunkt, um den Cluster zu erstellen. Ersetzen Sie die folgenden Werte in der bereitgestellten Vorlage: • <REGION> – Die AWS-Region, in der der Cluster gehostet wird. • <HEADNODE_SUBNET> – Das öffentliche Subnetz der VPC. • <ADDITIONAL_HEAD_NODE_SG> – Der Name der Sicherheitsgruppe, die Sie für den Hauptknoten erstellt haben. • <KEY_NAME> – Geben Sie den Namen eines vorhandenen Amazon EC2Schlüsselpaars ein. Ressourcen mit diesem Schlüsselpaar haben Secure Shell (SSH)-Zugriff auf den Hauptknoten. • <ALLOWED_IPS> – Geben Sie den CIDR-formatierten IP-Adressbereich ein, der SSH-Verbindungen zum Hauptknoten herstellen darf. • <ADDITIONAL_HEAD_NODE_POLICY> – Geben Sie den Namen der IAM-Richtlinie ein, die Sie für den Hauptknoten erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• <BUCKET_NAME> – Geben Sie den Namen des S3-Buckets ein, den Sie erstellt haben. • <COMPUTE_SUBNET> – Geben Sie den Namen des privaten Subnetzes in der VPC ein. • <ADDITIONAL_COMPUTE_NODE_POLICY> – Geben Sie den Namen der IAM-Richtlinie ein, die Sie für den Datenverarbeitungsknoten erstellt haben.	
Erstellen Sie den -Cluster.	Geben Sie in der AWS ParallelCluster CLI den folgenden Befehl ein. Dadurch wird die CloudFormation Vorlage bereitgestellt und der Cluster erstellt. Weitere Informationen zu diesem Befehl finden Sie unter pcluster create-cluster in der AWS- ParallelCluster Dokumentation. `pcluster create-cluster -n <cluster_name> -c cluster.yaml`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie die Cluster-Erstellung.	Geben Sie den folgenden Befehl ein, um die Clustererstellung zu überwachen. Weitere Informationen zu diesem Befehl finden Sie unter pcluster describe-cluster in der AWS- ParallelCluster Dokumentation. `pcluster describe-cluster -n <cluster_name>`	AWS-Administrator

Verwenden der Grafana-Dashboards

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zugriff auf das Grafana-Portal.	1. Geben Sie den folgenden Befehl ein, um die öffentliche IP-Adresse des Hauptknotens abzurufen. `pcluster describe-cluster -n <cluster_name> --query headNode.publicIpAddress` 2. Navigieren Sie in einem Webbrowser zur folgenden URL, um auf das Grafana-Dashboard zuzugreifen. https://<head_node_public_ip_address>	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie auf der Grafana-Frontseite das 4-Quader-Dashboard-Symbol im linken Menü und dann Allgemein aus. Dies zeigt eine Liste der konfigurierten Dashboards. Die folgenden Dashboards sind in Grafana verfügbar: • Cluster-Kosten – Enthält Informationen zu den Kosten des Clusters • Cluster-Protokolle – Enthält Informationen zu den Protokollen des Clusters • Details zu Datenverarbeitungsknoten – Enthält Informationen über Nutzungsstatistiken der Datenverarbeitungsknoten • Liste der Datenverarbeitungsknoten – Enthält die Liste der Datenverarbeitungsknoten des Clusters • GPU-Knoten – Enthält Informationen über Nutzungsstatistiken der GPU-Knoten • Auftragsdetails – Enthält Informationen zur	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Auslastung der Auftragsr essourcen • Details zum Hauptknoten – Enthält Informationen über Nutzungsstatistiken des Hauptknotens • ParallelCluster Zusammenfassung – Enthält Informationen zur Cluster-Nutzung	

Bereinigen Sie die Lösung, damit keine damit verbundenen Kosten anfallen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Cluster.	Geben Sie den folgenden Befehl ein, um den Cluster zu löschen. Weitere Informati onen zu diesem Befehl finden Sie unter pcluster delete-cl uster in der AWS- ParallelC luster Dokumentation. `pcluster delete-cluster -n <cluster_name>`	AWS-Administrator
Löschen Sie die IAM-Richt linien.	Löschen Sie die Richtlinien, die Sie für den Hauptknoten und den Datenverarbeitungs knoten erstellt haben. Weitere Informationen zum Löschen von Richtlinien finden Sie unter Löschen von IAM-Richt	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	linien in der IAM-Dokum entation.	
Löschen Sie die Sicherhei tsgruppe und die Regel.	Löschen Sie die Sicherhei tsgruppe, die Sie für den Hauptknoten erstellt haben. Weitere Informationen finden Sie unter Löschen von Sicherheitsgruppenregeln und Löschen einer Sicherhei tsgruppe in der Amazon-VPC-Dokumentation.	AWS-Administrator
Löschen Sie den S3-Bucket.	Löschen Sie den S3-Bucket , den Sie zum Speichern der Konfigurationsskripts erstellt haben. Weitere Informationen finden Sie unter Löschen eines Buckets in der Amazon S3-Dokumentation.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Auf den Hauptknoten kann im Browser nicht zugegriffen werden.	Überprüfen Sie die Sicherheitsgruppe und vergewissern Sie sich, dass der eingehende Port 443 geöffnet ist.
Grafana wird nicht geöffnet.	Überprüfen Sie auf dem Hauptknoten das Containerprotokoll auf `docker logs Grafana`.
Einige Metriken haben keine Daten.	Überprüfen Sie auf dem Hauptknoten die Containerprotokolle aller Container.

Zugehörige Ressourcen

AWS-Dokumentation

- IAM-Richtlinien für Amazon EC2

Andere AWS-Ressourcen

- AWS ParallelCluster
- Überwachung des Dashboards für AWS ParallelCluster (AWS-Blogbeitrag)

Sonstige Ressourcen

- Prometheus-Überwachungssystem
- Grafana

Einrichten einer virtuellen Desktop-Infrastruktur (VDI) mit Auto Scaling mithilfe von NICE EnginFrame und NICE DCV Session Manager

Erstellt von Dario La Porta und Salvatore Maccarone (AWS)

Code-Repository: elastic-vdi-infrastructure	Umgebung: PoC oder Pilotprojekt	Technologien: Hochleistungs-Computing; Infrastruktur
AWS-Services: AWS CDK; AWS CloudFormation; Amazon EC2 Auto Scaling ; Elastic Load Balancing (ELB)		

Übersicht

NICE DCV ist ein leistungsstarkes Remote-Anzeigeprotokoll, mit dem Sie Remote-Desktops und Anwendungen von jeder Cloud oder jedem Rechenzentrum über unterschiedliche Netzwerkbedingungen auf jedes Gerät streamen können. Mit NICE DCV und Amazon Elastic Compute Cloud (Amazon EC2) können Sie grafikintensive Anwendungen remote auf EC2-Instances ausführen und ihre Benutzeroberflächen auf einfachere Remote-Client-Computer streamen. Dadurch entfällt die Notwendigkeit teurer dedizierter Workstations und die Notwendigkeit, große Datenmengen zwischen der Cloud und Client-Computern zu übertragen.

Dieses Muster richtet eine voll funktionsfähige, automatische Skalierung der virtuellen Desktop-Infrastruktur (VDI) von Linux und Windows ein, auf die über eine webbasierte Benutzeroberfläche zugegriffen werden kann. Die VDI-Lösung bietet Benutzern für Forschung und Entwicklung (R&D) eine zugängliche und leistungsstarke Benutzeroberfläche, über die sie grafikintensive Analyseanfragen einreichen und Ergebnisse remote überprüfen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Administratorberechtigungen und eine Reihe von Zugriffsschlüsseln.

- AWS Cloud Development Kit (AWS CDK) Toolkit, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren des AWS-CDK.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert für Ihr AWS-Konto. Weitere Informationen finden Sie unter Installieren oder Aktualisieren der neuesten Version der AWS CLI.
- Python, installiert und konfiguriert. Weitere Informationen finden Sie unter Quellversionen (Python-Website).
- Eine oder mehrere Virtual Private Clouds (VPCs) sind verfügbar.
- Zwei oder mehr Elastic IP-Adressen verfügbar. Weitere Informationen zum Standardlimit finden Sie unter Elastic IP-Adresslimit.
- Richten Sie für die Linux-EC2-Instances ein Secure Shell (SSH)-Schlüsselpaar ein. Weitere Informationen finden Sie unter Schlüsselpaare und Linux-Instances.

Produktversionen

- AWS-CDK-Version 2.26.0 oder höher
- Python Version 3.8 oder höher

Architektur

Zielarchitektur

Die folgende Abbildung zeigt die verschiedenen Komponenten dieser VDI-Lösung. Der Benutzer interagiert mit NICE EnginFrame , um Amazon EC2-Instances gemäß den Amazon EC2-Auto Scaling-Gruppen für Windows- und Linux-NICE-DCV-Instances zu starten.

Automatisierung und Skalierung

Der in diesem Muster enthaltene Code erstellt eine benutzerdefinierte VPC, öffentliche und private Subnetze, ein Internet-Gateway, ein NAT-Gateway, einen Application Load Balancer, Sicherheitsgruppen und IAM-Richtlinien. AWS CloudFormation wird auch verwendet, um die Flotte von Linux- und Windows NICE-DCV-Servern zu erstellen.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- NICE DCV ist ein leistungsstarkes Remote-Anzeigeprotokoll, mit dem Sie Remote-Desktops und Anwendungs-Streaming von jeder Cloud oder jedem Rechenzentrum an jedes Gerät unter unterschiedlichen Netzwerkbedingungen bereitstellen können. In diesem Muster bietet es einebandbreitensparende Erfahrung, die High Performance Computing (HPC)-3D-Grafiken remote streamt.
- Mit NICE DCV Session Manager können Sie den Lebenszyklus von NICE DCV-Sitzungen in einer Flotte von NICE DCV-Servern erstellen und verwalten.
- NICE EnginFrame ist eine erweiterte Frontend-Webschnittstelle für den Zugriff auf technische und wissenschaftliche Anwendungen in der Cloud.

Code-Repository

Der Code für dieses Muster ist in der Auto-Scaling-VDI-Lösung mit NICE EnginFrame und NICE DCV Session Manager-Repository verfügbar.

Sekunden

Bereitstellen der virtuellen Desktop-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository, das den Code enthält. `git clone https://github.com/aws-samples/elastic-vdi-infrastructure.git`	Cloud-Architekt
Installieren Sie die erforderlichen AWS-CDK-Bibliotheken.	Installieren Sie die AWS-CDK-Bibliotheken.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd elastic-vdi-infrastructure`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip3 install -r requirements.txt`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameter.	1. Öffnen Sie die Datei app.py in einem Texteditor Ihrer Wahl. 2. Ersetzen Sie den `CHANGE_ME` Wert für die folgenden erforderlichen Parameter: • `region` – Die AWS-Zielregion. Eine vollständige Liste finden Sie unter AWS-Regionen. • `account` – Die ID des AWS-Zielkontos. Weitere Informationen finden Sie unter Suchen Ihrer AWS-Konto-ID. • `key_name` – Das Schlüsselpaar, das für den Zugriff auf die Linux-EC2-Instances verwendet wird. 3. (Optional) Ändern Sie die Werte für die folgenden Parameter, um die Lösung für Ihre Umgebung anzupassen: • `ec2_type_enginframe` – Der EnginFrame Instance-Typ • `ec2_type_broker` – Der Instance-Typ des Session-Manager-Brokers	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `ebs_enginframe_size` – Die Größe des Amazon Elastic Block Store (Amazon EBS)-Volumes für die EnginFrame Instance • `ebs_broker_size` – Die Größe des EBS-Volumes für die Session Manager-Broker-Instance • `TagName` and `TagValue` – Das Fakturierungs-Tag für die Ressourcen • `efadmin_uid` – Die eindeutige Kennung des EnginFrame Administratorbenutzers (efadmin) • `linux_shared_storage_size` – OpenZFS-Größe in Gibibyte (GiB) • `Shared_Storage_Linux` – Der Mountingpunkt des gemeinsam genutzten Speichers • `Enginframe_installer` – Der Download-Link für EnginFrame • `Session_Manager_Broker_Installer` – Der Download-Link für den Session Manager-Broker	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Speichern und schließen Sie die Datei app.py.	

Stellen Sie die Lösung bereit.	Führen Sie die folgenden Befehle nacheinander aus.
	`cdk bootstrap`
	`cdk deploy Assets-Stack Parameters-Stack`
	`cdk deploy Elastic-Vdi-Infrastructure`
	Wenn die Bereitstellung abgeschlossen ist, werden die folgenden beiden Ausgaben zurückgegeben:
	• `Elastic-Vdi-Infrastructure.EnginFrameURL` – Die HTTPS-Adresse des EnginFrame Portals
	• `Elastic-Vdi-InfrastruSecretEFadminPassword` – Der Amazon-Ressourcenname (ARN) des Secrets, das das Passwort für den efadmin-Benutzer enthält
	Notieren Sie sich diese Werte. Sie verwenden sie später in diesem Muster.
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Flotte der Linux-Server bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen aus. 3. Wählen Sie im Ordner cloudformation_files die Datei dcv-linux-fleet.yaml aus. 4. Definieren Sie auf der Seite Stack-Details angeben die folgenden Parameter: • Stack-Name – Der Name des Stacks. • DcvFleet – Der Name der NICE-DCV-Flotte. Lassen Sie diesen Wert nicht leer und verwenden Sie keine Leerzeichen. • InstanceType – Der Instance-Typ der Flotte. • RootVolumeSize – Die Stamm-Volume-Größe der Linux-EC2-Instance. • MinSize – Die Mindestanzahl von Knoten, die verfügbar sein und keine DCV-Sitzung ausführen sollen. Wenn Sie beispielsweise eingeben2, beginnt die	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lösung mit 2 Knoten. Wenn ein Benutzer eine Sitzung erstellt, verringert sich die Anzahl der verfügbaren Knoten auf 1, und die Lösung erstellt einen weiteren Knoten, um das Minimum aufrechtzuerhalten. • MaxSize – Die maximale Anzahl von Knoten in der Flotte. Benutzer können keine neuen Sitzungen starten, wenn das Maximum erreicht wurde. • BillingTagName – Der Tag-Name, der für die Fakturierung verwendet wird. Dieser Tag-Name muss sich von dem für den Windows-Stack verwendeten Tag-Namen unterscheiden. • BillingTagValue – Der Tag-Wert, der für die Fakturierung verwendet wird. 5. Schließen Sie den Assistenten zur Stack-Erstellung ab und wählen Sie dann Absenden, um mit der Erstellung des Stacks zu beginnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Flotte von Windows-Servern bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen aus. 3. Wählen Sie im Ordner cloudformation_files die Datei dcv-windows-fleet.yaml aus. 4. Definieren Sie auf der Seite Stack-Details angeben die folgenden Parameter: • Stack-Name – Der Name des Stacks. • DcvFleet – Der Name der NICE-DCV-Flotte. Lassen Sie diesen Wert nicht leer und verwenden Sie keine Leerzeichen. • InstanceType – Der Instance-Typ der Flotte. • RootVolumeSize – Die Stamm-Volume-Größe der Windows EC2-Instance. • MinSize – Die Mindestanzahl von Knoten, die verfügbar sein und keine DCV-Sitzung ausführen sollen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• MaxSize – Die maximale Anzahl von Knoten in der Flotte. • BillingTagName – Der Tag-Name, der für die Fakturierung verwendet wird. Dieser Tag-Name muss sich von dem für den Linux-Stack verwendeten Namen unterscheiden. • BillingTagValue – Der Tag-Wert, der für die Fakturierung verwendet wird. 5. Schließen Sie den Assistenten zur Stack-Erstellung ab und wählen Sie dann Absenden, um mit der Erstellung des Stacks zu beginnen.	

Zugriff auf die bereitgestellte Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das EnginFrame Administratorpasswort ab.	Das EnginFrame Verwaltungskonto heißt efadmin und das Passwort wird in AWS Secrets Manager als Secret gespeichert. Der ARN des Secrets wird dynamisch generiert und ist in	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Ausgabe der AWS-CDK-Bereitstellung sichtbar. 1. Suchen Sie im vorherigen Epos in der Lösungshistorie bereitstellen unter der `Elastic-Vdi-Infrastructure.SecretEFadminPassword` Ausgabe den ARN des generierten Secrets. 2. Führen Sie einen der folgenden Schritte aus, um das Secret abzurufen: • Verwenden Sie die Secrets-Manager-Konsole. Weitere Informationen finden Sie unter Abrufen von Secrets. • Geben Sie den get-secret-value-Befehl ein. `aws secretsmanager get-secret-value \ --secret-id <secret_arn> \ --query SecretString \ --output text`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf das EnginFrame Portal zu.	1. Suchen Sie im vorherigen Epos in der Lösungshistorie bereitstellen unter der `Elastic-Vdi-Infrastructure.EnginFrameURL` Ausgabe die HTTPS-Adresse des EnginFrame Portals. 2. Geben Sie in einem Webbrowser die HTTPS-Adresse des Portals ein. 3. Geben Sie die Anmeldeinformationen für den efadmin-Benutzer ein.	Cloud-Architekt
Starten Sie eine Windows-Sitzung.	1. Wählen Sie im EnginFrame Portal im Menü Windows Desktop aus. 2. Wenn Sie aufgefordert werden, sich als Windows-Administrator anzumelden, geben Sie dasselbe Passwort ein, das für den efadmin-Benutzer verwendet wurde. 3. Vergewissern Sie sich, dass die Windows-Sitzung erfolgreich gestartet wurde.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine Linux-Sitzung.	1. Wählen Sie im EnginFrame Portal im Menü Linux Desktop aus. 2. Wenn Sie aufgefordert werden, sich anzumelden, geben Sie die Anmeldeinformationen für den efadmin-Benutzer ein. 3. Vergewissern Sie sich, dass die Linux-Sitzung erfolgreich gestartet wurde.	Cloud-Architekt

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Stacks.	Löschen Sie in der AWS-CloudFormation Konsole die Stacks für die Windows- und Linux-Serverflotten. Weitere Informationen finden Sie unter Löschen eines Stacks.	Cloud-Architekt
Löschen Sie die Infrastruktur.	Löschen Sie die bereitgestellte Infrastruktur mit dem folgenden AWS-CDK-Befehl. `cdk destroy --all`	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Die Bereitstellung wurde nicht abgeschlossen, da sie unterbrochen wurde.	Folgen Sie den Anweisungen im Clean up-Epics und wiederholen Sie dieses Muster, um die Umgebung erneut bereitzustellen.

Zugehörige Ressourcen

- NICE DCV
- NICE EnginFrame

Hybride Cloud

Themen

Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode

Erstellt von Deepak Kumar (AWS)

Umgebung: Produktion	Technologien: Hybrid Cloud; Infrastruktur; Migration	Arbeitslast: Alle anderen Workloads
AWS-Services: AWS Direct Connect		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie Sie den Hybrid Linked Mode verwenden können, um Bestände in einem lokalen Rechenzentrum und einem softwaredefinierten Rechenzentrum (SDDC) von VMware Cloud on AWS mithilfe einer einzigen VMware vSphere Client-Schnittstelle anzuzeigen und zu verwalten.

Durch die Konfiguration des Hybrid Linked Mode können Sie Ihre lokalen virtuellen Maschinen (VMs) und Anwendungen in das Cloud-SDDC migrieren. Ihre IT-Teams können dann Ihre cloudbasierten Ressourcen mit vertrauten VMware-Tools verwalten, ohne dass neue Tools erforderlich sind. Mithilfe der VMware Cloud Gateway Appliance können Sie auch einen konsistenten Betrieb und eine vereinfachte Verwaltung sicherstellen.

Dieses Muster bietet zwei Optionen für die Konfiguration des Hybrid Linked Mode, Sie können jedoch jeweils nur eine Option verwenden. Die erste Option installiert die Cloud Gateway Appliance und verwendet sie, um eine Verbindung vom lokalen vCenter Server zum Cloud-SDDC herzustellen. Die zweite Option konfiguriert den Hybrid Linked Mode vom Cloud-SDDC aus.

Voraussetzungen und Einschränkungen

Voraussetzungen (beide Optionen)

- Ein vorhandenes lokales Rechenzentrum und ein Cloud-SDDC.
- Eine bestehende Verbindung zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC, die AWS Direct Connect, ein VPN oder beides verwendet.
- Das lokale Rechenzentrum und das Cloud-SDDC werden mit dem Network Time Protocol (NTP) oder einer anderen autoritativen Zeitquelle synchronisiert.
- Die maximale Latenz einer Round-Trip-Zeit zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC beträgt nicht mehr als 100 ms.
- Cloud-Administratoren mit Zugriff auf Ihre lokale Umgebung.
- Der vollqualifizierte Domänenname (FQDN) des vCenter Servers muss in eine private IP-Adresse aufgelöst werden.

Voraussetzungen für Option 1

- Die lokale Umgebung sollte auf vSphere 6.5.0d oder höher ausgeführt werden.
- Die Cloud Gateway Appliance und der vCenter Server können über AWS Direct Connect, ein VPN oder beides kommunizieren.
- Die Cloud Gateway Appliance erfüllt die Hardwareanforderungen.
- Die Firewall-Ports sind geöffnet.

Voraussetzungen für Option 2

- Der lokale vCenter Server wird auf vSphere 6.0 Update 3 oder höher oder auf vSphere 6.5.0d oder höher ausgeführt.
- Anmeldeinformationen sind für die lokale vSphere Single Sign-On (SSO) -Domäne verfügbar.
- Benutzer in der lokalen Umgebung haben nur Lesezugriff auf den Basis-DN (Basis-DN).
- Der lokale DNS-Server (Domain Name System) ist für VMware Management Gateway konfiguriert.
- Implementieren Sie Netzwerkverbindungstests mit dem VMware Connectivity Validator.
- Die Firewall-Ports sind geöffnet.

Einschränkungen

- Der hybride verknüpfte Modus kann nur eine lokale vCenter Server Enhanced Linked Mode-Domäne verbinden.
- Der hybride verknüpfte Modus unterstützt nur lokale vCenter Server, auf denen Version 6.7 oder höher ausgeführt wird.

Architektur

Das folgende Diagramm zeigt beide Optionen für die Konfiguration des verknüpften Hybrid-Modus.

Migrieren verschiedener Workload-Typen mithilfe des verknüpften Hybrid-Modus

Der Hybrid Linked Mode unterstützt die Migration von Workloads zwischen einem lokalen Rechenzentrum und einem Cloud-SDDC, indem entweder eine Cold-Migration oder eine Live-Migration mit VMware vSphere vMotion verwendet wird. Zu den Faktoren, die bei der Auswahl der Migrationsmethode berücksichtigt werden müssen, gehören der Typ und die Version des virtuellen Switches, der Verbindungstyp zum Cloud-SDDC und die Version der virtuellen Hardware.

Eine Cold-Migration ist für VMs geeignet, bei denen es zu Ausfallzeiten kommt. Sie können die VMs herunterfahren, migrieren und dann wieder einschalten. Die Migrationszeit ist schneller, da der aktive Speicher nicht kopiert werden muss. Wir empfehlen die Verwendung einer Cold-Migration für Anwendungen, die Ausfallzeiten in Kauf nehmen (z. B. Tier-3-Anwendungen oder Entwicklungs- und Test-Workloads). Wenn es bei Ihren VMs nicht zu Ausfallzeiten kommen kann, sollten Sie eine Live-Migration mit vMotion für Ihre geschäftskritischen Anwendungen in Betracht ziehen.

Das folgende Diagramm bietet einen Überblick über die verschiedenen Arten der Workload-Migration im Hybrid Linked Mode.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und VMware entwickelt wurde.
- Die VMware Cloud Gateway Appliance ermöglicht eine Reihe von Hybrid-Cloud-Anwendungsfällen, bei denen lokale Ressourcen mit Cloud-Ressourcen verbunden werden.
- VMware vSphere ist die Virtualisierungsplattform von VMware, die Rechenzentren in aggregierte Computerinfrastrukturen umwandelt, die CPU-, Speicher- und Netzwerkressourcen umfassen.

Epen

Option 1 — Verwenden Sie den verknüpften Hybrid-Modus mit der Cloud Gateway-Appliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Cloud Gateway-Appliance.	1. Melden Sie sich bei der VMware Cloud on AWS AWS-Konsole an und laden Sie die Cloud Gateway Appliance herunter. 2. Installieren Sie die Cloud Gateway Appliance in Ihrer lokalen Umgebung mit den folgenden zwei Schritten: • Wählen Sie Start, um die Cloud Gateway Appliance zu konfigurieren und dann bereitzustellen. • Konfigurieren Sie den verknüpften Hybrid-Mo dus. Weitere Informationen und detaillierte Schritte finden Sie unter Konfiguration des Hybrid Linked Mode mithilfe der vCenter Cloud Gateway Appliance in der VMware-Do kumentation.	Cloud-Administrator

Option 2 — Verwenden Sie den verknüpften Hybrid-Modus aus dem Cloud-SDDC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den verknüpften Hybrid-Modus über das Cloud-SDDC.	1. Melden Sie sich bei der VMware Cloud on AWS AWS-Konsole an und überprüfen Sie mit dem Connectivity Validator die gesamte erforderliche Netzwerkkonnektivität. Weitere Informationen dazu finden Sie in der VMware-Dokumentation unter Überprüfen der Netzwerkkonnektivität für den Hybrid Linked Mode. 2. Melden Sie sich beim vSphere Client des Cloud-SDDC an, wählen Sie Menü, dann Administration und dann Domains aus. 3. Wählen Sie im Abschnitt Hybrid Cloud Linked Domains aus und stellen Sie dann eine Verbindung zu Ihrem lokalen vCenter Server her. 4. Fügen Sie der Cloud-SDDC Lightweight Directory Access Protocol (LDAP) -Domäne eine Identitätsquelle hinzu. Weitere Informationen dazu finden Sie unter Hinzufügen einer Identitätsquelle zur SDDC-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	LDAP-Domäne in der VMware-Dokumentation.	

Zugehörige Ressourcen

- Konfiguration des verknüpften Hybrid-Modus
- Konfiguration des hybriden verknüpften Modus für VMware Cloud on AWS

Konfigurieren Sie VMware vRealize Automation für die Bereitstellung von VMs auf VMware Cloud on AWS

Erstellt von Deepak Kumar (AWS)

Umgebung: Produktion	Technologien: Hybrid Cloud; Infrastruktur	Arbeitslast: Alle anderen Workloads
AWS-Services: AWS Direct Connect; AWS-Standort-zu-Standort-VPN		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware vRealize Automation ist eine Automatisierungssoftware, mit der Sie IT-Ressourcen anfordern und verwalten können. Wenn Sie sich für die Konfiguration von vRealize Automation mit VMware Cloud on AWS entscheiden, können Sie die Bereitstellung von virtuellen Maschinen (VMs), Anwendungen und IT-Services in mehreren Rechenzentren und Cloud-Umgebungen automatisieren.

Ihre IT-Teams können dann Katalogelemente erstellen, um die Servicebereitstellung und die Betriebsfunktionen zu konfigurieren, die Ihre Benutzer anfordern und mit ihren vorhandenen vRealize Automation-Tools verwenden können. Sie können auch Ihre IT-Agilität und Effizienz verbessern, indem Sie VMware Cloud on AWS mit vRealize Automation Cloud Assembly integrieren.

Dieses Muster beschreibt, wie VMware vRealize Automation so konfiguriert wird, dass virtuelle Maschinen oder Anwendungsfunktionen auf VMware Cloud on AWS automatisch erstellt werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandenes lokales Rechenzentrum und ein softwaredefiniertes Rechenzentrum (SDDC) von VMware Cloud on AWS. Weitere Informationen zum Cloud-SDCC finden Sie unter Über softwaredefinierte Rechenzentren in der VMware-Dokumentation.
- Eine bestehende Verbindung zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC, die AWS Direct Connect, ein VPN (routen- oder richtlinienbasiert) oder beides verwendet.
- Das lokale Rechenzentrum und das Cloud-SDDC werden mit dem Network Time Protocol (NTP) oder einer anderen autoritativen Zeitquelle synchronisiert.
- Die maximale Latenz einer Round-Trip-Zeit zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC beträgt nicht mehr als 100 ms.
- Der vollqualifizierte Domänenname (FQDN) des vCenter Servers muss in eine private IP-Adresse aufgelöst werden.
- Cloud-SDDC-Benutzer mit Zugriff auf Ihre lokale Umgebung.
- Zugriff auf Organisationsinhaber in der vRealize Automation Cloud Assembly-Dienstrolle.
- Endbenutzer mit der Berechtigung in vRealize Automation Service Broker, den Dienst zu nutzen.
- Der CIDR-Bereich (Classless Inter-Domain Routing) des lokalen Rechenzentrums muss für die Generierung von API-Token aus der VMware Cloud on AWS AWS-Konsole geöffnet sein. Die folgende Liste enthält die Rollen, die mindestens für die Generierung von API-Token erforderlich sind:
  - Mitglied der Organisation
  - Inhaber der Organisation
  - Servicerollen — VMware Cloud on AWS
  - Administrator
  - NSX Cloud-Administrator
  - NSX-Cloud-Auditor

Weitere Informationen dazu finden Sie unter Konnektivitätsoptionen für VMware Cloud on AWS AWS-SDDCs im AWS-Partnernetzwerk-Blog.

Einschränkungen

- Sie können nur 20 VMware Cloud-Konten mit öffentlichen Endpoints in einer vRealize Automation konfigurieren. Weitere Informationen dazu finden Sie unter Maxima für Skalierbarkeit und Parallelität in der VMware-Dokumentation.

Produktversionen

- vRealize Automation Version 8.x oder höher
- VMware vRealize Identity Manager Version 3.x oder höher
- VMware vRealize Suite Lifecycle Manager Version 8.x oder höher

Architektur

Das folgende Diagramm zeigt die vRealize Automation-Services, die die Infrastruktur sowohl von lokalen als auch von VMware Cloud on AWS AWS-Umgebungen nutzen können.

Komponenten von VMware Cloud Assembly

VMware Cloud Assembly ist eine Kernkomponente von vRealize Automation. Sie können damit VMs und Rechenressourcen bereitstellen und bereitstellen. In der folgenden Tabelle werden die Komponenten von VMware Cloud Assembly beschrieben, die für die Bereitstellung von VMs auf VMware Cloud on AWS konfiguriert werden müssen.

Komponenten	Definition
Cloud-Konto	Das Cloud-Konto enthält Verbindungsdetails (z. B. Servername, Benutzername und Passwort, Zugriffsschlüssel und API-Token). VMware Cloud Assembly verwendet das Cloud-Konto, um eine Bestandsaufnahme Ihrer Ressourcen zu erstellen.
Cloud-Zonen	Cloud-Zonen identifizieren Ressourcengrenzen im Cloud-Konto (z. B. AWS-Regionen und das Cloud-SDDC). Cloud-Zonen verknüpfen Rechenressourcen mit dem Cloud Assembly-Projekt.
Projekte	Ein Projekt ist eine logische Einheit, die aus Benutzern und Ressourcen wie Cloud-Zon en besteht. Es besteht auch aus Ressource

	nkontingenten und VM-Benennungsrichtlinien, die beim Erstellen der VM verwendet werden.
Zuordnungen von Geschmacksrichtungen	Flavor-Mapping liefert Informationen über die Kapazität der VM (z. B. Anzahl der CPUs und Speichermenge), die in der Cloud-Vorlage verwendet wird.
Image-Zuordnungen	Die Image-Mapping ordnet die VMware vSphere VM-Vorlage und das Amazon Web Services (AWS) -Image zu, die in der Cloud-Vorlage verwendet werden. Weitere Informationen dazu finden Sie in der VMware-Dokumentation unter Weitere Informationen zu Image-Zuordnungen in vRealize Automation.
Netzwerkprofil	Das Netzwerkprofil steuert die Platzierungsentscheidung, bei der bei der VM-Bereitstellung ein Netzwerk ausgewählt wird.
Speicherprofil	Das Speicherprofil steuert die Entscheidung über die Platzierung und Auswahl des Speichers bei der VM-Bereitstellung.
Cloud-Vorlagen	VMware Cloud-Vorlagen sind ein wichtiger Bestandteil von vRealize Automation, da sie die Bereitstellung und Orchestrierung der Cloud-Infrastruktur definieren. Die Cloud-Vorlagen sind Spezifikationen für die Ressourcen und beinhalten den Ressourcentyp, die Ressource neigenschaften und die von Benutzern zu erfassenden Eingaben.

Tools

- VMware vRealize Automation — vRealize Automation ist eine Plattform zur Infrastrukturautomatisierung mit ereignisgesteuerter Statusverwaltung und Compliance. Sie wurde

entwickelt, um Unternehmen bei der Steuerung und Sicherung von Self-Service-Clouds, Multi-Cloud-Automatisierung mit Governance und basierter Infrastrukturbereitstellung zu unterstützen. DevOps

- VMware Cloud on AWS — VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und VMware entwickelt wurde.

Epen

Generieren Sie die API-Token

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die API-Token von Ihrem VMware Cloud on AWS AWS-Konto aus.	1. Melden Sie sich bei der VMware Cloud Console an. 2. Wählen Sie auf der VMware Cloud Services-Symbolleiste Mein Konto und dann API-Token aus. 3. Geben Sie einen Namen für Ihr API-Token ein, geben Sie die erforderliche Lebensdauer an und definieren Sie die Bereiche für das Token. 4. Aktivieren Sie das Kontrollkästchen ID öffnen und wählen Sie dann Generate aus. 5. Notieren Sie sich die Anmeldeinformationen des API-Tokens. Weitere Informationen dazu finden Sie in der VMware-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokumentation unter Wie generiere ich API-Token.	

Installieren Sie vRealize Automation in Ihrem lokalen Rechenzentrum

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die erforderliche Software herunter.	Laden Sie die ISO-Datei für VMware vRealize Suite vom My VMware-Portal herunter. Dieses Paket enthält vRealize Suite Lifecycle Manager, VMware Identity Manager und vRealize Automation.	Cloud-Administrator
Installieren Sie die -Software.	Installieren Sie die Software und stellen Sie eine Verbindung zu Ihrem Cloud-SDCC her, indem Sie den Anweisungen unter Installation von vRealize Suite Lifecycle Manager mit Easy Installer for vRealize Automation und VMware Identity Manager in der VMware-Dokumentation folgen. Wichtig: Stellen Sie sicher, dass Folgendes für Ihre Installation verfügbar ist: • Das lokale VMware vCenter Server-Setup und die Anmeldeinformationen	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die Netzwerkdetails für die vRealize Automation-IP und das Subnetz • Der vRealize Automation-Lizenzschlüssel	

Connect VMware Cloud on AWS mit VMware Cloud Assembly

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihre Cloud-Konten.	1. Öffnen Sie in der VMware Cloud-Konsole die Registerkarte Infrastruktur, wählen Sie Verwalten — Cloud-Konten und dann Cloud-Konten hinzufügen aus. 2. Wählen Sie VMware Cloud on AWS als Typ aus. 3. Fügen Sie die API-Token -Informationen ein, die Sie zuvor aufgezeichnet haben. Dadurch werden alle verfügbaren Cloud-SDDCs in Ihrer VMware Cloud on AWS-Organisation aufgefüll t. 4. Wählen Sie das erforderl iche Cloud-SDCC aus und geben Sie dann den vCenter-Benutzernamen und das Kennwort für das SDDC ein.	Cloud-Architekt, Cloud-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Nachdem Sie erfolgreich authentifiziert wurden, können Sie das integrierte VMware Cloud on AWS AWS-Konto mit dem Status OK anzeigen. Weitere Informationen dazu finden Sie unter Erstellen eines VMware Cloud on AWS AWS-Cloud-Kontos in vRealize Automation in der VMware-Dokumentation.	
Konfigurieren Sie das Projekt.	1. Öffnen Sie in der VMware Cloud Console die Registerkarte Projekte und wählen Sie dann Neues Projekt aus. 2. Geben Sie den Namen Ihres Projekts ein. 3. Öffnen Sie die Registerkarte Cloud-Zonen und wählen Sie das Standard-Cloud-Konto für VMware Cloud on AWS aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Cloud-Zone konfigurieren.	1. Öffnen Sie in der VMware Cloud Console Cloud Zones und wählen Sie die Cloud-Zone für Ihr SDDC-Rech enzentrum aus. 2. Standardmäßig hat `cloudadmin@vmc.local` (dies ist die standardmäßige lokale Benutzer-ID für das vCenter des Cloud-SDDC) nur Zugriff auf die Bereitstellung in der. `Compute-ResourcePool` 3. Öffnen Sie die Registerkarte Compute unter Cloud Zones und wählen Sie dann Compute- aus. ResourcePool	Cloud-Administrator
Konfigurieren Sie das Flavor-Mapping.	1. Öffnen Sie die Registerkarte Flavor Mappings und erstellen Sie ein neues Flavor-Mapping. 2. Geben Sie den Flavor-Namen ein, wählen Sie das VMware Cloud on AWS AWS-Konto aus und geben Sie dann die Anzahl der vCPUs und die Speichergenge an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Image-Zuordnung.	1. Öffnen Sie Image Mappings und erstellen Sie ein neues Image-Mapping. 2. Geben Sie den Bildnamen ein. 3. Wählen Sie das VMware Cloud on AWS AWS-Konto aus und stellen Sie die erforderlichen Cloud-Kon tovorlagen bereit.	Cloud-Administrator
Netzwerkprofil konfigurieren.	1. Öffnen Sie das Netzwerkp rofil und erstellen Sie ein neues Netzwerkprofil. 2. Geben Sie den Namen des Netzwerkprofils ein. 3. Öffnen Sie die Registerk arte Netzwerk und wählen Sie das vorhandene Netzwerk aus, das Sie für die Bereitstellung verwenden möchten.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Speicherprofil.	1. Öffnen Sie das Speicherprofil und wählen Sie Neues Speicherprofil. 2. Geben Sie den Namen des Speicherprofils ein. 3. Erstellen Sie im Abschnitt Richtlinien eine neue Richtlinie. 4. Wählen Sie Workload Datastore aus. Hat standardmäßig `cloudadmin@vmc.local` nur Zugriff auf die Bereitstellung im Datenspeicher des Workloads.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Cloud-Vorlage.	1. Öffnen Sie die Registerkarte „Design“, wählen Sie „Cloud-Vorlagen“ und dann „Neu von“ und „Leere Leinwand“. 2. Geben Sie den Namen und die Beschreibung der Cloud-Vorlage an. 3. Wählen Sie das Projekt aus, das Sie zuvor erstellt haben. 4. Ziehen Sie von der Entwurfsseite für Cloud-Template-Ressourcen die Komponenten entsprechend Ihren Anforderungen auf die leere Arbeitsfläche. 5. Wählen Sie Test, um die Vorlage zu testen und etwaige Probleme zu beheben. 6. Wählen Sie Deployment und geben Sie den Bereitstellungsnamen für die Bereitstellung der VMs ein. Weitere Informationen dazu finden Sie in der VMware-Dokumentation unter Erstellen einer einfachen Cloud-Vorlage.	Cloud-Administrator

Zugehörige Ressourcen

- Connect vRealize Automation Version 8.x mit Ihrem SDDC:
- Stellen Sie ein SDDC aus der VMware Cloud on AWS AWS-Konsole bereit
- Integration von AWS Direct Connect mit VMware Cloud on AWS

Stellen Sie mithilfe von VMware Cloud on AWS ein VMware-SDDC auf AWS bereit

Erstellt von Deepak Kumar (AWS) und Derek Cox (AWS)

Umgebung: Produktion	Technologien: Hybrid Cloud; Infrastruktur	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon VPC		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie Sie ein VMware-basiertes Software-Defined Data Center (SDDC) erstellen, das in der Amazon Web Services (AWS) Cloud gehostet wird. Sie können ein SDDC bereitstellen, um Ihre VMware vSphere-basierten Workloads in die AWS-Cloud zu migrieren und AWS-Services zu nutzen, während Sie Ihre vorhandenen VMware-Tools und -Fähigkeiten nutzen. Sie können dieses SDDC verwenden, um Ihre Produktionsanwendungen in privaten, öffentlichen und Hybrid-Cloud-Umgebungen auf VMware vSphere-Basis mit optimiertem Zugriff auf AWS-Services auszuführen. Sie können das SDDC beispielsweise als sekundären Standort für die Notfallwiederherstellung oder zur Erweiterung Ihres Rechenzentrums auf verschiedene geografische Standorte verwenden.

VMware Cloud on AWS ist ein pay-as-you-go (On-Demand-) Service, mit dem Unternehmen jeder Größe Workloads in VMware vSphere-basierten Cloud-Umgebungen ausführen können, indem sie eine breite Palette von AWS-Services nutzen. Sie können mit mindestens 2 Hosts pro SDDC-Cluster beginnen und in Ihrer Produktionsumgebung auf bis zu 16 Hosts pro Cluster skalieren. Weitere Informationen finden Sie auf der Website von VMware Cloud on AWS. Weitere Informationen zu SDDCs finden Sie in der VMware-Dokumentation unter Über softwaredefinierte Rechenzentren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eröffnen Sie ein MyVMware-Konto und füllen Sie alle Felder aus.
- Eröffnen Sie ein AWS-Konto. Anweisungen finden Sie im AWS Knowledge Center.
- Eröffnen Sie ein MyVMware Cloud on AWS-Konto. Ein Aktivierungslink wird an die E-Mail-Adresse gesendet, die Sie bei der Registrierung angegeben haben.

Einschränkungen

- Weitere Informationen finden Sie auf den Seiten mit den Konfigurationsbeschränkungen für VMware Cloud on AWS auf der VMware-Website.

Produktversionen

- Weitere Informationen finden Sie in den Versionshinweisen zu VMware Cloud on AWS in der VMware-Dokumentation.

Architektur

Zieltechnologie-Stack

Das folgende Diagramm zeigt den VMware-Software-Stack, einschließlich vSphere, vCenter, vSAN und NSX-T, der auf einer dedizierten AWS-Bare-Metal-Infrastruktur ausgeführt wird. Sie können Ihre VMware-basierten Ressourcen und Tools auf AWS mit nahtloser Integration mit anderen AWS-Services wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Redshift, AWS Direct Connect, Amazon Relational Database Service (Amazon RDS) und Amazon DynamoDB verwalten.

Die grundlegende Einheit von VMware Cloud on AWS ist ein SDDC, das die folgenden Komponenten umfasst:

- Compute: Die Rechenkomponente ist die unterste Ebene des VMware Cloud on AWS SDDC. VMware Cloud on AWS läuft auf Amazon EC2 EC2-Bare-Metal-Instance-Typen. Dazu gehören

`i3.metal` `i3en.metal`, und`i4i.metal`, und bieten direkten Zugriff auf physische Ressourcen wie Prozessoren und Speicher.

Wichtig: Der `i3.metal` Instanztyp für VMware Cloud on AWS, einschließlich On-Demand-Optionen und Abonnementoptionen mit Laufzeiten von einem Jahr und drei Jahren, wird voraussichtlich am 31. Dezember 2026 sein Ende der Lebensdauer und des Supports erreichen. Darüber hinaus können Neukunden derzeit keine Instances anfordern. `i3.metal` Weitere Informationen finden Sie in der Ankündigung im VMware Cloud-Blog.

- Speicher: SDDC-Cluster unterstützen VMware vSAN mit einer All-Flash-Konfiguration für Speicher unter Verwendung von NVMe (Non-Volatile Memory Express) -Flash-Speicher, der schnellen und leistungsstarken Speicher bietet. Ab SDDC-Version 1.20 bietet VMware Cloud on AWS Unterstützung für zwei Arten von externem Speicher: Amazon FSx for NetApp ONTAP und VMware Cloud Flex Storage.
- Netzwerke: Netzwerkfunktionen und -richtlinien werden mithilfe von VMware NSX-T im SDDC-Cluster verwaltet. Mehrstufige virtuelle Netzwerke werden im SDDC-Cluster erstellt, um Netzwerkressourcen von physischen Geräten zu trennen. Auf diese Weise können Benutzer von VMware Cloud on AWS logische, softwaredefinierte Netzwerke erstellen.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und VMware entwickelt wurde.

Epen

Erstellen Sie eine VPC und ein Subnetz in Ihrem AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei Ihrem AWS-Konto an.	Melden Sie sich mit Anmeldein formationen mit Administr atorberechtigungen bei Ihrem AWS-Konto an.	Cloud-Administrator
Erstellen einer neuen VPC.	In diesem Schritt definieren Sie eine Virtual Private Cloud	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(VPC), die eine Verbindung zum SDDC herstellt. Wenn Sie bereits über eine VPC verfügen, die Sie für das SDDC verwenden möchten, überspringen Sie diesen Schritt. 1. Wählen Sie die AWS-Region für die Bereitstellung Ihrer VMware Cloud on AWS AWS-SDDC. 2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. 3. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. 4. Wählen Sie VPC erstellen aus. 5. Geben Sie VPC-Einstellungen wie das VPC-Name-Tag, den IPv4-CIDR-Block, Tenancy (als Standard beibehalten) an, und wählen Sie dann Create VPC aus. 6. Wenn die VPC erstellt wurde, wählen Sie Schließen. Weitere Informationen finden Sie in der AWS-Dokum	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	entation unter Erstellen und Konfigurieren Ihrer VPC.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein privates Subnetz.	Sie erstellen nun für jede Availability Zone ein privates Subnetz für das Elastic Network Interface (ENI). Wir empfehlen, ein Subnetz zu verwenden, an das kein Internet-Gateway angeschlossen ist. 1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. 2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. 3. Wählen Sie Create Subnet aus. 4. Wählen Sie auf der Seite Create Subnet die VPC aus, die Sie zuvor erstellt haben. 5. Vervollständigen Sie die Einstellungen für das Subnetz, einschließlich eines Subnetznamens, einer Availability Zone und eines IPv4-CIDR-Blocks. 6. Wählen Sie Create Subnet aus. Wiederholen Sie diese Schritte, um Subnetze für jede	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Availability Zone in der Region zu erstellen.	

Aktivieren Sie VMware Cloud on AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Dienst.	Wenn Sie sich für ein MyVMware-Konto registrie ren, sendet Ihnen VMware eine Willkommens-E-Mail und einen Aktivierungslink an die von Ihnen angegebene E-Mail-Adresse. 1. Öffnen Sie in der Willkommens-E-Mail in Ihrem Browser den Link Service aktivieren. 2. Melden Sie sich mit MyVMware-Anmeldein formationen an. 3. Lesen und akzeptier en Sie die Allgemeinen Geschäftsbedingungen für die Nutzung der Dienste. 4. Schließen Sie den Kontoaktivierungsprozess ab. Sie werden zur VMware Cloud on AWS AWS-Konso le weitergeleitet. (Hinweis: VMware Cloud on AWS AWS-Konten basieren auf einer Organisation, die	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine Gruppe oder einen Geschäftsbereich darstellt , der das Konto abonniert hat. Diese Organisation steht in keiner Beziehung zu AWS Organizations.) 5. Erstellen Sie auf der Seite „Organisation auswählen oder erstellen“ eine Organisation, die mit dem MyVMware-Konto verknüpft ist. 6. Geben Sie zur logischen Unterscheidung den Namen und die Adresse der Organisation ein. 7. Wählen Sie Organisat ion erstellen aus, um den Vorgang abzuschließen. Weitere Informationen zu diesem Prozess finden Sie im SDDC Deployment and Best Practices Guide on AWS in der AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie IAM-Rollen zu.	Wenn die Organisation erstellt wurde, weisen Sie bestimmten Benutzern privilegierten Zugriff auf die Cloud Services und die SDDC-Konsole, SDDC und NSX-Komponenten zu. Anweisungen finden Sie in der VMware-Dokumentation unter Zuweisen einer VMC-Servicerolle zu einem Organisationsmitglied. Es gibt zwei Arten von Organisationsrollen: • Organisationsinhaber können Benutzer hinzufügen, entfernen und ändern und auf alle Cloud-Ressourcen zugreifen. • Organisationsmitglieder können nur auf Cloud-Ressourcen zugreifen.	Cloud-Administrator

Stellen Sie ein SDDC bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie ein SDDC in Ihrem VMware Cloud on AWS AWS-Konto bereit.	Wichtig: Nachdem ein AWS-Konto einer VMware-Organisation als registrierter Verkäufer zugeordnet wurde, kann die AWS-Kontonummer nicht mehr aktualisiert werden.	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pro VMware-Organisation kann es nur einen registrierten AWS-Verkäufer geben. So stellen Sie ein SDDC bereit: 1. Melden Sie sich unter https://vmc.vmware.com bei der VMC-Konsole an. 2. Wählen Sie VMware Cloud on AWS Service aus den verfügbaren Services. 3. Wählen Sie Create SDDC aus. 4. Geben Sie SDDC-Eigenschaften wie AWS-Region, Bereitstellung (Einzelhost, Multi-Host oder Stretched Cluster), Hosttyp, SDDC-Name, Anzahl der Hosts, Hostkapazität und Gesamtkapazität ein, und wählen Sie dann Weiter aus. 5. Connect zu Ihrem AWS-Konto her und wählen Sie dann Weiter. 6. Wählen Sie Ihre zuvor konfigurierte VPC und Ihr Subnetz aus und klicken Sie dann auf Weiter. 7. Geben Sie den CIDR-Block des Management-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Subnetzes für das SDDC ein und wählen Sie dann WEITER. Weitere Informationen finden Sie im VMware Cloud-Blog unter Auswahl von IP-Subnetzen und Konnektivität für Ihr SDDC. 8. Aktivieren Sie die beiden Kontrollkästchen, um zu bestätigen, dass Sie die Verantwortung für die Kosten für die Bereitstellung eines SDDC übernehmen, und wählen Sie dann SDDC bereitstellen aus. Wenn Sie Deploy SDDC wählen, wird Ihnen eine Gebühr berechnet. Sie können den Bereitstellungsvorgang, der einige Zeit in Anspruch nimmt, nicht anhalten oder abbrechen. Weitere Informationen zum Erstellen eines SDDC finden Sie unter Bereitstellen eines SDDC über die VMC-Konsole in der VMC-Konsole in der VMC-Dokumentation.	

Zugehörige Ressourcen

- Bereitstellung und Verwaltung eines softwaredefinierten Rechenzentrums (VMware-Dokumentation)
- Funktionen von VMware Cloud on AWS (AWS-Website)
- Beschleunigen Sie die Cloud-Migration und -Modernisierung mit VMware Cloud on AWS (Video)

Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS

Erstellt von Deepak Kumar (AWS), Piotr Pitera (AWS) und Sachin Trivedi (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: VMware vRealize Network Insight	Ziel: VMware Cloud on AWS
R-Typ: Umziehen	Arbeitslast: Alle anderen Workloads	Technologien: Hybrid Cloud; Infrastruktur; Migration
AWS-Services: VMware Cloud auf AWS		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie Sie VMware vRealize Network Insight in VMware Cloud on integrieren AWS und den Verkehrsfluss von Ihren virtuellen Maschinen überprüfen. Diese Integration hilft Ihnen auch bei der Planung von Anwendungsmigrationen zu VMware Cloud on. AWS

vRealize Network Insight bietet Einblick in Ihre Netzwerkinfrastruktur. Es bietet Netzwerküberwachungs- und Analysefunktionen, um die Sicherheit zu verbessern, Migrationsrisiken zu minimieren und die Leistung zu optimieren. Sie können dieses Tool verwenden, um den Datenfluss von Ihren virtuellen Maschinen zu überwachen und empfohlene Sicherheitsregeln auf der Grundlage des beobachteten Datenverkehrs einzusehen. Weitere Informationen zu vRealize Network Insight finden Sie in der VMware-Dokumentation.

VMware Cloud on AWS ist ein pay-as-you-go (On-Demand-) Service, der es Unternehmen jeder Größe ermöglicht, Workloads in VMware vSphere-basierten Cloud-Umgebungen auszuführen, indem sie eine Vielzahl von verwenden. AWS-Services Sie können mit mindestens 2 Hosts pro SDDC-

Cluster beginnen und in Ihrer Produktionsumgebung auf bis zu 16 Hosts pro Cluster skalieren. Weitere Informationen finden Sie auf der Website von VMware Cloud on AWS. Weitere Informationen zu SDDCs finden Sie unter About Software-Defined Data Centers in der VMware-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- VMware Cloud on AWS SDDC, bereitgestellt

Einschränkungen

- Bekannte Einschränkungen finden Sie in der VMware-Dokumentation.

Produktversionen

- vRealize Network Insight Version 5.0.0
- VMware Cloud on AWS SDDC Version 1.24

Architektur

Quelltechnologie-Stack

- vRealize Network Insight

Zieltechnologie-Stack

- VMware Cloud auf AWS

Zielarchitektur

Das folgende Diagramm zeigt die Konnektivität zwischen VMware Cloud on AWS und vRealize Network Insight vor Ort.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von VMware AWS und VMware entwickelt wurde.
- VMware vRealize Network Insight ist ein Überwachungs- und Analysetool, das Einblicke in die Netzwerkinfrastruktur für die Sicherheitsplanung und Fehlerbehebung bietet.

Epen

Richten Sie Ihre Umgebung für vRealize Network Insight ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein VMware-Benutzerkonto.	Erstellen Sie ein VMware-Benutzerkonto oder melden Sie sich mit Ihrem vorhandenen VMware-Konto an. Um ein neues Konto zu eröffnen: 1. Melden Sie sich für ein VMware Customer Connect-Konto an, indem Sie das Registrierungsformular ausfüllen. Neue Benutzer erhalten eine E-Mail zur Aktivierung ihrer Konten. 2. Geben Sie den Authentifizierungscode aus der E-Mail ein. 3. Melden Sie sich bei Customer Connect an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die OVA-Dateien für vRealize Network Insight herunter.	Laden Sie die OVA-Dateien für vRealize Network Insight herunter:. 1. Navigieren Sie zur Download-Seite für das VMware-Produkt unter https://my.vmware.com/group/vmware/home. 2. Suchen Sie nach vRealize Network Insight. 3. Laden Sie die neuesten Plattform- und Collector-OVA-Dateien von vRealize Network Insight Version 5.0.0 herunter.	Cloud-Administrator
Stellen Sie vRealize Network Insight bereit.	Anweisungen zur Bereitstellung finden Sie in der VMware-Dokumentation.	Cloud-Administrator

Fügen Sie eine Datenquelle und einen Collector hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Datenquelle hinzu.	1. Melden Sie sich bei vRealize Network Insight an. 2. Wählen Sie Einstellungen, Konten und Datenquellen, Quelle hinzufügen. 3. Wählen Sie für Typ die Option On-Premise vCenter Server aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der VMware-Dokumentation.	
Richten Sie einen Collector für die Datenquelle ein.	Anweisungen finden Sie in der VMware-Dokumentation.	Cloud-Administrator

Analysieren Sie Anwendungsabhängigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine -Anwendung.	Wenn Sie noch keine Anwendung in vRealize Network Insight haben, folgen Sie den Schritten in der VMware-Dokumentation, um eine zu erstellen.	Cloud-Administrator
Entdecken und analysieren Sie Ihre Anwendung.	1. Verwenden Sie vRealize Network Insight, um Ihre Anwendung zu ermitteln. Anweisungen finden Sie in der VMware-Dokumentation. 2. Analysieren Sie Ihre Anwendung. Anweisungen finden Sie in der VMware-Dokumentation.	Cloud-Administrator

Zugehörige Ressourcen

- Bereitstellen eines VMware-SDDC auf AWS mithilfe von VMware Cloud on AWS (AWS Prescriptive Guidance)

- Konfigurieren Sie eine Rechenzentrumserweiterung für VMware Cloud AWS unter Verwendung des Hybrid Linked Mode (Prescriptive Guidance)AWS
- Migrieren Sie VMware SDDC auf VMware Cloud AWS unter Verwendung von VMware HCX (Prescriptive Guidance)AWS
- Dokumentation zu VMware vRealize Network Insight (VMware-Website)

Migrieren Sie VMs mithilfe von HCX OS Assisted Migration zu VMware Cloud on AWS

Erstellt von Deepak Kumar (AWS) und Himanshu Gupta (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Nicht-vSphere-Umgebung	Ziel: VMware Cloud on AWS SDDC
R-Typ: Umziehen	Arbeitslast: Alle anderen Workloads	Technologien: Hybrid-Cloud; Migration

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie eine virtuelle Maschine (VM) mithilfe von OS Assisted Migration (OSAM) von einer Nicht-vSphere-Umgebung zu VMware Cloud on Amazon Web Services (AWS) migriert wird.

OSAM ist Teil der VMware Hybrid Cloud Extension (HCX), die in VMware Cloud on AWS enthalten ist. Sie können OSAM verwenden, um eine Nicht-vSphere-Umgebung wie VMware KVM oder Hyper-V zu VMware Cloud on AWS zu migrieren. OSAM verwendet Sentinel-Software, die Sie auf einer Windows- oder Linux-Gast-VM installieren, um die Replikation der VM aus Ihrer lokalen Umgebung in ein softwaredefiniertes Rechenzentrum (SDDC) auf VMware Cloud on AWS zu unterstützen.

Dieses Muster erklärt, wie Sie OSAM aktivieren, Sentinel-Software auf einer Windows-VM installieren, eine Verbindung herstellen und sich bei einer HCX Sentinel Gateway (SGW) -Appliance am Quellstandort registrieren und eine Weiterleitungsverbindung mit einer HCX Sentinel Data Receiver (SDR) -Appliance am Zielstandort herstellen, um die Migration zu initiieren.

Weitere Informationen zu OSAM finden Sie in der VMware-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Installieren Sie HCX in Ihren Quell- und Zielumgebungen. Informationen zu den HCX-Voraussetzungen finden Sie unter Migration von VMware SDDC zu VMware Cloud on AWS mit VMware HCX in der Dokumentation AWS Prescriptive Guidance Guidance-Dokumentation.
- Informationen zu den Voraussetzungen für OSAM finden Sie in der Installationscheckliste in der VMware-Dokumentation.
- Informationen zu den OSAM-Ports finden Sie unter VMware HCX-Port-Anforderungen auf der VMware Ports and Protocols-Website.

Einschränkungen

- Konfigurationsbeschränkungen für VMware HCX 4.2.0
- Überlegungen zur OSAM-Bereitstellung
- Unterstützte Gastbetriebssysteme
- Überlegungen zum Gastbetriebssystem

Produktversionen

- VMware HCX 4.2.0
- VMware SDDC 1.12

Architektur

Das folgende Diagramm zeigt, wie HCX OSAM mit der Sentinel-Software zusammenarbeitet, um Nicht-vSphere-VMs aus Ihrer lokalen Umgebung auf VMware Cloud on AWS zu replizieren.

OSAM besteht aus drei Komponenten:

- Die Sentinel Gateway (SGW) -Appliance, die zur Verbindung und Weiterleitung von Workloads und Anwendungen in der VMware-basierten Quellumgebung verwendet wird
- Der Sentinel Data Receiver (SDR), der in der VMware Cloud on AWS AWS-Zielumgebung verwendet wird, um migrierte Workloads von der Quelle zu empfangen

- Sentinel-Software, die auf jeder Gast-VM installiert sein muss, die Sie migrieren möchten

OSAM verwendet die Sentinel-Software, die auf Windows- oder Linux-Gast-VMs installiert ist, um die Replikation einer lokalen VM auf ein VMware-SDDC zu unterstützen. Die Sentinel-Software, die Sie auf Gast-VMs installieren, sammelt die Systemkonfigurationen von der Gast-VM und unterstützt Sie bei der Datenreplikation. Diese Informationen werden auch verwendet, um das Inventar der Gast-VMs für die Migration zu erstellen, und helfen dabei, die Festplatten auf der Replikat-VM für Replikations- und Migrationszwecke vorzubereiten.

Tools

- VMware HCX 4.2.0
- VMware Cloud on AWS SDDC

Epen

HCX konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie HCX Cloud und HCX Connector bereit.	Folgen Sie den Anweisungen unter HCX Connector- und HCX Cloud-Installationen in der VMware-Dokumentation.	Cloud-Administrator, Systemadministrator

Konfigurieren Sie OSAM und migrieren Sie virtuelle Maschinen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie HCX Sentinel.	So installieren Sie Sentinel unter Linux: 1. Wählen Sie im vCenter Server für den HCX Connector Interconnect,	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Multi-Site Service Mesh, Sentinel Management aus. 2. Wählen Sie Linux-Paket herunterladen. 3. Installieren Sie den Sentinel-Agenten auf einem Linux-Computer. Weitere Informationen finden Sie in der VMware-Dokumentation unter Herunterladen und Installieren der HCX Sentinel Agent-Software.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie virtuelle Maschinen.	Gehen Sie folgendermaßen vor, um Ihre VMs in Gruppen (sogenannten Mobilität sgruppen) zu migrieren: 1. Wählen Sie im vSphere Client im HCX-Plug-In Dienste, Migration aus. 2. Wählen Sie Migrate (Migrieren). 3. Wählen Sie Non vSphere Inventory, Remotever bindungen aus. Daraufhin wird die Liste der VMs angezeigt, auf denen Sie HCX Sentinel installiert haben. 4. Geben Sie als Gruppenna me den Namen der Mobilitätsgruppe ein, die Sie für die VMs erstellen möchten. 5. Wählen Sie die VMs aus, die Sie migrieren möchten, und klicken Sie dann auf Hinzufügen, um sie der Mobilitätsgruppe hinzuzufü gen. 6. Für jede VM: a. Wählen Sie den Ziel-Compute-Container aus. b. Wählen Sie den Zielspeic her aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Wählen Sie das Migrationsprofil aus. d. Wählen Sie den Zielordner aus. 7. Um den Migrationsprozess zu starten, wählen Sie Go. HCX validiert Ihre VM-Auswahl, bevor die Migration beginnt. Weitere Informationen finden Sie unter Migration virtueller Maschinen mit Mobilitätsgruppen und Überwachung und Schätzung der Migration mit Mobilitätsgruppen in der VMware-Dokumentation.	

Zugehörige Ressourcen

VMware-Dokumentation:

- Benutzerhandbuch für VMware HCX
- Installieren Sie die Checkliste B — HCX mit einer VMC SDDC-Zielumgebung
- VMware HCX in der VMware Cloud on AWS
- HCX OS unterstützte Migration für VMware Cloud on AWS
- Versionshinweise zu VMware HCX 4.2.1

Senden Sie mithilfe von VMware Aria Operations for Logs Logs von VMware Cloud on AWS an Splunk

Erstellt von Deepak Kumar (AWS) und Piotr Pitera (AWS)

Umgebung: Produktion	Quelle: Protokolle und Ereignisse von VMware Cloud on AWS	Ziel: Lokaler Splunk-Endpunkt
R-Typ: Umziehen	Arbeitslast: Alle anderen Workloads	Technologien: Hybrid Cloud; Infrastruktur; Migration
AWS-Services: VMware Cloud auf AWS		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie AWS Ereignisse oder Protokolle von VMware Cloud mithilfe von VMware Aria Operations for Logs an ein Syslog oder einen HTTP-Endpunkt wie Splunk weitergeleitet werden.

VMware Aria Operations for Logs ist ein Tool zur Protokollanalyse, das eine verbesserte Transparenz und eine beschleunigte Fehlerbehebung in der VMware Cloud on-Umgebung bietet. AWS Sie können dieses Tool so konfigurieren, dass entweder alle oder ein Teil der Protokolle oder Ereignisse in VMware Cloud AWS an einen Syslog- oder HTTP-Endpunkt gesendet werden. Der Endpunkt kann entweder ein Software-as-a-Service (SaaS) -Endpunkt oder ein lokaler Endpunkt wie Splunk sein. (Dieses Muster enthält die Anweisungen für Splunk.) Weitere Informationen zu VMware Aria Operations for Logs finden Sie in der VMware-Dokumentation.

VMware Cloud on AWS ist ein pay-as-you-go (On-Demand-) Service, der es Unternehmen jeder Größe ermöglicht, Workloads in VMware vSphere-basierten Cloud-Umgebungen auszuführen, indem

sie eine Vielzahl von verwenden. AWS-Services Sie können mit mindestens 2 Hosts pro SDDC-Cluster (Software-Defined Data Center) beginnen und in Ihrer Produktionsumgebung auf bis zu 16 Hosts pro Cluster skalieren. Weitere Informationen finden Sie auf der Website von VMware Cloud. AWS Weitere Informationen zu SDDCs finden Sie unter About Software-Defined Data Centers in der VMware-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Splunk, vor Ort konfiguriert

Einschränkungen

Sie können sich für ein kostenloses Testabonnement für VMware Aria Operations for Logs registrieren. Dieses Abonnement ist 30 Tage gültig und hat die folgenden Einschränkungen:

- Maximale Größe der Protokolle, die Sie weiterleiten können: 50 GB Protokolle pro Tag
- Maximale Anzahl von Konfigurationen für die Protokollweiterleitung, die Sie erstellen können: 10
- Maximale Anzahl von Konfigurationen für die Protokollweiterleitung, die Sie aktivieren können: 5

Um auf alle Servicefunktionen zugreifen zu können, müssen Sie ein Upgrade auf ein Premium-Abonnement durchführen.

Weitere Informationen zu Test- und Premium-Abonnements finden Sie unter VMware Aria Operations for Logs (SaaS) Subscriptions and Billing in der VMware-Dokumentation. Weitere Informationen zu Nutzungsbeschränkungen finden Sie unter Nutzungsbeschränkungen für Funktionen in der VMware-Dokumentation.

Produktversionen

- VMware Cloud auf AWS SDDC Version 1.24
- VMware Aria Operations for Logs Version 8.10
- Lokale Version 9.x von Splunk

Architektur

Quelltechnologie-Stack

- VMware Cloud auf AWS
- VMware Aria Operations for Logs

Zieltechnologie-Stack

- Splunk vor Ort

Zielarchitektur

Das folgende Diagramm zeigt die Konnektivität zwischen einem Unternehmensrechenzentrum und VMware Aria Operations for Logs in VMware Cloud on AWS.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von VMware AWS und VMware entwickelt wurde.
- VMware Aria Operations for Logs ist ein Tool zur Protokollanalyse und Fehlerbehebung für VMware Cloud on AWS.

Epen

Stellen Sie ein SDDC bereit und aktivieren Sie VMware Aria Operation for Logs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine VMware Cloud auf AWS SDDC bereit.	Folgen Sie den Anweisung en unter Bereitstellen eines VMware SDDC auf mithilfe AWS von VMware Cloud on AWS in Prescriptive Guidance. AWS	Cloud-Architekt, Cloud-Adm inistrator
Melden Sie sich für VMware Aria Operations for Logs an.	Anweisungen finden Sie in der VMware-Dokumentation.	Cloud-Architekt

Stellen Sie einen Cloud-Proxy bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen Cloud-Proxy bereit.	Um Logs an eine lokale Instanz von Splunk weiterzul eiten, müssen Sie einen Cloud-Proxy für VMware Aria Operations for Logs hinzufüge n. Dieser Proxy empfängt Informationen vom lokalen Rechenzentrum und sendet sie zur Analyse an VMware Aria Operations for Logs. So laden Sie den Cloud-Proxy herunter und installieren ihn: 1. Stellen Sie sicher, dass die Ports 443, 22 und 514 zwischen Ihrer lokalen Umgebung und VMware Cloud on geöffnet sind. AWS Für zusätzliche Ports können Sie 1514/TCP oder 6514/TCP verwenden . Weitere Informationen zu Ports finden Sie unter VMware Aria Operations for Logs Firewall-Empfehlun gen in der VMware-Do kumentation. 2. Melden Sie sich bei VMware Aria Operation s an, um Protokolle zu erhalten.	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie auf der Startseite im Widget Add Collector aus. 4. Kopieren Sie auf dem Bildschirm Cloud Proxy Virtual Appliance den Token-Schlüssel. Sie müssen diesen Schlüssel innerhalb von 24 Stunden verwenden, um die folgenden Schritte abzuschließen. 5. Wählen Sie den Download-Link für die OVA-Datei. 6. Navigieren Sie zum VMware vSphere Web Client, wählen Sie Ihren Cluster aus und wählen Sie dann OVF-Vorlage bereitstellen aus. 7. Wenn Sie zur Eingabe des Schlüssels aufgefordert werden, fügen Sie den Token-Schlüssel ein, den Sie in Schritt 4 kopiert haben. 8. Wählen Sie Fertig stellen, um den Cloud-Proxy zu installieren.	

Leiten Sie Logs an einen lokalen Splunk-Endpunkt weiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Protokollweiterleitung.	Um Logs an den Splunk-Endpunkt weiterzuleiten: 1. Melden Sie sich bei VMware Aria Operations an, um Protokolle zu erhalten. 2. Navigieren Sie zu Log Management. 3. Wählen Sie Log Forwarding. 4. Wählen Sie Neue Konfiguration und nehmen Sie die folgenden Einstellungen vor: • Geben Sie einen Namen für die Konfiguration der Protokollweiterleitung ein. • Wählen Sie als Ziel die Option On Premises aus. • Wählen Sie für Cloud Proxy den Cloud-Proxy aus, den Sie zuvor installiert haben. • Wählen Sie als Endpunkttyp die Option TCP aus. • Geben Sie für Endpunkt-URL Ihre lokale Splunk-URL im folgenden Format ein:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`tcp://x.x.x.x (your Splunk IP address): 514` • (Optional) Für Tags können Sie Tag-Namen und -Werte angeben, um das Abfragen zu erleichtern. • Wählen Sie „Auf alle Protokolle anwenden“ oder „Auf bestimmte Protokolle anwenden“. Wenn Sie alle VMware Cloud on AWS AWS-Logs an Splunk senden möchten, wählen Sie Apply to all logs. 5. Wählen Sie Überprüfen. 6. Wählen Sie Speichern. Weitere Informationen finden Sie unter Protokolle von VMware Aria Operations weiterleiten in der VMware-Dokumentation.	

Zugehörige Ressourcen

- VMware Cloud auf der AWS Website
- Über softwaredefinierte Rechenzentren (VMware-Dokumentation)
- Stellen Sie mithilfe AWS von VMware Cloud on ein VMware-SDDC bereit AWS(AWS Prescriptive Guidance)

- Migrieren Sie Workloads mithilfe AWS von VMware HCX (Prescriptive Guidance) auf die VMware CloudAWS
- Konfigurieren Sie eine Rechenzentrumserweiterung auf VMware Cloud AWS unter Verwendung des Hybrid Linked Mode (Prescriptive Guidance)AWS

Einrichten einer CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere mithilfe von AWS CDK und GitLab

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

Code-Repository: – amazon-ecs-anywhere-cicdpipeline-cdk-sample	Umgebung: PoC oder Pilotprojekt	Technologien: Hybrid Cloud; Container und Microservices; Infrastruktur; DevOps
Workload: Open-Source	AWS-Services: AWS CDK; AWS CodePipeline; Amazon ECS; AWS Systems Manager ; AWS CodeCommit	

Übersicht

Amazon ECS Anywhere ist eine Erweiterung des Amazon Elastic Container Service (Amazon ECS). Es bietet Unterstützung für die Registrierung einer externen Instance, z. B. eines On-Premises-Servers oder einer virtuellen Maschine (VM), in Ihrem Amazon-ECS-Cluster. ist eine Funktion, die dazu beiträgt, Kosten zu senken und komplexe lokale Container-Orchestrierung und -Vorgänge zu minimieren. Sie können ECS Anywhere verwenden, um Container-Anwendungen sowohl in On-Premises- als auch in Cloud-Umgebungen bereitzustellen und auszuführen. Dadurch entfällt die Notwendigkeit, dass Ihr Team mehrere Domains und Fähigkeiten erlernt oder komplexe Software selbst verwaltet.

Dieses Muster beschreibt einen step-by-step Ansatz zur Bereitstellung eines Amazon-ECS-Clusters mit Amazon ECS Anywhere-Instances mithilfe von Amazon Web Services (AWS) Cloud Development Kit (AWS CDK)-Stacks. Anschließend verwenden Sie AWS CodePipeline , um eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) einzurichten. Anschließend replizieren Sie Ihr GitLab Code-Repository in AWS CodeCommit und stellen Ihre containerisierte Anwendung auf dem Amazon-ECS-Cluster bereit.

Dieses Muster soll denjenigen helfen, die On-Premises-Infrastruktur verwenden, um Container-Anwendungen auszuführen und GitLab zur Verwaltung der Anwendungscodebasis zu verwenden. Sie können diese Workloads mithilfe von AWS Cloud-Services verwalten, ohne Ihre vorhandene On-Premises-Infrastruktur zu stören.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Containeranwendung, die auf einer On-Premises-Infrastruktur ausgeführt wird.
- Ein GitLab Repository, in dem Sie Ihre Anwendungscodebasis verwalten. Weitere Informationen finden Sie unter Repository (GitLab).
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren oder Aktualisieren der neuesten Version der AWS CLI (AWS CLI-Dokumentation).
- AWS CDK Toolkit, global installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren des AWS-CDK (AWS-CDK-Dokumentation).
- npm, installiert und konfiguriert für das AWS-CDK in TypeScript. Weitere Informationen finden Sie unter Herunterladen und Installieren von Node.js und npm (npm-Dokumentation).

Einschränkungen

- Einschränkungen und Überlegungen finden Sie unter Externe Instances (Amazon ECS Anywhere) in der Amazon-ECS-Dokumentation.

Produktversionen

- AWS CDK Toolkit Version 2.27.0 oder höher
- npm Version 7.20.3 oder höher
- Node.js Version 16.6.1 oder höher

Architektur

Zieltechnologie-Stack

- AWS-CDK
- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit

- AWS CodePipeline
- Amazon ECS Anywhere
- Amazon Elastic Container Registry (Amazon ECR)
- AWS Identity and Access Management (IAM)
- AWS System Manager
- GitLab -Repository

Zielarchitektur

Dieses Diagramm stellt zwei primäre Workflows dar, die in diesem Muster beschrieben werden: die Bereitstellung des Amazon-ECS-Clusters und die Einrichtung der CI/CD-Pipeline, die die CI/CD-Pipeline einrichtet und bereitstellt, wie folgt:

1. Bereitstellen des Amazon-ECS-Clusters
   a. Wenn Sie den ersten AWS-CDK-Stack bereitstellen, wird ein CloudFormation Stack auf AWS erstellt.
   b. Dieser CloudFormation Stack stellt einen Amazon ECS-Cluster und zugehörige AWS-Ressourcen bereit.
   c. Um eine externe Instance bei einem Amazon ECS-Cluster zu registrieren, müssen Sie AWS Systems Manager Agent (SSM Agent) auf Ihrer VM installieren und die VM als von AWS Systems Manager verwaltete Instance registrieren.
   d. Sie müssen auch den Amazon-ECS-Container-Agenten und Docker auf Ihrer VM installieren, um ihn als externe Instance beim Amazon-ECS-Cluster zu registrieren.
   e. Wenn die externe Instance beim Amazon-ECS-Cluster registriert und konfiguriert ist, kann sie mehrere Container auf Ihrer VM ausführen, die als externe Instance registriert ist.
   f. Der Amazon-ECS-Cluster ist aktiv und kann die Anwendungs-Workloads über Container ausführen. Die Amazon ECS Anywhere-Container-Instance wird in einer On-Premises-Umgebung ausgeführt, ist aber dem Amazon-ECS-Cluster in der Cloud zugeordnet.
2. Einrichten und Bereitstellen der CI/CD-Pipeline
   a. Wenn Sie den zweiten AWS-CDK-Stack bereitstellen, wird ein weiterer CloudFormation Stack auf AWS erstellt.
   b. Dieser CloudFormation Stack stellt eine Pipeline in CodePipeline und verwandten AWS-Ressourcen bereit.

c. Sie übertragen Änderungen am Anwendungscode per Push und führen sie in ein On-Premises-GitLab Repository zusammen.

d. Das GitLab Repository wird automatisch in das CodeCommit Repository repliziert.

e. Die Aktualisierungen des CodeCommit Repositorys starten automatisch CodePipeline.

f. CodePipeline kopiert Code aus CodeCommit und erstellt den Build für bereitstellbare Anwendungen in CodeBuild.

g. CodePipeline erstellt ein Docker-Image der CodeBuild Build-Umgebung und überträgt es an das Amazon ECR-Repo.

h. CodePipeline initiiert CodeDeploy Aktionen, die das Container-Image aus dem Amazon ECR-Repo abrufen.

i. CodePipeline stellt das Container-Image auf dem Amazon-ECS-Cluster bereit.

Automatisierung und Skalierung

Dieses Muster verwendet das AWS-CDK als Infrastructure as Code (IaC)-Tool, um diese Architektur zu konfigurieren und bereitzustellen. AWS CDK hilft Ihnen, die AWS-Ressourcen zu orchestrieren und Amazon ECS Anywhere und die CI/CD-Pipeline einzurichten.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht. Dieses Muster verwendet auch Amazon ECS Anywhere, das Unterstützung für die Registrierung eines On-Premises-Servers oder einer VM in Ihrem Amazon-ECS-Cluster bietet.

Andere Tools

- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js-Umgebung ausgeführt wird und verwendet wird, um Pakete freizugeben oder zu leihen und die Bereitstellung privater Pakete zu verwalten.
- Vagrant ist ein Open-Source-Dienstprogramm für die Erstellung und Wartung portabler virtueller Softwareentwicklungsumgebungen. Zu Demonstrationszwecken verwendet dieses Muster Vagrant, um eine On-Premises-VM zu erstellen.

Code-Repository

Der Code für dieses Muster ist in der GitHub CI/CD-Pipeline für Amazon ECS Anywhere unter Verwendung des AWS-CDK-Repositorys verfügbar.

Bewährte Methoden

Beachten Sie bei der Bereitstellung dieses Musters die folgenden bewährten Methoden:

- Bewährte Methoden für die Entwicklung und Bereitstellung einer Cloud-Infrastruktur mit dem AWS-CDK
- Bewährte Methoden für die Entwicklung von Cloud-Anwendungen mit AWS CDK (AWS-Blogbeitrag)

Polen

Überprüfen der AWS-CDK-Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-CDK-Version.	Überprüfen Sie die Version des AWS CDK Toolkits, indem	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den folgenden Befehl eingeben. `cdk --version` Dieses Muster erfordert Version 2.27.0 oder höher. Wenn Sie eine frühere Version haben, folgen Sie den Anweisungen in der AWS-CDK-Dokumentation, um sie zu aktualisieren.	
Überprüfen Sie die npm-Version.	Überprüfen Sie die Version von npm, indem Sie den folgenden Befehl eingeben. `npm --version` Dieses Muster erfordert Version 7.20.3 oder höher. Wenn Sie eine frühere Version haben, folgen Sie den Anweisungen in der npm-Dokumentation, um sie zu aktualisieren.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie AWS-Anmeldeinformationen ein.	Richten Sie AWS-Anmeldeinformationen ein, indem Sie den `aws configure` Befehl eingeben und den Anweisungen folgen.
	
	`$aws configure`
	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`
		DevOps Techniker

Bootstrapping der AWS-CDK-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das AWS-CDK-Code-Repository.	1. Klonen Sie die CI/CD-Pipeline für Amazon ECS Anywhere mithilfe des AWS-CDK-Repositorys für dieses Muster, indem Sie den folgenden Befehl eingeben. `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cicd-pipeline-cdk-sample.git`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Navigieren Sie in das geklonte Verzeichnis, indem Sie den folgenden Befehl eingeben. `cd amazon-ecs-anywhere-cicd-pipeline-cdk-sample`	
Bootstrappen Sie die Umgebung.	Stellen Sie die CloudFormation Vorlage für das Konto und die AWS-Region bereit, die Sie verwenden möchten, indem Sie den folgenden Befehl eingeben. `cdk bootstrap <account-number>/<Region>` Weitere Informationen finden Sie unter Bootstrapping in der AWS-CDK-Dokumentation.	DevOps Techniker

Erstellen und Bereitstellen der Infrastruktur für Amazon ECS Anywhere

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien.	Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien, indem Sie die folgenden Befehle eingeben.
	`$cd EcsAnywhereCdk`
	`$npm install`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$npm fund` Mit diesen Befehlen werden alle Pakete aus dem Beispiel-Repository installiert. Weitere Informationen finden Sie unter npm ci und npm install in der npm-Dokumentation. Wenn Sie bei der Eingabe dieser Befehle Fehler zu fehlenden Paketen erhalten, lesen Sie den Abschnitt Fehlerbehebung dieses Musters.	
Erstellen Sie das Projekt.	Geben Sie den folgenden Befehl ein, um den Projektcode zu erstellen. `npm run build` Weitere Informationen zum Erstellen und Bereitstellen des Projekts finden Sie unter Ihre erste AWS-CDK-App in der AWS-CDK-Dokumentation.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Infrastruktur-Stack von Amazon ECS Anywhere bereit.	1. Listen Sie die Stacks auf, indem Sie den folgenden Befehl eingeben.
	`$cdk list`
	2. Bestätigen Sie, dass die Ausgabe die `ECSAnywherePipelineStack` Stacks `EcsAnywhereInfraStack` und zurückgibt.
	3. Stellen Sie den `EcsAnywhereInfraStack` Stack bereit, indem Sie den folgenden Befehl eingeben.
	`$cdk deploy EcsAnywhereInfraStack`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Stack-Erstellung und -Ausgabe.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Wählen Sie auf der Seite Stacks den `EcsAnywhereInfraStack` Stack aus. 3. Vergewissern Sie sich, dass der Stack-Status entweder `CREATE_IN_PROGRESS` oder ist`CREATE_COMPLETE` . Die Einrichtung des Amazon-ECS-Clusters kann einige Zeit dauern. Fahren Sie erst fort, wenn die Stack-Erstellung abgeschlossen ist.	DevOps Techniker

Einrichten einer On-Premises-VM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Ihre VM ein.	Erstellen Sie eine Vagrant-VM, indem Sie den `vagrant up` Befehl aus dem Stammverzeichnis eingeben, in dem sich Vagrantfile befindet. Weitere	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie in der Vagrant-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie Ihre VM als externe Instance.	1. Melden Sie sich mit dem `vagrant ssh` Befehl bei der Vagrant-VM an. Weitere Informationen finden Sie in der Vagrant-Dokumentation. 2. Installieren Sie AWS CLI auf der VM, indem Sie die AWS CLI-Installationsanweisungen befolgen und die folgenden Befehle eingeben. `$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" \ > -o "awscliv2.zip" $sudo apt install unzip $unzip awscliv2.zip $sudo ./aws/install $aws configure AWS Access Key ID [None]: <your-access-key-ID> AWS Secret Access Key [None]: <your-secret-access-key> Default region name [None]: <your-Region-name> Default output format [None]:` 1. Erstellen Sie einen Aktivierungscode und eine ID, mit	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	der Sie Ihre VM bei AWS Systems Manager registrieren und Ihre externe Instance aktivieren können. Die Ausgabe dieses Befehls enthält die Aktivierungs-ID und die Werte des Aktivierungscodes.
	`aws ssm create-activation \ > --iam-role EcsAnywhereInstanceRole \ > | tee ssm-activation.json`
	Wenn Sie beim Ausführen dieses Befehls eine Fehlermeldung erhalten, lesen Sie den Abschnitt Fehlerbehebung.
	2. Exportieren Sie die Aktivierungs-ID und die Codewerte.
	`export ACTIVATION_ID=<activation-ID> export ACTIVATION_CODE=<activation-code>`
	3. Laden Sie das Installationsskript auf Ihre VM herunter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`curl --proto "https" -o "ecs-anywhere-install.sh" \ > "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh"`
	4. Führen Sie das Installationsskript auf Ihrer VM aus.
	`sudo bash ecs-anywhere-install.sh \ --cluster EcsAnywhereCluster \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <region-name>`
	Dadurch wird Ihre VM als externe Amazon ECS Anywhere-Instance eingerichtet und die Instance im Amazon-ECS-Cluster registriert. Weitere Informationen finden Sie unter Registrieren einer externen Instance in einem Cluster in der Amazon-ECS-Dokumentation. Wenn Probleme auftreten, lesen Sie den Abschnitt Fehlerbehebung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie den Status von Amazon ECS Anywhere und der externen VM.	Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Ihre VM mit der Amazon-EC S-Steuerebene verbunden ist und läuft.
	`$aws ssm describe-instance-information`
	`$aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps Techniker

Bereitstellen der CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Verzweigung im CodeCommit Repo.	Erstellen Sie eine Verzweigung mit dem Namen `main` im CodeCommit Repository, indem Sie den ersten Commit für das Repository erstellen. Sie können der AWS-Dokumentation folgen, um einen Commit in zu erstellen CodeCommit. Nachfolgend finden Sie einen Beispielbefehl. `aws codecommit put-file \ --repository-name EcsAnywhereRepo \ --branch-name main \ --file-path README.md \`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--file-content "Test" \ --name "Dev Ops" \ --email "devops@example.com" \ --commit-message "Adding README."`	
Richten Sie die Repo-Spiegelung ein.	Sie können ein GitLab Repository zu und von externen Quellen spiegeln. Sie können auswählen, welches Repository als Quelle dient. Verzweigungen, Tags und Commits werden automatisch synchronisiert. Richten Sie einen Push-Spiegel zwischen dem GitLab Repository, das Ihre Anwendung hostet, und dem CodeCommit Repository ein. Anweisungen finden Sie unter Einrichten eines Push-Spiegels von GitLab zu CodeCommit (GitLab Dokumentation). Hinweis: Standardmäßig synchronisiert die Spiegelung das Repository automatisch. Wenn Sie die Repositorys manuell aktualisieren möchten, finden Sie weitere Informationen unter Aktualisieren eines Spiegels (GitLab Dokumentation).	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CI/CD-Pipeline-Stack bereit.	Stellen Sie den `EcsAnywherePipelineStack` Stack bereit, indem Sie den folgenden Befehl eingeben. `$cdk deploy EcsAnywherePipelineStack`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die CI/CD-Pipeline.	1. Nehmen Sie Änderungen am Anwendungscode vor und übertragen Sie ihn an das On-Premises-Quell- GitLab Repository. Weitere Informationen finden Sie unter Push-Optionen (GitLab Dokumentation). Bearbeiten Sie beispielsweise die `-../application/index.html` Datei, um den Wert der Anwendungsversion zu aktualisieren. 2. Wenn der Code in das CodeCommit Repo repliziert wird, wird die CI/CD-Pipeline gestartet. Führen Sie eine der folgenden Aktionen aus: • Wenn Sie die automatische Spiegelung verwenden, um das GitLab Repo mit dem CodeCommit Repo zu synchronisieren, fahren Sie mit dem nächsten Schritt fort. • Wenn Sie die manuelle Spiegelung verwenden, übertragen Sie die Änderungen des Anwendungscodes in das CodeCommit	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repo, indem Sie den Anweisungen unter Spiegel aktualisieren (GitLab Dokumentation) folgen. 3. Geben Sie auf Ihrem lokalen Computer in einem Webbrowser http://localhost:80 ein. Dadurch wird die NGINX-Webseite geöffnet, da Port 80 in Vagrantfile an localhost weitergeleitet wird. Vergewissern Sie sich, dass Sie den aktualisierten Anwendungsversionswert anzeigen können. Dadurch wird die Pipeline- und Image-Bereitstellung validiert. 4. (Optional) Wenn Sie die Bereitstellung in der AWS-Managementkonsole überprüfen möchten, gehen Sie wie folgt vor: a. Öffnen Sie die Amazon-ECS-Konsole unter https://console.aws.amazon.com/ecs/. b. Wählen Sie die zu verwendende Region in der Navigationsleiste aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Klicken Sie im Navigationsbereich auf Cluster. d. Wählen Sie auf der Seite Cluster den EcsAnywhereCluster Cluster aus. e. Wählen Sie Aufgabendefinitionen aus. f. Vergewissern Sie sich, dass der Container ausgeführt wird.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen und löschen Sie die Ressourcen.	Nachdem Sie dieses Muster durchgegangen sind, sollten Sie die von Ihnen erstellten proof-of-concept Ressourcen entfernen. Geben Sie zum Bereinigen die folgenden Befehle ein.
	`$cdk destroy EcsAnywherePipelineStack`
	`$cdk destroy EcsAnywhereInfraStack`
		DevOps Techniker

Fehlerbehebung

Problem	Lösung

Fehler bei fehlenden Paketen bei der Installation von Paketabhängigkeiten.	Geben Sie einen der folgenden Befehle ein, um fehlende Pakete aufzulösen.
	`$npm ci`
	or
	`$npm install -g @aws-cdk/<package_name>`

Wenn Sie den `aws ssm create-activation` Befehl auf der VM ausführen, erhalten Sie den folgenden Fehler. `An error occurred (ValidationException) when calling the CreateActivation operation: Nonexistent role or missing ssm service principal in trust policy: arn:aws:iam::000000000000:role/EcsAnywhereInstanceRole`	Der `EcsAnywhereInfraStack` Stack ist nicht vollständig bereitgestellt, und die IAM-Rolle, die zum Ausführen dieses Befehls erforderlich ist, wurde noch nicht erstellt. Überprüfen Sie den Stack-Status in der CloudFormation Konsole. Wiederholen Sie den Befehl, nachdem sich der Status in geändert hat`CREATE_COMPLETE` .

Eine Amazon-ECS-Zustandsprüfung gibt zurück`UNHEALTHY` , und im Abschnitt Services des Clusters in der Amazon-ECS-Konsole wird der folgende Fehler angezeigt.
`service EcsAnywhereService was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster.`
	Starten Sie den Amazon-ECS-Agenten auf Ihrer Vagrant-VM neu, indem Sie die folgenden Befehle eingeben.
	`$vagrant ssh`
	`$sudo systemctl restart ecs`
	`$sudo systemctl status ecs`

Zugehörige Ressourcen

- Amazon ECS Anywhere-Marketingseite
- Dokumentation zu Amazon ECS Anywhere
- Amazon ECS Anywhere-Demo (Video)
- Workshop-Beispiele für Amazon ECS Anywhere (GitHub)
- Repository-Spiegelung (GitLab Dokumentation)

Mehr Muster

- Automatisieren der Einrichtung von regionsübergreifendem Peering mit AWS Transit Gateway
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- Migrieren Sie Hadoop-Daten mithilfe von LiveData WANdisco Migrator zu Amazon S3
- Migrieren Sie VMware-VMs mit HCX Automation mithilfe von PowerCLI
- Migrieren Sie Workloads mithilfe von VMware HCX zur VMware Cloud on AWS
- Ändern von HTTP-Headern bei der Migration von F5 zu einem Application Load Balancer in AWS
- ???
- Verwenden Sie Bol Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren
- Verwenden von Serverspec für die testgesteuerte Entwicklung von Infrastrukturcode

Infrastruktur

Themen

- Lokales Validieren des Codes Account Factory für Terraform (AFT)
- Mehr Muster

Zugreifen auf einen Bastion-Host mithilfe von Session Manager und Amazon EC2 Instance Connect

Erstellt von Piotr Chotkowski (AWS) und Witold Kowalik (AWS)

Code-Repository: Zugreifen auf einen Bastion-Host mithilfe von Session Manager und Amazon EC2 Instance Connect	Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; Cloudnativ; Sicherheit, Identität, Compliance; Netzwerk
AWS-Services: Amazon EC2; AWS Systems Manager; Amazon VPC		

Übersicht

Ein Bastion-Host, der manchmal als Jumpbox bezeichnet wird, ist ein Server, der einen einzigen Zugriffspunkt von einem externen Netzwerk auf die Ressourcen in einem privaten Netzwerk bietet. Ein Server, der einem externen öffentlichen Netzwerk wie dem Internet ausgesetzt ist, stellt ein potenzielles Sicherheitsrisiko für unbefugten Zugriff dar. Es ist wichtig, den Zugriff auf diese Server zu sichern und zu kontrollieren.

Dieses Muster beschreibt, wie Sie Session Manager und Amazon EC2 Instance Connect verwenden können, um eine sichere Verbindung zu einem Amazon Elastic Compute Cloud (Amazon EC2)-Bastion-Host herzustellen, der in Ihrem AWS-Konto bereitgestellt wird. Session Manager ist eine Funktion von AWS Systems Manager . Zu den Vorteilen dieses Musters gehören:

- Der bereitgestellte Bastion-Host hat keine offenen, eingehenden Ports, die dem öffentlichen Internet zugänglich gemacht werden. Dadurch wird die potenzielle Angriffsfläche reduziert.
- Sie müssen keine langfristigen Secure Shell (SSH)-Schlüssel in Ihrem AWS-Konto speichern und verwalten. Stattdessen generiert jeder Benutzer bei jeder Verbindung mit dem Bastion-Host ein neues SSH-Schlüsselpaar. AWS Identity and Access Management (IAM)-Richtlinien, die den AWS-Anmeldeinformationen des Benutzers zugeordnet sind, steuern den Zugriff auf den Bastion-Host.

Zielgruppe

Dieses Muster richtet sich an Leser, die Erfahrung mit grundlegendem Verständnis von Amazon EC2, Amazon Virtual Private Cloud (VPC) und Hashicorp Terraform haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2, installiert und konfiguriert
- Session Manager-Plugin für die AWS CLI, installiert
- Terraform-CLI, installiert
- Speicher für den Terraform-Status , z. B. ein Amazon Simple Storage Service (Amazon S3)-Bucket und eine Amazon DynamoDB-Tabelle, die als Remote-Backend zum Speichern des Terraform-Status dient. Weitere Informationen zur Verwendung von Remote-Backends für den Terraform-Status finden Sie unter S3-Backends (Terraform-Dokumentation). Ein Codebeispiel, das die Remote-Statusverwaltung mit einem S3-Backend einrichtet, finden Sie unter remote-state-s3-Backend (Terraform Registry). Beachten Sie die folgenden Voraussetzungen:
  - Der S3-Bucket und die DynamoDB-Tabelle müssen sich in derselben AWS-Region befinden.
  - Beim Erstellen der DynamoDB-Tabelle muss der Partitionsschlüssel `LockID` (wobei die Groß- und Kleinschreibung beachtet werden muss) und der Partitionsschlüsseltyp sein`String`. Alle anderen Tabelleneinstellungen müssen ihre Standardwerte haben. Weitere Informationen finden Sie unter Informationen zu Primärschlüsseln und Erstellen einer Tabelle in der DynamoDB-Dokumentation.
- Ein SSH-Client, installiert

Einschränkungen

- Dieses Muster ist als Machbarkeitsnachweis (PoC) oder als Grundlage für die weitere Entwicklung gedacht. Es sollte nicht in seiner aktuellen Form in Produktionsumgebungen verwendet werden. Passen Sie vor der Bereitstellung den Beispielcode im Repository an Ihre Anforderungen und Ihren Anwendungsfall an.
- Bei diesem Muster wird davon ausgegangen, dass der Ziel-Bastion-Host Amazon Linux 2 als Betriebssystem verwendet. Es ist zwar möglich, andere Amazon Machine Images (AMIs) zu verwenden, aber andere Betriebssysteme liegen für dieses Muster außerhalb des Bereichs.

- In diesem Muster befindet sich der Bastion-Host in einem privaten Subnetz ohne NAT-Gateway und Internet-Gateway. Dieses Design isoliert die EC2-Instance vom öffentlichen Internet. Sie können eine bestimmte Netzwerkkonfiguration hinzufügen, die es ihr ermöglicht, mit dem Internet zu kommunizieren. Weitere Informationen finden Sie unter Verbinden Ihrer Virtual Private Cloud (VPC) mit anderen Netzwerken in der Amazon-VPC-Dokumentation. Entsprechend hat der Bastion-Host nach dem Prinzip der geringsten Berechtigung keinen Zugriff auf andere Ressourcen in Ihrem AWS-Konto, es sei denn, Sie erteilen explizit Berechtigungen. Weitere Informationen finden Sie unter Ressourcenbasierte Richtlinien in der IAM-Dokumentation.

Produktversionen

- AWS CLI Version 2
- Terraform Version 1.3.9

Architektur

Zieltechnologie-Stack

- Eine VPC mit einem einzelnen privaten Subnetz
- Die folgenden Schnittstellen-VPC-Endpunkte:
  - `amazonaws.<region>.ssm` – Der Endpunkt für den Systems-Manager-Service.
  - `amazonaws.<region>.ec2messages` – Systems Manager verwendet diesen Endpunkt, um Aufrufe vom SSM Agent an den Systems Manager-Service zu tätigen.
  - `amazonaws.<region>.ssmmessages` – Session Manager verwendet diesen Endpunkt, um über einen sicheren Datenkanal eine Verbindung zu Ihrer EC2-Instance herzustellen.
- Eine `t3.nano` EC2-Instance, auf der Amazon Linux 2 ausgeführt wird
- IAM-Rolle und Instance-Profil
- Amazon-VPC-Sicherheitsgruppen und Sicherheitsgruppenregeln für die Endpunkte und EC2-Instance

Zielarchitektur

Das Diagramm zeigt den folgenden Prozess:

1. Der Benutzer übernimmt eine IAM-Rolle, die über Berechtigungen für Folgendes verfügt:
   - Authentifizieren, Autorisieren und Herstellen einer Verbindung mit der EC2-Instance
   - Starten einer Sitzung mit Session Manager
2. Der Benutzer initiiert eine SSH-Sitzung über Session Manager.
3. Session Manager authentifiziert den Benutzer, überprüft die Berechtigungen in den zugehörigen IAM-Richtlinien, überprüft die Konfigurationseinstellungen und sendet eine Nachricht an SSM Agent, um eine bidirektionale Verbindung zu öffnen.
4. Der Benutzer überträgt den öffentlichen SSH-Schlüssel über Amazon EC2Metadaten an den Bastion-Host. Dies muss vor jeder Verbindung erfolgen. Der öffentliche SSH-Schlüssel bleibt 60 Sekunden lang verfügbar.
5. Der Bastion-Host kommuniziert mit den Schnittstellen-VPC-Endpunkten für Systems Manager und Amazon EC2.
6. Der Benutzer greift über Session Manager über einen mit TLS 1.2 verschlüsselten bidirektionalen Kommunikationskanal auf den Bastion-Host zu.

Automatisierung und Skalierung

Die folgenden Optionen sind verfügbar, um die Bereitstellung zu automatisieren oder diese Architektur zu skalieren:

- Sie können die Architektur über eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) bereitstellen.
- Sie können den Code ändern, um den Instance-Typ des Bastion-Hosts zu ändern.
- Sie können den Code ändern, um mehrere Bastion-Hosts bereitzustellen. Fügen Sie in der `bastion-host/main.tf` Datei im `aws_instance` Ressourcenblock das `count` Meta-Argument hinzu. Weitere Informationen finden Sie in der Terraform-Dokumentation.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang. Dieses Muster verwendet Session Manger, eine Funktion von Systems Manager.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Andere Tools

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit dem Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können. Dieses Muster verwendet die Terraform-CLI .

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Zugreifen auf einen Bastion-Host mithilfe von Session Manager und Amazon EC2 Instance Connect verfügbar.

Bewährte Methoden

- Wir empfehlen die Verwendung automatisierter Code-Scan-Tools, um die Sicherheit und Qualität des Codes zu verbessern. Dieses Muster wurde mithilfe von Checkov, einem statischen Code-Ressource-Tool für IaC, gescannt. Wir empfehlen Ihnen, mindestens grundlegende Validierungs- und Formatierungsprüfungen durchzuführen, indem Sie die `terraform fmt -check -recursive` Terraform-Befehle `terraform validate` und verwenden.
- Es hat sich bewährt, automatisierte Tests für IaC hinzuzufügen. Weitere Informationen zu den verschiedenen Ansätzen zum Testen von Terraform-Code finden Sie unter Testen von HashiCorp Terraform (Terraform-Blogbeitrag).

- Während der Bereitstellung ersetzt Terraform die EC2-Instance jedes Mal, wenn eine neue Version des Amazon Linux 2-AMI erkannt wird. Dadurch wird die neue Version des Betriebssystems bereitgestellt, einschließlich Patches und Upgrades. Wenn der Bereitstellungsplan selten ist, kann dies ein Sicherheitsrisiko darstellen, da die Instance nicht über die neuesten Patches verfügt. Es ist wichtig, Sicherheitspatches häufig zu aktualisieren und auf bereitgestellte EC2-Instances anzuwenden. Weitere Informationen finden Sie unter Update-Verwaltung in Amazon EC2.
- Da dieses Muster ein Machbarkeitsnachweis ist, verwendet es von AWS verwaltete Richtlinien, wie z. B. `AmazonSSMManagedInstanceCore`. Von AWS verwaltete Richtlinien decken häufige Anwendungsfälle ab, gewähren jedoch keine Berechtigungen mit den geringsten Rechten. Wir empfehlen Ihnen, nach Bedarf benutzerdefinierte Richtlinien zu erstellen, die geringste Berechtigungen für die in dieser Architektur bereitgestellten Ressourcen gewähren. Weitere Informationen finden Sie unter Erste Schritte mit von AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen.
- Verwenden Sie ein Passwort, um den Zugriff auf SSH-Schlüssel zu schützen und Schlüssel an einem sicheren Ort zu speichern.
- Richten Sie die Protokollierung und Überwachung für den Bastion-Host ein. Protokollierung und Überwachung sind sowohl aus betrieblicher als auch aus Sicherheitssicht wichtig für die Wartung von Systemen. Es gibt mehrere Möglichkeiten, Verbindungen und Aktivitäten in Ihrem Bastion-Host zu überwachen. Weitere Informationen finden Sie in den folgenden Themen der Systems Manager-Dokumentation:
  - Überwachen von AWS Systems Manager
  - Protokollierung und Überwachung in AWS Systems Manager
  - Prüfen der Sitzungsaktivität
  - Protokollieren von Sitzungsaktivitäten

Sekunden

Bereitstellen der Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis an den Speicherort, an dem	DevOps Techniker, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Beispieldateien speichern möchten. 2. Geben Sie den folgenden Befehl ein. `git clone https://github.com/aws-samples/secured-bastion-host-terraform.git`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie das Terraform -Arbeitsverzeichnis.	Dieser Schritt ist nur für die erste Bereitstellung erforderl ich. Wenn Sie das Muster erneut bereitstellen, fahren Sie mit dem nächsten Schritt fort. Geben Sie im Stammverz eichnis des geklonten Repositorys den folgenden Befehl ein, wobei: • `$S3_STATE_BUCKET` ist der Name des S3-Buckets, der den Terraform-Status enthält • `$PATH_TO_STATE_FIL E` ist der Schlüssel zur Terraform-Zustandsdatei, z. B. `infra/bastion-host /tetfstate` • `$AWS_REGION` ist die Region, in der der S3-Bucket bereitgestellt wird `terraform init \ -backend-config="b ucket=$S3_STATE_BU CKET" \ -backend-config="k ey=$PATH_TO_STATE_ FILE" \ -backend-config="r egion=$AWS_REGION`	DevOps Ingenieur, Entwickler, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Alternativ können Sie die Datei config.tf öffnen und im `terraform` Abschnitt diese Werte manuell angeben.	
Stellen Sie die Ressourcen bereit.	1. Geben Sie im Stammverz eichnis des geklonten Repositorys den folgenden Befehl ein. `terraform apply -var-file="dev.tfvars"` 2. Überprüfen Sie die Liste aller Änderungen, die auf Ihr AWS-Konto angewendet werden, und bestätigen Sie dann die Bereitstellung. 3. Warten Sie, bis alle Ressourcen bereitgestellt sind.	DevOps Ingenieur, Entwickler, Terraform

Einrichten der lokalen Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die SSH-Verbindung.	Aktualisieren Sie die SSH-Konfigurationsdatei, um SSH-Verbindungen über Session Manager zuzulasse n. Anweisungen finden Sie unter Zulassen von SSH-Verbi ndungen für Session Manager. Dadurch können autorisierte Benutzer einen Proxy-Befehl	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eingeben, der eine Session Manager-Sitzung startet und alle Daten über eine bidirekti onale Verbindung überträgt.	
Generieren Sie die SSH-Schlü ssel.	Geben Sie den folgenden Befehl ein, um ein lokales privates und öffentliches SSH-Schlüsselpaar zu generiere n. Sie verwenden dieses Schlüsselpaar, um eine Verbindung zum Bastion-Host herzustellen. `ssh-keygen -t rsa -f my_key`	DevOps Techniker, Entwickler

Herstellen einer Verbindung mit dem Bastion-Host mithilfe von Session Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Instance-ID ab.	1. Um eine Verbindung mit dem bereitgestellten Bastion-Host herzustellen, benötigen Sie die ID der EC2-Instance. Führen Sie einen der folgenden Schritte aus, um die ID zu finden: • Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigatio nsbereich Instances aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Suchen Sie die Bastion-Host-Instance.
	• Geben Sie in der AWS CLI den folgenden Befehl ein.
	`aws ec2 describe-instances`
	Um die Ergebnisse zu filtern, geben Sie den folgenden Befehl ein, wobei das Tag `$BASTION_HOST_TAG` ist, das Sie dem Bastion-Host zugewiesen haben. Der Standardwert für dieses Tag ist `sandbox-dev-bastion-host` .
	`aws ec2 describe-instances \ --filters "Name=tag:Name,Values=$BASTION_HOST_TAG" \ --output text \ --query 'Reservations[*].Instances[*].InstanceId' \ --output text`
	2. Kopieren Sie die ID der EC2-Instance. Sie verwenden diese ID später.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie den öffentlichen SSH-Schlüssel.	Hinweis: In diesem Abschnitt laden Sie den öffentlichen Schlüssel in die Instance-Metadaten des Bastion-Hosts hoch. Nachdem der Schlüssel hochgeladen wurde, haben Sie 60 Sekunden Zeit, um eine Verbindung mit dem Bastion-Host zu starten. Nach 60 Sekunden wird der öffentlic he Schlüssel entfernt. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung dieses Musters. Führen Sie die nächsten Schritte schnell aus, um zu verhindern, dass der Schlüssel entfernt wird, bevor Sie eine Verbindung zum Bastion-Host herstellen. 1. Senden Sie den SSH-Schlüssel mithilfe von EC2 Instance Connect an den Bastion-Host. Geben Sie den folgenden Befehl ein, wobei: • `$INSTANCE_ID` ist die ID der EC2-Instance • `$PUBLIC_KEY_FILE` ist der Pfad zu Ihrer öffentlic hen Schlüsseldatei, z. B. `my_key.pub` Wichtig: Achten Sie darauf, den öffentlichen	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schlüssel und nicht den privaten Schlüssel zu verwenden. `aws ec2-instance-connect send-ssh-public-key \ --instance-id $INSTANCE_ID \ --instance-os-user ec2-user \ --ssh-public-key file://$PUBLIC_KEY_FILE` 2. Warten Sie, bis Sie eine Meldung erhalten, die angibt, dass der Schlüssel erfolgreich hochgeladen wurde. Fahren Sie sofort mit dem nächsten Schritt fort.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung mit dem Bastion-Host her.	1. Geben Sie den folgenden Befehl ein, um über Session Manager eine Verbindung zum Bastion-Host herzustellen, wobei: • `$PRIVATE_KEY_FILE` ist der Pfad zu Ihrem privaten Schlüssel, z. B. `my_key` • `$INSTANCE_ID` ist die ID der EC2-Instance `ssh -i $PRIVATE_KEY_FILE ec2-user@$INSTANCE_ID` 2. Bestätigen Sie die Verbindung, indem Sie eingeben `yes`. Dadurch wird eine SSH-Verbindung mithilfe von Session Manager geöffnet. Hinweis: Es gibt weitere Optionen zum Öffnen einer SSH-Verbindung mit dem Bastion-Host. Weitere Informationen finden Sie unter Alternative Ansätze zum Herstellen einer SSH-Verbindung mit dem Bastion-Host im Abschnitt Zusätzliche Informationen dieses Musters.	Allgemeines AWS

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die bereitgestellten Ressourcen.	1. Um alle bereitgestellten Ressourcen zu entfernen, führen Sie den folgenden Befehl aus dem Stammverzeichnis des geklonten Repositorys aus. `terraform destroy -var-file="dev.tfvars"` 2. Bestätigen Sie das Entfernen der Ressourcen.	DevOps Ingenieur, Entwickler, Terraform

Fehlerbehebung

Problem	Lösung
`TargetNotConnected` -Fehler beim Versuch, eine Verbindung zum Bastion-Host herzustellen	1. Starten Sie den Bastion-Host gemäß den Anweisungen unter Starten Sie Ihre Instance neu in der Amazon EC2-Dokumentation. 2. Nachdem die Instance erfolgreich neu gestartet wurde, senden Sie den öffentlichen Schlüssel erneut an den Bastion-Host und versuchen Sie erneut, die Verbindung herzustellen.
`Permission denied` -Fehler beim Versuch, eine Verbindung zum Bastion-Host herzustellen	Nachdem der öffentliche Schlüssel auf den Bastion-Host hochgeladen wurde, haben Sie nur 60 Sekunden Zeit, um die Verbindung zu starten. Nach 60 Sekunden wird der Schlüssel automatisch entfernt, und Sie können ihn nicht verwenden, um eine Verbindung mit der

Problem	Lösung
	Instance herzustellen. In diesem Fall können Sie den Schritt wiederholen, um den Schlüssel erneut an die Instance zu senden.

Zugehörige Ressourcen

AWS-Dokumentation

- AWS Systems Manager Session Manager (Systems Manager-Dokumentation)
- Installieren des Session Manager-Plugins für die AWS CLI (Systems Manager-Dokumentation)
- Zulassen von SSH-Verbindungen für Session Manager (Systems Manager-Dokumentation)
- Informationen zur Verwendung von EC2 Instance Connect (Amazon EC2Dokumentation)
- Herstellen einer Verbindung über EC2 Instance Connect (Amazon EC2Dokumentation)
- Identity and Access Management für Amazon EC2 (Amazon EC2Dokumentation)
- Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2 ausgeführt werden (IAM-Dokumentation)
- Bewährte Methoden für die Sicherheit in IAM (IAM-Dokumentation)
- Kontrollieren des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen (Amazon-VPC-Dokumentation)

Sonstige Ressourcen

- Terraform-Entwicklerwebseite
- Befehl: validieren (Terraform-Dokumentation)
- Befehl: fmt (Terraform-Dokumentation)
- Testen von HashiCorp Terraform (HashiCorp Blogbeitrag)
- Checkov-Webseite

Zusätzliche Informationen

Alternative Ansätze zum Herstellen einer SSH-Verbindung mit dem Bastion-Host

Port-Weiterleitung

Sie können die `-D 8888` Option verwenden, um eine SSH-Verbindung mit dynamischer Port-Weiterleitung zu öffnen. Weitere Informationen finden Sie in diesen Anweisungen unter explainshell.com. Im Folgenden finden Sie ein Beispiel für einen Befehl zum Öffnen einer SSH-Verbindung mithilfe der Port-Weiterleitung.

```
ssh -i $PRIVATE_KEY_FILE -D 8888 ec2-user@$INSTANCE_ID
```

Dies ist eine Art von Verbindung, die einen SOCKS-Proxy öffnet, der den Datenverkehr von Ihrem lokalen Browser über den Bastion-Host weiterleiten kann. Wenn Sie Linux oder MacOS verwenden, geben Sie ein, um alle Optionen anzuzeigen`man ssh`. Dadurch wird das SSH-Referenzhandbuch angezeigt.

Verwenden des bereitgestellten Skripts

Anstatt die unter Herstellen einer Verbindung mit dem Bastion-Host mithilfe von Session Manager im Abschnitt „Epics“ beschriebenen Schritte manuell auszuführen, können Sie das im Code-Repository enthaltene Skript connect.sh verwenden. Dieses Skript generiert das SSH-Schlüsselpaar, überträgt den öffentlichen Schlüssel an die EC2-Instance und initiiert eine Verbindung mit dem Bastion-Host. Wenn Sie das Skript ausführen, übergeben Sie das Tag und den Schlüsselnamen als Argumente. Im Folgenden finden Sie ein Beispiel für den Befehl zum Ausführen des Skripts.

```
./connect.sh sandbox-dev-bastion-host my_key
```

Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD und lokalem Microsoft Active Directory

Erstellt von Brian Westmoreland (AWS)

Umgebung: Produktion	Technologien: Infrastruktur; Netzwerke DevOps; Sicherheit, Identität, Compliance; Betriebssysteme	Arbeitslast: Microsoft
AWS-Services: AWS Managed Microsoft AD; Amazon Route 53; AWS RAM; AWS Directory Service; AWS Organizations; AWS Direct Connect; AWS CLI		

Übersicht

Dieses Muster bietet Anleitungen zur Zentralisierung der DNS-Auflösung (Domain Name System) in einer AWS-Umgebung mit mehreren Konten mithilfe von AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). In diesem Muster ist der AWS-DNS-Namespace eine Unterdomäne des lokalen DNS-Namespace. Dieses Muster bietet auch Anleitungen zur Konfiguration der lokalen DNS-Server für die Weiterleitung von Abfragen an AWS, wenn die lokale DNS-Lösung Microsoft Active Directory verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine AWS-Umgebung mit mehreren Konten, die mithilfe von AWS Organizations eingerichtet wurde.
- Netzwerkkonnektivität zwischen AWS-Konten hergestellt.
- Netzwerkkonnektivität zwischen AWS und der lokalen Umgebung hergestellt (mithilfe von AWS Direct Connect oder einer beliebigen VPN-Verbindung).

- AWS-Befehlszeilenschnittstelle (AWS CLI), die auf einer lokalen Workstation konfiguriert ist.
- AWS Resource Access Manager (AWS RAM) wurde verwendet, um Amazon Route 53 53-Regeln zwischen Konten gemeinsam zu nutzen. Daher muss das Teilen in der Umgebung von AWS Organizations aktiviert sein, wie im Abschnitt Epics beschrieben.

Einschränkungen

- Die AWS Managed Microsoft AD Standard Edition hat ein Limit von 5 Aktien.
- Die AWS Managed Microsoft AD Enterprise Edition hat ein Limit von 125 Aktien.
- Diese Lösung in diesem Muster ist auf AWS-Regionen beschränkt, die die gemeinsame Nutzung über AWS-RAM unterstützen.

Produktversionen

- Microsoft Active Directory wird auf Windows Server 2008, 2012, 2012 R2 oder 2016 ausgeführt

Architektur

Zielarchitektur

In diesem Design ist AWS Managed Microsoft AD im AWS-Konto für gemeinsame Dienste installiert. Obwohl dies keine Anforderung ist, geht dieses Muster von dieser Konfiguration aus. Wenn Sie AWS Managed Microsoft AD in einem anderen AWS-Konto konfigurieren, müssen Sie möglicherweise die Schritte im Abschnitt Epics entsprechend ändern.

Dieses Design verwendet Route 53 53-Resolver, um die Namensauflösung mithilfe von Route 53 53-Regeln zu unterstützen. Wenn die lokale DNS-Lösung Microsoft DNS verwendet, ist die Erstellung einer bedingten Weiterleitungsregel für den AWS-Namespace (`aws.company.com`), der eine Unterdomäne des Unternehmens-DNS-Namespace (`company.com`) ist, nicht einfach. Wenn Sie versuchen, eine herkömmliche bedingte Weiterleitung zu erstellen, führt dies zu einem Fehler. Dies liegt daran, dass Microsoft Active Directory bereits für jede Subdomain von als maßgeblich angesehen wird. `company.com` Um diesen Fehler zu umgehen, müssen Sie zunächst eine Delegierung erstellen, um die Autorität für diesen `aws.company.com` Namespace zu delegieren. Anschließend können Sie die bedingte Weiterleitung erstellen.

Die Virtual Private Cloud (VPC) für jedes Spoke-Konto kann einen eigenen eindeutigen DNS-Namespace haben, der auf dem AWS-Stammnamespace basiert. In diesem Design hängt jedes Spoke-Konto eine Abkürzung des Kontonamens an den AWS-Basisnamespace an. Nachdem die privaten gehosteten Zonen im Spoke-Konto erstellt wurden, werden die Zonen mit der VPC im Spoke-Konto sowie mit der VPC im zentralen AWS-Netzwerkkonto verknüpft. Dadurch kann das zentrale AWS-Netzwerkkonto DNS-Anfragen beantworten, die sich auf die Spoke-Konten beziehen.

Automatisierung und Skalierung

Dieses Design verwendet Route 53 Resolver-Endpunkte, um DNS-Abfragen zwischen AWS und Ihrer lokalen Umgebung zu skalieren. Jeder Route 53 Resolver-Endpunkt umfasst mehrere elastische Netzwerkschnittstellen (verteilt auf mehrere Availability Zones), und jede Netzwerkschnittstelle kann bis zu 10.000 Abfragen pro Sekunde verarbeiten. Route 53 Resolver unterstützt bis zu 6 IP-Adressen pro Endpunkt, sodass dieses Design insgesamt bis zu 60.000 DNS-Abfragen pro Sekunde unterstützt, die über mehrere Availability Zones verteilt sind, um eine hohe Verfügbarkeit zu gewährleisten.

Darüber hinaus berücksichtigt dieses Muster automatisch das future Wachstum innerhalb von AWS. Die vor Ort konfigurierten DNS-Weiterleitungsregeln müssen nicht geändert werden, um neue VPCs und die zugehörigen privaten Hosting-Zonen zu unterstützen, die zu AWS hinzugefügt werden.

Tools

AWS-Services

- AWS Directory Service für Microsoft Active Directory ermöglicht Ihren verzeichnissensitiven Workloads und AWS-Ressourcen die Nutzung von Microsoft Active Directory in der AWS-Cloud.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- Mit AWS Resource Access Manager (AWS RAM) können Sie Ihre Ressourcen sicher für mehrere AWS-Konten gemeinsam nutzen, um den betrieblichen Aufwand zu reduzieren und für Transparenz und Überprüfbarkeit zu sorgen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können. In diesem Muster wird die AWS-CLI verwendet, um Route 53 53-Autorisierungen zu konfigurieren.

Epen

Erstellen und teilen Sie ein AWS Managed Microsoft AD-Verzeichnis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie AWS Managed Microsoft AD bereit.	1. Erstellen und konfigurieren Sie ein neues Verzeichnis. Ausführliche Schritte finden Sie unter Erstellen Ihres AWS Managed Microsoft AD-Verzeichnisses im AWS Directory Service Administration Guide. 2. Notieren Sie die IP-Adressen der AWS Managed Microsoft AD-Domänencontroller. Auf diese wird in einem späteren Schritt verwiesen.	AWS-Administrator
Teilen Sie das Verzeichnis.	Nachdem das Verzeichnis erstellt wurde, teilen Sie es mit anderen AWS-Konten in der AWS-Organisation. Anweisungen finden Sie unter Ihr Verzeichnis teilen im AWS Directory Service Administration Guide. Hinweis: Die AWS Managed Microsoft AD Standard Edition hat ein Limit von 5 Aktien. Die	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Enterprise Edition hat ein Limit von 125 Aktien.	

Route 53 konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Route 53 53-Resolver.	Route 53 53-Resolver erleichtern die Auflösung von DNS-Abfragen zwischen AWS und dem lokalen Rechenzentrum. 1. Installieren Sie Route 53 Resolver, indem Sie den Anweisungen im Route 53 Developer Guide folgen. 2. Konfigurieren Sie Route 53 53-Resolver in privaten Subnetzen in mindestens zwei Availability Zones innerhalb der zentralen AWS-Netzwerkkonto-VPC für hohe Verfügbarkeit. Hinweis: Die Verwendung der zentralen AWS-Netzwerkkonto-VPC ist zwar nicht erforderlich, die verbleibenden Schritte gehen jedoch von dieser Konfiguration aus.	AWS-Administrator
Erstellen Sie Route 53 53-Regeln.	Ihr spezieller Anwendungsfall erfordert möglicherweise eine	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	große Anzahl von Route 53 53-Regeln, aber Sie müssen die folgenden Regeln als Grundlage konfigurieren:
	• Eine ausgehende Regel für den lokalen Namespace (`company.com`) mithilfe der ausgehenden Route 53 53-Resolver.
	  • Teilen Sie diese Regel mit Spoke-AWS-Konten.
	  • Ordnen Sie diese Regel Spoke-Account-VPCs zu.
	• Eine ausgehende Regel für den AWS-Namespace (`aws.company.com`), die auf das zentrale Netzwerkkonto Route 53 Inbound Resolvers verweist.
	  • Teilen Sie diese Regel mit Spoke-AWS-Konten.
	  • Ordnen Sie die Regel den Spoke-Account-VPCs zu.
	  • Ordnen Sie diese Regel nicht der zentralen AWS-Netzwerkkonto-VPC zu (in der sich die Route 53 53-Resolver befinden).
	• Eine zweite ausgehende Regel für den AWS-Namespace (`aws.company.com`), die auf die AWS Managed Microsoft AD-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Domain-Controller verweist (verwenden Sie die IPs aus dem vorherigen Epic). • Ordnen Sie diese Regel der zentralen AWS-Netzwerkkonto-VPC zu (in der sich die Route 53 53-Resolver befinden). • Teilen Sie diese Regel nicht mit anderen AWS-Konten und verknüpfen Sie sie nicht mit ihnen. Weitere Informationen finden Sie unter Managing Forwarding Rules im Route 53 Developer Guide.	

Konfigurieren Sie das lokale Active Directory-DNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Delegation.	Verwenden Sie das Microsoft DNS-Snap-In (`dnsmgmt.msc`), um eine neue Delegierung für den `company.com` Namespace in Active Directory zu erstellen. Der Name der delegierten Domäne sollte lauten. `aws` Dies ist der vollqualifizierte Domänenname (FQDN) der Delegation. `aws.compa`	Active Directory

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ny.com` Verwenden Sie für die Nameserver die IP-Adressen der eingehend en Route 53 53-Resolv er von AWS im zentralen DNS-AWS-Konto für die IP-Werte und verwenden Sie sie `server.aws.company .com` für den Namen.	
Erstellen Sie den bedingten Forwarder.	Verwenden Sie das Microsoft DNS-Snap-In (`dnsmgmt.m sc`), um eine neue bedingte Weiterleitung für zu erstellen `. aws.company.com` Verwenden Sie die IP-Adressen der AWS Managed Microsoft AD-Domänencontroll er für das Ziel der bedingten Weiterleitung.	Active Directory

Private gehostete Route 53 53-Zonen für Spoke-AWS-Konten erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die privaten gehosteten Zonen von Route 53	Erstellen Sie in jedem Spoke-Konto eine private gehostete Route 53 53-Zone. Ordnen Sie diese privat gehostete Zone der Spoke-Konto-VPC zu. Eine ausführliche Anleitung finden Sie unter Creating a private hosted zone im Route 53 Developer Guide.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Autorisierungen erstellen.	Verwenden Sie die AWS-CLI, um eine Autorisierung für die zentrale AWS-Netzwerkkonto-VPC zu erstellen. Führen Sie diesen Befehl im Kontext jedes Spoke-AWS-Kontos aus: `aws route53 create-vpc-association-authorization --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` Wobei: • `<hosted-zone-id>` ist die privat gehostete Route 53 53-Zone im Spoke-Konto. • `<region>`und `<vpc-id>` sind die AWS-Region und VPC-ID des zentralen AWS-Netzwerkkontos VPC.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Assoziationen.	Erstellen Sie mithilfe der AWS-CLI die Route 53 53-Zuordnung für die private gehostete Zone für die zentrale AWS-Netzwerkkonto-VPC. Führen Sie diesen Befehl im Kontext des zentralen AWS-Netzwerkkontos aus: `aws route53 associate-vpc-with-hosted-zone --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` Wobei: • `<hosted-zone-id>` ist die privat gehostete Route 53 53-Zone im Spoke-Konto. • `<region>`und `<vpc-id>` sind die AWS-Region und VPC-ID des zentralen AWS-Netzwerkkontos.	AWS-Administrator

Zugehörige Ressourcen

- Vereinfachen Sie das DNS-Management in einer Umgebung mit mehreren Konten mit Route 53 Resolver (AWS-Blogbeitrag von Mahmoud Matouk)
- Erstellen eines Verzeichnisses mit AWS Managed Microsoft AD (Dokumentation zu AWS Directory Service)

- Teilen eines von AWS verwalteten Microsoft AD-Verzeichnisses (AWS Directory Service Service-Dokumentation)
- Installation eines Route 53 53-Resolvers (Amazon Route 53 53-Dokumentation)
- Erstellen einer privaten, gehosteten Route 53 53-Zone (Amazon Route 53 53-Dokumentation)

Zentralisieren der Überwachung mithilfe von Amazon CloudWatch Observability Access Manager

Erstellt von Anand Krishna Varanasi (AWS), Bolmy Bol (AWS), Ashish Kumar (AWS), Balaji Vedagiri (AWS), JAGDISH KomAKULA (AWS), Bolat Chandra Poth (AWS) und Vivek Thangamuthu (AWS)

Code-Repository: cloudwatch-obervability-access-manager-terraform	Umgebung: Produktion	Technologien: Infrastruktur; Strategie für mehrere Konten; Betrieb
AWS-Services: Amazon CloudWatch; Amazon CloudWatch Logs		

Übersicht

Beobachtbarkeit ist entscheidend für die Überwachung, das Verständnis und die Fehlerbehebung von Anwendungen. Anwendungen, die sich über mehrere Konten erstrecken, wie bei AWS Control Tower- oder Landing Zone-Implementierungen, generieren eine große Anzahl von Protokollen und Ablaufverfolgungsdaten. Um Probleme schnell zu beheben oder Benutzeranalysen oder Geschäftsanalysen zu verstehen, benötigen Sie eine gemeinsame Beobachtbarkeitsplattform für alle Konten. Der Amazon CloudWatch Observability Access Manager bietet Ihnen Zugriff auf und Kontrolle über mehrere Kontoprotokolle von einem zentralen Ort aus.

Sie können den Observability Access Manager verwenden, um Beobachtbarkeitsdatenprotokolle anzuzeigen und zu verwalten, die von Quellkonten generiert wurden. Quellkonten sind einzelne AWS-Konten, die Beobachtbarkeitsdaten für ihre Ressourcen generieren. Beobachtbarkeitsdaten werden zwischen Quellkonten und Überwachungskonten gemeinsam genutzt. Die freigegebenen Beobachtbarkeitsdaten können Metriken in Amazon CloudWatch, Protokolle in Amazon CloudWatch Logs und Ablaufverfolgungen in AWS X-Ray enthalten. Weitere Informationen finden Sie in der Dokumentation zu Observability Access Manager.

Dieses Muster richtet sich an Benutzer, die Anwendungen oder Infrastrukturen haben, die in mehreren AWS-Konten ausgeführt werden und einen gemeinsamen Ort zum Anzeigen von Protokollen benötigen. Es erklärt, wie Sie Observability Access Manager mithilfe von Terraform

einrichten können, um den Status und Zustand dieser Anwendungen oder Infrastruktur zu überwachen. Sie können diese Lösung auf verschiedene Arten installieren:

- Als eigenständiges Terraform-Modul, das Sie manuell einrichten
- Durch die Verwendung einer Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD)
- Durch die Integration mit anderen Lösungen wie AWS Control Tower Account Factory for Terraform (AFT)

Die Anweisungen im Abschnitt „Epics“ behandeln die manuelle Implementierung. Informationen zu den AFT-Installationsschritten finden Sie in der Readme-Datei für das GitHub Observability Access Manager-Repository.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Terraform wurde in Ihrem System oder in automatisierten Pipelines installiert oder referenziert. (Wir empfehlen Ihnen, die neueste Version zu verwenden.)
- Ein -Konto, das Sie als zentrales Überwachungskonto verwenden können. Andere Konten erstellen Links zum zentralen Überwachungskonto, um Protokolle anzuzeigen.
- (Optional) Ein Quellcode-Repository wie GitHub, AWS CodeCommit, Atlassian Bitbucket oder ein ähnliches System. Ein Quellcode-Repository ist nicht erforderlich, wenn Sie automatisierte CI/CD-Pipelines verwenden.
- (Optional) Berechtigungen zum Erstellen von Pull-Anforderungen (PRs) für die Codeüberprüfung und Codezusammenarbeit in GitHub.

Einschränkungen

Observability Access Manager verfügt über die folgenden Service Quotas, die nicht geändert werden können. Berücksichtigen Sie diese Kontingente, bevor Sie diese Funktion bereitstellen. Weitere Informationen finden Sie unter -CloudWatch Servicekontingente in der - CloudWatch Dokumentation.

- Quellkonto-Links: Sie können jedes Quellkonto mit maximal fünf Überwachungskonten verknüpfen.
- Senken: Sie können nur eine Senke pro Konto verwenden.

Darüber hinaus gilt:

- Senken und Links müssen in derselben AWS-Region erstellt werden. Sie dürfen nicht regionsübergreifend sein.
- Für die regionsübergreifende, kontoübergreifende Überwachung können Sie konto- und regionsübergreifende CloudWatch Dashboards für Alarme und Metriken erstellen, mit Ausnahme von Protokollen und Ablaufverfolgungen. Eine weitere Option besteht darin, eine zentrale Protokollierung mithilfe von Amazon OpenSearch Service zu erstellen.

Architektur

Komponenten

Amazon CloudWatch Observability Access Manager besteht aus zwei Hauptkomponenten, die eine kontoübergreifende Beobachtbarkeit ermöglichen:

- Eine Senke bietet Quellkonten die Möglichkeit, Beobachtbarkeitsdaten an das zentrale Überwachungskonto zu senden. Eine Senke bietet im Grunde eine Gateway-Verbindung, mit der Quellkonten eine Verbindung herstellen können. Es kann nur ein Sink-Gateway oder eine Sink-Verbindung geben und mehrere Konten können eine Verbindung zu diesem herstellen.
- Jedes Quellkonto verfügt über einen Link zur Sink-Gateway-Verbindung, und über diesen Link werden Beobachtbarkeitsdaten gesendet. Sie müssen eine Senke erstellen, bevor Sie Links von jedem Quellkonto erstellen.

Architektur

Das folgende Diagramm veranschaulicht Observability Access Manager und seine Komponenten.

Tools

AWS-Services

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.

Tools

- Terraform ist ein Infrastructure as Code (IaC HashiCorp)-Tool von , mit dem Sie Cloud- und On-Premises-Ressourcen erstellen und verwalten können.
- AWS Control Tower Account Factory for Terraform (AFT) richtet eine Terraform-Pipeline ein, die Sie bei der Bereitstellung und Anpassung von Konten in AWS Control Tower unterstützt. Sie können optional AFT verwenden, um Observability Access Manager in großem Umfang über mehrere Konten hinweg einzurichten.

Code-Repository

Der Code für dieses Muster ist im GitHub Observability Access Manager-Repository verfügbar.

Bewährte Methoden

- Markieren Sie in AWS Control Tower-Umgebungen das Protokollierungskonto als zentrales Überwachungskonto (Senke).
- Wenn Sie mehrere Organisationen mit mehreren Konten in AWS Organizations haben, empfehlen wir Ihnen, die Organisationen anstelle einzelner Konten in die Konfigurationsrichtlinie aufzunehmen. Wenn Sie eine kleine Anzahl von Konten haben oder wenn die Konten nicht Teil einer Organisation in der Sink-Konfigurationsrichtlinie sind, können Sie stattdessen einzelne Konten einbeziehen.

Sekunden

Einrichten des Senkenmoduls

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das GitHub Observability Access Manager-Repository:	AWS DevOps, Cloud-Adm inistrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/cloudwatch-observability-access-manager-terraform`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie Eigenschaftswerte für das Senkenmodul an.	Geben Sie in der `main.tf` Datei (im `deployments/aft-account-customizations/LOGGING/terraform/` Ordner des Repositorys) Werte für die folgenden Eigenschaften an: • `sink_name` : Der Name der Amazon- CloudWatch Senke. • `allowed_oam_resource_types` : Observability Access Manager unterstützt derzeit CloudWatch Metriken, Protokollgruppen und AWS X-Ray-Ablaufverfolgungen. • `allowed_source_accounts` : Die Quellkonten, die Protokolle an das zentrale CloudWatch Senkenkonto senden dürfen. • `allowed_source_organizations` : Die Control Tower-Quellorganisation, die Protokolle an das zentrale CloudWatch Senkenkonto senden dürfen. Weitere Informationen finden Sie unter AWS::Oam::Sink	AWS DevOps, Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der AWS- CloudFormation Dokumentation.	

Installieren Sie das Senkenmodul.	Exportieren Sie die Anmeldeinformationen des AWS-Kontos, das Sie als Überwachungskonto ausgewählt haben, und installieren Sie das Senkenmodul Observability Access Manager:
	`Terraform Init`
	`Terrafom Plan`
	`Terraform Apply`
		AWS DevOps, Cloud-Administrator, AWS-Administrator

Einrichten des Linkmoduls

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Geben Sie Eigenschaftswerte für das Linkmodul an.	Geben Sie in der `main.tf` Datei (im `deployments/aft-account-customizations/LOGGING/terraform/` Ordner des Repositorys) Werte für die folgenden Eigenschaften an:
	• `account_label` : Verwenden Sie einen der folgenden Werte:
	  • `$AccountName` : Der Name des Kontos.
	  • `$AccountEmail` : Eine global eindeutige E-Mail-
		AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Adresse, die die E-Mail-Domain enthält (z. B. `hello@example.com`) • `$AccountEmailNoDomain` : Eine E-Mail-Adresse ohne den Domänennamen. • `allowed_oam_resource_types` : Observability Access Manager unterstützt derzeit CloudWatch Metriken, Protokollgruppen und AWS X-Ray-Abl aufverfolgungen. Weitere Informationen finden Sie unter AWS::Oam::Link in der AWS- CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie das Linkmodul für einzelne Konten.	Exportieren Sie die Anmeldeinformationen einzelner Konten und installieren Sie das Observability-Access-Manager-Link-Modul:
	`Terraform Plan`
	`Terraform Apply`
	Sie können das Linkmodul einzeln für jedes Konto einrichten oder AFT verwenden, um dieses Modul automatisch über eine große Anzahl von Konten zu installieren.
		AWS DevOps, Cloud-Administrator, Cloud-Architekt

Genehmigen von sink-to-link Verbindungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Statusmeldung.	1. Melden Sie sich beim Überwachungskonto an. 2. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/. 3. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus. Auf der rechten Seite sollte die Statusmeldung Überwachu	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ngskonto mit einem grünen Häkchen aktiviert angezeigt werden. Das bedeutet, dass das Überwachungskonto über eine Observability Access Manager-Senke verfügt, mit der die Links anderer Konten eine Verbindung herstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Genehmigen Sie die link-to-sink Verbindungen.	1. Wählen Sie die Option Ressourcen zum Verknüpfen von Konten unter der Statusmeldung aus. Die Informationen bestätigen, dass dies das Überwachungskonto ist, listen die Daten auf, die von den Tenant-Quellkonten freigegeben werden (Protokolle, Metriken, Ablaufverfolgungen) und zeigen die Kontobezeichnung als $ anAccount Name. Dieser Bildschirm bietet zwei Optionen zum Verknüpfen von Tenant-Konten mit dem Überwachungskonto: Genehmigung auf Organisationsebene oder Genehmigung auf Kontoebene. Für jede Option können Sie eine AWS- CloudFormation Vorlage für die Genehmigung herunterladen oder jedes Konto einzeln genehmigen. 2. Wählen Sie der Einfachheit halber Beliebiges Konto aus, das auf jeder Kontoebene genehmigt werden soll. Diese Option	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bietet einen Genehmigungslink für das Konto. 3. Wählen Sie URL kopieren, um den Link zu kopieren. 4. Melden Sie sich bei jedem Quellkonto an. 5. Fügen Sie in einem Browserfenster den Link ein und wählen Sie Link mit Senke verbinden genehmigen aus. 6. Wiederholen Sie diesen Vorgang für weitere Quellkonten. Weitere Informationen finden Sie unter Verknüpfen von Überwachungskonten mit Quellkonten in der Amazon-CloudWatch Dokumentation.	

Überprüfen der kontoübergreifenden Beobachtbarkeitsdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kontoübergreifende Daten anzeigen.	1. Melden Sie sich beim zentralen Überwachungskonto an. 2. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie im linken Navigationsbereich Optionen aus, um kontoübergreifende Protokolle, Metriken und Ablaufverfolgungen anzuzeigen.	

(Optional) Aktivieren von Quellkonten für das Vertrauensüberwachungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie Metriken, Dashboards, Protokolle, Widgets und Alarme von anderen Konten an.	Als zusätzliche Funktion können Sie die CloudWatch Metriken, Dashboards, Protokolle, Widgets und Alarme für andere Konten freigeben. Jedes Konto verwendet eine IAM-Rolle namens CloudWatch,CrossAccountSharingRole um Zugriff auf diese Daten zu erhalten. Quellkonten, die eine Vertrauensstellung zum zentralen Überwachungskonto haben, können diese Rolle übernehmen und Daten aus dem Überwachungskonto anzeigen. CloudWatch stellt ein CloudFormation Beispielskript zum Erstellen der Rolle bereit. Wählen Sie Rolle	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in IAM verwalten aus und führen Sie dieses Skript in den Konten aus, in denen Sie Daten anzeigen möchten. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root" ] }, "Action": "sts:AssumeRole" } ] }` Weitere Informationen finden Sie unter Aktivieren der kontoübergreifenden Funktionalität in in der -	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudWatch CloudWatch Dokumentation.	

(Optional) Konto- und regionenübergreifendes Überwachungskonto anzeigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den konto- und regionsübergreifenden Zugriff ein.	Im zentralen Überwachungskonto können Sie optional eine Kontoauswahl hinzufügen, um einfach zwischen Konten zu wechseln und ihre Daten anzuzeigen, ohne sich authentifizieren zu müssen. 1. Melden Sie sich beim zentralen Überwachungskonto an. 2. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/. 3. Wählen Sie im linken Navigationsbereich Setttings aus. 4. Wählen Sie im Abschnitt Kontoübergreifende Region anzeigen die Option Konfigurieren aus. 5. Wählen Sie Aktivieren und dann das Kontrollkästchen Selektor anzeigen in der Konsole aus.	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie eine dieser Optionen aus: • Eingabe der Konto-ID: Mit dieser Option werden Sie aufgefordert, die Konto-ID jedes Mal manuell einzugeben, wenn Sie Konten ändern möchten, um kontoübergreifende Daten anzuzeigen. • AWS Organization-Konto auswahl: Wenn Sie CloudWatch in AWS Organizations integriert haben, bietet diese Option eine Dropdown-Auswahl mit einer vollständigen Liste der Konten in der Organisation. • Benutzerdefinierte Kontoauswahl: Mit dieser Option können Sie manuell eine Liste von Konto-IDs eingeben, um den Selektor zu füllen. 7. Wählen Sie Änderungen speichern aus. Weitere Informationen finden Sie unter Kontoüber greifende regionsübergreifen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	de CloudWatch Konsole in der - CloudWatch Dokumentation.	

Zugehörige Ressourcen

- CloudWatch Kontoübergreifende Beobachtbarkeit (Amazon- CloudWatch Dokumentation)
- API-Referenz für Amazon CloudWatch Observability Access Manager (Amazon- CloudWatch Dokumentation)
- Ressource: aws_oam_sink (Terraform-Dokumentation)
- Datenquelle: aws_oam_link (Terraform-Dokumentation)
- CloudWatchObservabilityAccessManager (AWS Boto3-Dokumentation)

EC2-Instances beim Start auf obligatorische Tags überprüfen

Umgebung: Produktion	Technologien: Infrastruktur; Management und Verwaltung; Sicherheit, Identität, Compliance; Cloud-nativ	AWS-Dienste: Amazon EC2; AWS; Amazon CloudTrail CloudWatch; Amazon SNS

Übersicht

Amazon Elastic Compute Cloud (Amazon EC2) bietet eine skalierbare Rechenkapazität in der Amazon-Web-Services(AWS)-Cloud. Amazon EC2 beseitigt die Notwendigkeit, im Voraus in Hardware investieren zu müssen. Daher können Sie Anwendungen schneller entwickeln und bereitstellen.

Sie können Tagging verwenden, um Ihre AWS-Ressourcen auf unterschiedliche Weise zu kategorisieren. EC2-Instance-Tagging ist nützlich, wenn Sie viele Ressourcen in Ihrem Konto haben und Sie anhand der Tags schnell eine bestimmte Ressource identifizieren möchten. Sie können Ihren EC2-Instances mithilfe von Tags benutzerdefinierte Metadaten zuweisen. Ein Tag besteht aus einem benutzerdefinierten Schlüssel und Wert. Wir empfehlen Ihnen, einen konsistenten Satz von Stichwörtern zu erstellen, um die Anforderungen Ihrer Organisation zu erfüllen.

Dieses Muster bietet eine CloudFormation AWS-Vorlage, mit der Sie EC2-Instances auf bestimmte Tags überwachen können. Die Vorlage erstellt ein Amazon CloudWatch Events-Ereignis, das nach AWS CloudTrail TagResource- oder UntagResourceEreignissen Ausschau hält, um zu erkennen, dass neue EC2-Instances markiert oder Tags entfernt werden. Wenn ein vordefiniertes Tag fehlt, ruft es eine AWS-Lambda-Funktion auf, die mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Meldung über einen Verstoß an eine von Ihnen angegebene E-Mail-Adresse sendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hochladen des bereitgestellten Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.

Einschränkungen

- Diese Lösung unterstützt CloudTrail TagResourceunsere UntagResourceEreignisse. Es werden keine Benachrichtigungen für andere Ereignisse erstellt.
- Diese Lösung sucht nur nach Tag-Schlüsseln. Schlüsselwerte werden nicht überwacht.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage in jeder Region oder jedem Konto nur einmal ausführen.

Tools

AWS-Services

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der sichere, anpassbare Rechenkapazität in der Cloud bereitstellt. Er wurde entwickelt, um Entwicklern Cloud-Computing im Web-Scale-Maßstab zu erleichtern.
- AWS CloudTrail — CloudTrail ist ein AWS-Service, der Sie bei der Steuerung, Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos unterstützt. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events wird sofort auf betriebliche Änderungen aufmerksam und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne dass Server bereitgestellt oder verwaltet werden müssen. Lambda führt Ihren Code nur bei

Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `index.zip`ist eine komprimierte Datei, die den Lambda-Code für dieses Muster enthält.
- `ec2-require-tags.yaml`ist eine CloudFormation Vorlage, die den Lambda-Code bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie den Lambda-Code bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `index.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen (EC2-Instances), die Sie überwachen möchten.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS-Region wie der S3-Bucket und stellen Sie die `ec2-require-tags.yaml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die EC2-Instances, die Sie überwachen möchten.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B. `index.zip` oder). `controls/index.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Benachrichtigungen über Verstöße erhalten möchten.	
Definieren Sie eine Protokollierungsebene.	Geben Sie die Protokollierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt
Geben Sie die erforderlichen Tag-Schlüssel ein.	Geben Sie die Tag-Schlüssel ein, nach denen Sie suchen möchten. Wenn Sie mehrere Schlüssel angeben möchten, trennen Sie sie durch Kommas ohne Leerzeichen. (`ApplicationId,CreatedBy,Environment,Organization` Sucht beispielsweise nach vier Schlüsseln.) Das Ereignis CloudWatch Ereignisse sucht nach diesen Tag-Schlüsseln und sendet eine Benachrichtigung, wenn sie nicht gefunden werden.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Objekte hochladen (Amazon S3 S3-Dokumentation)
- Kennzeichnen Sie Ihre Amazon EC2 EC2-Ressourcen (Amazon EC2 EC2-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudWatch Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Herstellen einer Verbindung mit einer Amazon EC2-Instance mithilfe von Session Manager

Erstellt von Jason Cornick (AWS), Abhishek Bastik Bola (AWS) und Yaniv Ron (AWS)

Umgebung: Produktion	Technologien: Infrastruktur; Cloudnativ; Endbenutzer-Computing; Betrieb	AWS-Services: Amazon CloudWatch Logs; AWS Systems Manager ;Amazon EC2

Übersicht

Dieses Muster beschreibt, wie Sie eine Verbindung zu einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance herstellen, indem Sie den Session Manager verwenden, eine Funktion von AWS Systems Manager . Mit diesem Muster können Sie Bash-Befehle auf einer EC2-Instance über einen Webbrowser ausführen. Session Manager erfordert nicht, dass Sie eingehende Ports öffnen, und erfordert keine öffentlichen IP-Adressen für EC2-Instances. Darüber hinaus entfällt die Notwendigkeit, Bastion-Hosts mit unterschiedlichen Secure Shell (SSH)-Schlüsseln zu warten. Sie können den Zugriff auf Session Manager mit AWS Identity and Access Management (IAM)-Richtlinien regeln und die Protokollierung konfigurieren, die wichtige Informationen wie Instance-Zugriff und -Aktionen aufzeichnet.

In diesem Muster konfigurieren Sie eine IAM-Rolle und verknüpfen sie mit einer Linux-EC2-Instance, die Sie mithilfe eines Amazon Machine Image (AMI) bereitstellen. Anschließend konfigurieren Sie die Protokollierung in Amazon CloudWatch Logs und verwenden Session Manager, um eine Sitzung mit der Instance zu starten.

Obwohl dieses Muster eine Verbindung zu einer Linux-EC2-Instance in der Amazon Web Services (AWS) Cloud herstellt, können Sie diesen Ansatz verwenden, um Session Manager für Verbindungen mit anderen Servern zu verwenden, z. B. On-Premises-Server oder andere virtuelle Maschinen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- Berechtigungen für den Zugriff auf den verwalteten Knoten. Anweisungen finden Sie unter Steuern des Benutzersitzungszugriffs auf verwaltete Knoten.
- VPC-Endpunkte für `ssm`, `ec2`, `ec2messagesssmmessages`, und `s3`. Anweisungen finden Sie unter Erstellen von VPC-Endpunkten in der Systems Manager-Dokumentation.

Architektur

Zieltechnologie-Stack

- Session Manager
- Amazon EC2
- CloudWatch Protokolle

Zielarchitektur

1. Der Benutzer authentifiziert seine Identität und Anmeldeinformationen über IAM.
2. Der Benutzer initiiert eine SSH-Sitzung über Session Manager und sendet API-Aufrufe an die EC2-Instance.
3. Der AWS Systems Manager SSM Agent, der auf der EC2-Instance installiert ist, stellt eine Verbindung zu Session Manager her und führt die Befehle aus.
4. Zu Prüfungs- und Überwachungszwecken sendet Session Manager die Protokollierungsdaten an CloudWatch Logs. Alternativ können Sie Protokolldaten an einen Amazon Simple Storage Service (Amazon S3)-Bucket senden. Weitere Informationen finden Sie unter Protokollieren von Sitzungsdaten mit Amazon S3 (Systems Manager-Dokumentation).

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, damit Sie sie überwachen und sicher archivieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten

skalieren. Dieses Muster verwendet ein Amazon Machine Image (AMI), um eine Linux-EC2-Instance bereitzustellen.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang. Dieses Muster verwendet Session Manager , eine Funktion von Systems Manager.

Bewährte Methoden

Wir empfehlen Ihnen, mehr über die Sicherheitssäule des AWS Well-Architected Framework zu erfahren, Verschlüsselungsoptionen zu erkunden und die Sicherheitsempfehlungen unter Session Manager einrichten (Systems Manager-Dokumentation) anzuwenden.

Polen

Einrichten der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle.	Erstellen Sie die IAM-Rolle für den SSM-Agenten. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen AWS-Service (IAM-Dokumentation) und beachten Sie Folgendes: 1. Wählen Sie für den AWS-Service EC2 aus. 2. Wählen Sie für Berechtigungsrichtlinien aus `AmazonSSMManagedInstanceCore` .	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Geben Sie unter Rollennam e ein`EC2_SSM_Role` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die EC2-Instance.	1. Erstellen Sie die EC2-Instance. Folgen Sie den Anweisungen unter Starten einer Instance (Amazon EC2-Dokumentation) und beachten Sie Folgendes: a. Wählen Sie im Abschnitt Name und Tags die Option Zusätzliche Tags hinzufügen aus. Geben Sie unter Key (Schlüssel) „`Name`“ ein, und geben Sie in Value (Wert) „`Production_Server_One`“ ein. b. Wählen Sie ein Amazon Linux AMI aus, auf dem der SSM Agent vorinstalliert ist. Eine vollständige Liste finden Sie unter AMIs mit vorinstalliertem SSM Agent (Systems Manager-Dokumentation). c. Wählen Sie im Abschnitt Erweiterte Details im IAM-Instance-Profil EC2_SSM_Role aus. 2. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie im Navigationsbereich Fleet Manager aus. 4. Stellen Sie sicher, dass die Instance in der Liste der verwalteten Knoten angezeigt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Protokollierung ein.	1. Erstellen Sie eine Protokollgruppe in - CloudWatch Protokollen. Folgen Sie den Anweisungen unter Erstellen einer Protokollgruppe (CloudWatch Protokolldokumentation). Benennen Sie die neue Protokollgruppe `SessionManager` . 2. Konfigurieren Sie die Protokollierung für Session Manager. Folgen Sie den Anweisungen unter Protokollieren von Sitzungsdaten mit Amazon CloudWatch Logs (Systems-Manager-Dokumentation) und beachten Sie Folgendes: a. Wählen Sie nicht Nur verschlüsselte CloudWatch Protokollgruppen zulassen aus. b. Wählen Sie unter Protokollgruppe aus der Liste auswählen die Option ausSessionManager.	AWS-Systemadministrator

Eine Verbindung zur Instance herstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung mit der EC2-Instance her.	1. Starten Sie eine Sitzung in der Systems Manager-Konsole. Anweisungen finden Sie unter Starten einer Sitzung (Systems Manager-Dokumentation). Wählen Sie für Ziel-Instances die Optionsschaltfläche links neben der Production_Server_One-Instance aus. 2. Nachdem die Verbindung hergestellt wurde, führen Sie mehrere Bash-Befehle aus. 3. Beenden Sie in der Systems Manager-Konsole die Sitzung. Anweisungen finden Sie unter Beenden einer Sitzung (Systems-Manager-Dokumentation).	AWS-Systemadministrator
Validieren Sie die Protokollierung.	1. Öffnen Sie unter CloudWatch Protokolle den Protokollstream für die Protokollgruppe. Anweisungen finden Sie unter Anzeigen von Protokolldaten (CloudWatch Protokolldokumentation). 2. Vergewissern Sie sich in den Protokolldaten, dass	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Befehle, die Sie in der vorherigen Geschicht e ausgeführt haben, aufgeführt sind.	

Fehlerbehebung

Problem	Lösung
IAM-Probleme	Weitere Informationen finden Sie unter Fehlerbehebung (IAM-Dokumentation).

Zugehörige Ressourcen

- Erfüllen der Voraussetzungen für Session Manager (Systems-Manager-Dokumentation)
- Entwerfen und Implementieren von Protokollierung und Überwachung mit Amazon CloudWatch (AWS Prescriptive Guidance)

Erstellen einer Pipeline in AWS-Regionen, die AWS nicht unterstützen CodePipeline

Erstellt von Anand Krishna Varanasi (AWS)

Code-Repository: invisible-codepipeline-unsupported-regions	Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; DevOps
AWS-Services: AWS CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Übersicht

AWS CodePipeline ist ein Continuous Delivery (CD)-Orchestrierungsservice, der Teil einer Reihe von DevOps Tools von Amazon Web Services (AWS) ist. Es lässt sich in eine Vielzahl von Quellen integrieren (z. B. Versionsverwaltungssysteme und Speicherlösungen), Produkte und Services für kontinuierliche Integration (CI) von AWS und AWS-Partnern sowie Open-Source-Produkte, um einen - end-to-end Workflow-Service für schnelle Anwendungs- und Infrastrukturbereitstellungen bereitzustellen.

CodePipeline Wird jedoch nicht in allen AWS-Regionen unterstützt, und es ist nützlich, einen unsichtbaren Orchestrator zu haben, der AWS CI/CD-Services verbindet. Dieses Muster beschreibt, wie Sie eine end-to-end Workflow-Pipeline in AWS-Regionen implementieren, in denen noch nicht durch die Verwendung von AWS CI/CD-Services wie AWS CodeCommit, AWS CodeBuildund AWS unterstützt CodePipeline wird CodeDeploy.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Cloud Development Kit (AWS CDK) CLI Version 2.28 oder höher

Architektur

Zieltechnologie-Stack

Das folgende Diagramm zeigt eine Pipeline, die in einer Region erstellt wurde, die nicht unterstützt CodePipeline, z. B. die Region Afrika (Kapstadt). Ein Entwickler überträgt die CodeDeploy Konfigurationsdateien (auch als Lebenszyklus-Hook-Skripte für die Bereitstellung bezeichnet) an das Git-Repository, das von gehostet wird CodeCommit. (Siehe das GitHub Repository, das mit diesem Muster bereitgestellt wird.) Eine Amazon- EventBridge Regel initiiert automatisch CodeBuild.

Die CodeDeploy Konfigurationsdateien werden im CodeCommit Rahmen der Quellphase der Pipeline von abgerufen und an übertragen CodeBuild.

In der nächsten Phase CodeBuild führt die folgenden Aufgaben aus:

1. Lädt die TAR-Quellcodedatei der Anwendung herunter. Sie können den Namen dieser Datei mithilfe von Parameter Store konfigurieren, einer Funktion von AWS Systems Manager .
2. Lädt die CodeDeploy Konfigurationsdateien herunter.
3. Erstellt ein kombiniertes Archiv von Anwendungsquellcode und CodeDeploy Konfigurationsdateien, die für den Anwendungstyp spezifisch sind.
4. Initiiert die CodeDeploy Bereitstellung auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance mithilfe des kombinierten Archivs.

Tools

AWS-Services

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen auf Amazon EC2 oder On-Premises-Instances, AWS Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS)-Services.

- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.

Code

Der Code für dieses Muster ist im Repository GitHub CodePipeline Nicht unterstützte Regionen verfügbar.

Polen

Einrichten Ihrer Entwickler-Workstation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die AWS-CDK-CLI.	Anweisungen finden Sie in der AWS-CDK-Dokumentation.	AWS DevOps
Installieren Sie einen Git-Client.	Um Commits zu erstellen, können Sie einen auf Ihrem lokalen Computer installierten Git-Client verwenden und Ihre Commits dann in das CodeCommit Repository verschieben. Informationen zum Einrichten CodeCommit von mit Ihrem Git-Client finden Sie in der CodeCommit Dokumentation .	AWS DevOps
Installieren Sie "npm".	Installieren Sie den npm-Paketmanager. Weitere Informationen finden Sie in der npm-Dokumentation.	AWS DevOps

Einrichten der Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	Klonen Sie das GitHub CodePipeline Repository Nicht unterstützte Regionen auf Ihren lokalen Computer, indem Sie den folgenden Befehl ausführen. `git clone https://github.com/aws-samples/invisible-codepipeline-unsupported-regions`	DevOps Techniker
Legen Sie Parameter in cdk.json fest.	Öffnen Sie die `cdk.json` Datei und geben Sie Werte für die folgenden Parameter an: `"pipeline_account":"XXXXXXXXXXXX", "pipeline_region":"us-west-2", "repo_name": "app-dev-repo", "ec2_tag_key": "test-vm", "configName" : "cbdeployconfig", "deploymentGroupName": "cbdeploygroup", "applicationName" : "cbdeployapplication", "projectName" : "CodeBuildProject"` Wobei:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `pipeline_account` ist das AWS-Konto, in dem die Pipeline erstellt wird. • `pipeline_region` ist die AWS-Region, in der die Pipeline erstellt wird. • `repo_name` ist der Name des CodeCommit Repositorys. • `ec2_tag_key` ist das Tag, das an die EC2-Instance angehängt ist, für die Sie den Code bereitstellen möchten. • `configName` ist der Name der CodeDeploy Konfigurationsdatei. • `deploymentGroupName` ist der Name der CodeDeploy Bereitstellungsgruppe. • `applicationName` ist der CodeDeploy Anwendungsname. • `projectName` ist der CodeBuild Projektname.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die AWS-CDK-K onstruktbibliothek ein.	Verwenden Sie im geklonten GitHub Repository die folgenden Befehle, um die AWS-CDK-Konstruktb ibliothek zu installieren, Ihre Anwendung zu erstellen und zu synthetisieren, um die AWS- CloudFormation Vorlage für die Anwendung zu generieren.
	`npm i aws-cdk-lib`
	`npm run build`
	`cdk synth`
		AWS DevOps

Stellen Sie die AWS-CDK-B eispielanwendung bereit.	Stellen Sie den Code bereit, indem Sie den folgenden Befehl in einer nicht unterstüt zten Region ausführen (z. B. `af-south-1`). `cdk deploy`	AWS DevOps

Einrichten des CodeCommit Repositorys für CodeDeploy

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie CI/CD für die Anwendung ein.	Klonen Sie das CodeCommi t Repository, das Sie in der `cdk.json` Datei angegeben haben (dies wird `app-dev-repo` standardmäßig als bezeichnet), um die CI/CD-	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pipeline für die Anwendung einzurichten. `git clone https://git-codecommit.us-west-2.amazonaws.com/v1/repos/app-dev-repo` wobei der Name und die Region des Repositorys von den Werten abhängen, die Sie in der `cdk.json` Datei angegeben haben.	

Testen der Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Pipeline mit Bereitstellungsanweisungen.	Der `CodeDeploy_Files` Ordner des GitHub CodePipeline Repositorys Nicht unterstützte Regionen enthält Beispieldateien, die CodeDeploy anweisen, die Anwendung bereitzustellen. Die `appspec.yml` Datei ist eine CodeDeploy Konfigurationsdatei, die Hooks zur Steuerung des Ablaufs der Anwendungsbereitstellung enthält. Sie können die Beispieldateien `index.html` , `start_server.sh` , und verwenden`stop_server.sh` , `install_d`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ependencies.sh` um eine Website zu aktualisieren, die auf Apache gehostet wird. Dies sind Beispiele – Sie können den Code im GitHub Repository verwenden, um jede Art von Anwendung bereitzustellen. Wenn die Dateien in das CodeCommi t Repository übertragen werden, wird die unsichtba re Pipeline automatisch initiiert. Überprüfen Sie die Ergebnisse der Bereitstellung in den CodeDeploy Konsolen CodeBuild und .	

Zugehörige Ressourcen

- Erste Schritte (AWS-CDK-Dokumentation)
- Einführung in das Cloud Development Kit (CDK) (AWS Workshop Studio)
- AWS-CDK-Workshop

Bereitstellen eines Cassandra-Clusters auf Amazon EC2 mit privaten statischen IPs, um einen Neuausgleich zu vermeiden

Erstellt von Dipin Jain (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises-VM	Ziel: Amazon EC2
R-Typ: Hostwechsel	Workload: Open-Source	Technologien: Infrastruktur; Datenbanken; Migration
AWS-Services: Amazon EC2		

Übersicht

Die private IP einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance wird während ihres gesamten Lebenszyklus beibehalten. Die private IP kann sich jedoch während eines geplanten oder ungeplanten Systemabsturzs ändern, z. B. während eines Upgrades von Amazon Machine Image (AMI). In einigen Szenarien kann die Beibehaltung einer privaten statischen IP die Leistung und Wiederherstellungszeit von Workloads verbessern. Die Verwendung einer statischen IP für einen Apache-Cassandra-Seed-Knoten verhindert beispielsweise, dass dem Cluster ein Neuausgleichs-Overhead entsteht.

Dieses Muster beschreibt, wie Sie eine sekundäre Elastic-Network-Schnittstelle an EC2-Instances anfügen, um die IP während des Hostwechsels statisch zu halten. Das Muster konzentriert sich auf Cassandra-Cluster, aber Sie können diese Implementierung für jede Architektur verwenden, die von privaten statischen IPs profitiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Service (AWS)-Konto

Produktversionen

- DataStax Version 5.11.1
- Betriebssystem: Ubuntu 16.04.6 LTS

Architektur

Quellarchitektur

Die Quelle könnte ein Cassandra-Cluster auf einer lokalen virtuellen Maschine (VM) oder auf EC2-Instances in der AWS Cloud sein. Das folgende Diagramm veranschaulicht das zweite Szenario. Dieses Beispiel umfasst vier Cluster-Knoten: drei Seed-Knoten und einen Verwaltungsknoten. In der Quellarchitektur ist jedem Knoten eine einzelne Netzwerkschnittstelle zugeordnet.

Zielarchitektur

Der Ziel-Cluster wird auf EC2-Instances mit einer sekundären Elastic-Network-Schnittstelle gehostet, die an jeden Knoten angeschlossen ist, wie im folgenden Diagramm dargestellt.

Automatisierung und Skalierung

Sie können auch das Anhängen einer zweiten Elastic Network-Schnittstelle an eine EC2 Auto Scaling-Gruppe automatisieren, wie in einem AWS Knowledge Center-Video beschrieben.

Polen

Konfigurieren eines Cassandra-Clusters auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie EC2-Knoten, um einen Cassandra-Cluster zu hosten.	Starten Sie in der Amazon EC2-Konsole vier EC2-Instances für Ihre Ubuntu-Knoten in Ihrem AWS-Konto. Drei (Seed) Knoten werden für den Cassandra-Cluster verwendet, und der vierte	Cloud-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Knoten fungiert als Cluster-Verwaltungsknoten, auf dem Sie DataStax Enterprise (DSE) installieren OpsCenter. Anweisungen finden Sie in der Amazon EC2-Dokumentation.	
Bestätigen Sie die Knotenkommunikation.	Stellen Sie sicher, dass die vier Knoten über die Datenbank- und Cluster-Verwaltungsports miteinander kommunizieren können.	Netzwerkingenieur
Installieren Sie DSE OpsCenter auf dem Verwaltungsknoten.	Installieren Sie DSE OpsCenter 6.1 aus dem Debian-Paket auf dem Verwaltungsknoten. Anweisungen finden Sie in der DataStax Dokumentation .	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine sekundäre Netzwerkschnittstelle.	Cassandra generiert einen Universal Unique Identifier (UUID) für jeden Knoten basierend auf der IP-Adresse der EC2-Instance für diesen Knoten. Diese UUID wird verwendet, um virtuelle Knoten (vnodes) auf dem Ring zu verteilen. Wenn Cassandra auf EC2-Instances bereitgestellt wird, werden den Instances beim Erstellen automatisch IP-Adressen zugewiesen. Im Falle eines geplanten oder ungeplanten Ausfalls ändert sich die IP-Adresse für die neue EC2-Instance, die Datenverteilung ändert sich und der gesamte Ring muss neu ausgeglichen werden. Dies ist nicht erwünscht. Um die zugewiesene IP-Adresse beizubehalten, verwenden Sie eine sekundäre Elastic Network-Schnittstelle mit einer festen IP-Adresse. 1. Wählen Sie in der Amazon EC2-Konsole Netzwerkschnittstellen, Netzwerkschnittstelle erstellen aus. 2. Wählen Sie für Subnetz das Subnetz aus, in dem Sie	Cloud-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die EC2-Instance erstellt haben. 3. Wählen Sie für Private IPv4-Adresse die Option Automatische Zuweisung aus. 4. Wählen Sie für Sicherheitsgruppen eine Sicherheitsgruppe aus und wählen Sie dann Netzwerkschnittstelle erstellen aus. Weitere Informationen zum Erstellen einer Netzwerkschnittstelle finden Sie in der Amazon EC2-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie die sekundäre Netzwerkschnittstelle an Cluster-Knoten an.	1. Wählen Sie in der Amazon EC2-Konsole Instances aus. 2. Aktivieren Sie das Kontrollkästchen für die EC2-Instance, die Sie zuvor erstellt haben. 3. Wählen Sie Aktionen, Netzwerk, Netzwerkschnittstelle, anhängen. 4. Wählen Sie die Netzwerkschnittstelle aus, die Sie im vorherigen Schritt erstellt haben, und wählen Sie dann Anfügen aus. Weitere Informationen zum Anfügen einer Netzwerkschnittstelle finden Sie in der Amazon EC2-Dokumentation.	Cloud-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Routen in Amazon EC2 hinzu, um asymmetri sches Routing anzugehen.	Wenn Sie die zweite Netzwerkschnittstelle anfügen, führt das Netzwerk sehr wahrscheinlich asymmetri sches Routing durch. Um dies zu vermeiden, können Sie Routen für die neuen Netzwerkschnittstellen hinzufügen. Eine ausführliche Erläuterung und Behebung von asymmetri schem Routing finden Sie im AWS Knowledge Center-Vi deo oder Überwinden von asymmetrischem Routing auf Multi-Home-Servern (Kern im Linux Journal von Patrick McManus, 5. April 2004).	Netzwerkingenieur
Aktualisieren Sie DNS-Eintr äge so, dass sie auf die IP der sekundären Netzwerks chnittstelle verweisen.	Verweisen Sie den vollquali fizierten Domainnamen (FQDN) des Knotens auf die IP der sekundären Netzwerks chnittstelle.	Netzwerkingenieur
Installieren und konfigurieren Sie den Cassandra-Cluster mithilfe von DSE OpsCenter.	Wenn die Cluster-Knoten mit den sekundären Netzwerks chnittstellen bereit sind, können Sie den Cassandra -Cluster installieren und konfigurieren.	DBA

Wiederherstellen des Clusters nach einem Knotenausfall

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AMI für den Cluster-Seed-Knoten.	Erstellen Sie ein Backup der Knoten, damit Sie sie im Falle eines Knotenausfalls mit Datenbank-Binärdateien wiederherstellen können. Anweisungen finden Sie unter Erstellen eines AMI in der Amazon EC2Dokumentation.	Backup-Administrator
Wiederherstellung nach Knotenausfall.	Ersetzen Sie den ausgefall enen Knoten durch eine neue EC2-Instance, die über das AMI gestartet wurde, und fügen Sie die sekundäre Netzwerkschnittstelle des ausgefallenen Knotens an.	Backup-Administrator
Überprüfen Sie, ob der Cassandra-Cluster fehlerfrei ist.	Wenn der Ersatzknoten aktiv ist, überprüfen Sie den Clusterstatus in DSE OpsCenter.	DBA

Zugehörige Ressourcen

- Installieren von DSE OpsCenter 6.1 aus dem Debian-Paket (DataStax Dokumentation)
- So lassen Sie eine sekundäre Netzwerkschnittstelle in einer Ubuntu-EC2-Instance funktionieren (AWS Knowledge Center-Video)
- Bewährte Methoden für die Ausführung von Apache Cassandra auf Amazon EC2 (AWS-Blogbeitrag)

Erweitern Sie VRFs auf AWS mithilfe von AWS Transit Gateway Connect

Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; Netzwerke	AWS-Services: AWS Direct Connect; AWS Transit Gateway

Übersicht

Virtuelles Routing and Forwarding (VRF) ist eine Funktion herkömmlicher Netzwerke. Es verwendet isolierte logische Routingdomänen in Form von Routingtabellen, um den Netzwerkverkehr innerhalb derselben physischen Infrastruktur zu trennen. Sie können AWS Transit Gateway so konfigurieren, dass es die VRF-Isolierung unterstützt, wenn Sie Ihr lokales Netzwerk mit AWS verbinden. Dieses Muster verwendet eine Beispielarchitektur, um lokale VRFs mit verschiedenen Routentabellen für Transit-Gateways zu verbinden.

Dieses Muster verwendet virtuelle Transitschnittstellen (VIFs) in AWS Direct Connect- und Transit Gateway Connect-Anhängen, um die VRFs zu erweitern. Eine Transit-VIF wird für den Zugriff auf ein oder mehrere Amazon VPC-Transit-Gateways verwendet, die Direct Connect-Gateways zugeordnet sind. Ein Transit Gateway Connect-Anhang verbindet ein Transit-Gateway mit einer virtuellen Appliance eines Drittanbieters, die in einer VPC ausgeführt wird. Ein Transit Gateway Connect-Anhang unterstützt das GRE (Generic Routing Encapsulation) -Tunnelprotokoll für hohe Leistung und unterstützt das Border Gateway Protocol (BGP) für dynamisches Routing.

Der in diesem Muster beschriebene Ansatz bietet die folgenden Vorteile:

- Mit Transit Gateway Connect können Sie dem Transit Gateway Connect-Peer bis zu 1.000 Routen ankündigen und bis zu 5.000 Routen von diesem empfangen. Die Verwendung der Direct Connect-Transit-VIF-Funktion ohne Transit Gateway Connect ist auf 20 Präfixe pro Transit-Gateway beschränkt.
- Sie können die Isolierung des Datenverkehrs aufrechterhalten und Transit Gateway Connect verwenden, um gehostete Dienste auf AWS bereitzustellen, unabhängig davon, welche IP-Adressschemas Ihre Kunden verwenden.
- Der VRF-Verkehr muss keine öffentliche virtuelle Schnittstelle durchqueren. Dies erleichtert die Einhaltung der Compliance- und Sicherheitsanforderungen in vielen Organisationen.

- Jeder GRE-Tunnel unterstützt bis zu 5 Gbit/s, und Sie können bis zu vier GRE-Tunnel pro Transit Gateway Connect-Anhang haben. Dies ist schneller als viele andere Verbindungstypen, wie z. B. AWS-Site-to-Site-VPN-Verbindungen, die bis zu 1,25 Gbit/s unterstützen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Die erforderlichen AWS-Konten wurden erstellt (Einzelheiten finden Sie in der Architektur)
- Berechtigungen zur Übernahme einer AWS Identity and Access Management (IAM) -Rolle in jedem Konto.
- Die IAM-Rollen in jedem Konto müssen über Berechtigungen zur Bereitstellung von AWS Transit Gateway- und AWS Direct Connect Connect-Ressourcen verfügen. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Ihre Transit-Gateways und unter Identitäts- und Zugriffsmanagement für Direct Connect.
- Die Direct Connect-Verbindungen wurden erfolgreich erstellt. Weitere Informationen finden Sie unter Erstellen einer Verbindung mit dem Verbindungsassistenten.

Einschränkungen

- Es gibt Beschränkungen für Transit-Gateway-Anlagen an die VPCs in den Konten Produktion, Qualitätssicherung und Entwicklung. Weitere Informationen finden Sie unter Transit-Gateway-Anlagen zu einer VPC.
- Bei der Erstellung und Verwendung von Direct Connect-Gateways gibt es Grenzen. Weitere Informationen finden Sie unter AWS Direct Connect Connect-Kontingente.

Architektur

Zielarchitektur

Die folgende Beispielarchitektur bietet eine wiederverwendbare Lösung für die Bereitstellung von Transit-VIFs mit Transit Gateway Connect-Anhängen. Diese Architektur bietet Ausfallsicherheit durch die Verwendung mehrerer Direct Connect-Standorte. Weitere Informationen finden Sie unter Maximale Ausfallsicherheit in der Direct Connect-Dokumentation. Das lokale Netzwerk verfügt über Produktions-, QA- und Entwicklungs-VRFs, die auf AWS erweitert und mithilfe von dedizierten Routing-Tabellen isoliert werden.

In der AWS-Umgebung sind zwei Konten für die Erweiterung der VRFs vorgesehen: ein Direct Connect-Konto und ein Netzwerk-Hub-Konto. Das Direct Connect-Konto enthält die Verbindungs- und Transit-VIFs für jeden Router. Sie erstellen die Transit-VIFs über das Direct Connect-Konto, stellen sie jedoch auf dem Netzwerk-Hub-Konto bereit, sodass Sie sie dem Direct Connect-Gateway im Netzwerk-Hub-Konto zuordnen können. Das Netzwerk-Hub-Konto enthält das Direct Connect-Gateway und das Transit-Gateway. Die AWS-Ressourcen sind wie folgt verbunden:

1. Transit-VIFs verbinden die Router an den Direct Connect-Standorten mit AWS Direct Connect im Direct Connect-Konto.
2. Eine Transit-VIF verbindet Direct Connect mit dem Direct Connect-Gateway im Netzwerk-Hub-Konto.
3. Eine Transit-Gateway-Zuordnung verbindet das Direct Connect-Gateway mit dem Transit-Gateway im Netzwerk-Hub-Konto.
4. Transit Gateway Connect-Anhänge verbinden das Transit-Gateway mit den VPCs in den Produktions-, QA- und Entwicklungskonten.

Transit VIF-Architektur

Das folgende Diagramm zeigt die Konfigurationsdetails für die Transit-VIFs. Diese Beispielarchitektur verwendet ein VLAN für die Tunnelquelle, Sie könnten aber auch ein Loopback verwenden.

Im Folgenden finden Sie die Konfigurationsdetails, z. B. autonome Systemnummern (ASNs), für die Transit-VIFs.

Ressource	Item	Detail
Router-01	ASN	65534
Router-02	ASN	65534
Router-03	ASN	65534
Router-04	ASN	65534
Direct-Connect-Gateway	ASN	64601

Transit Gateway	ASN	64600
	CIDR-Block	10,100,254,0/24

Transit Gateway Connect-Architektur

Das folgende Diagramm und die folgenden Tabellen beschreiben, wie ein einzelnes VRF über einen Transit Gateway Connect-Anhang konfiguriert wird. Weisen Sie für zusätzliche VRFs eindeutige Tunnel-IDs, GRE-IP-Adressen des Transit-Gateways und BGP innerhalb von CIDR-Blöcken zu. Die Peer-GRE-IP-Adresse entspricht der Router-Peer-IP-Adresse aus der Transit-VIF.

Die folgende Tabelle enthält Details zur Router-Konfiguration.

Router	Tunnel	IP-Adresse	Quelle	Ziel
Router-01	Tunnel 1	169,254.101,17	VLAN 60	10.100,254,1
			169,254,100,1	
Router-02	Tunnel 11	169,254.101,81	VLAN 61	10,100,254,11
			169,254,100,5	
Router-03	Tunnel 21	169,254.101.145	VLAN 62	10,100,254,21
			169,254,100,9	
Router-04	Tunnel 31	169.254.101.209	VLAN 63	10,100,254,31
			169,254.100,13	

Die folgende Tabelle enthält Einzelheiten zur Konfiguration des Transit-Gateways.

Tunnel	GRE-IP-Adresse des Transit-Gateways	Peer-GRE-IP-Adresse	BGP innerhalb von CIDR-Blöcken
Tunnel 1	10.100.254.1	VLAN 60	169,254,101,16/29

		169,254,100,1	
Tunnel 11	10.100.254.11	VLAN 61	169,254,101,80/29
		169,254,100,5	
Tunnel 21	10.100.254.21	VLAN 62	169,254,101,144/29
		169,254,100,9	
Tunnel 31	10.100.254.31	VLAN 63	169,254,101,208/29
		169,254.100,13	

Bereitstellung

Im Abschnitt Epics wird beschrieben, wie Sie eine Beispielkonfiguration für eine einzelne VRF auf mehreren Kundenroutern bereitstellen. Nachdem die Schritte 1—5 abgeschlossen sind, können Sie neue Transit Gateway Connect-Anlagen erstellen, indem Sie die Schritte 6—7 für jedes neue VRF, das Sie auf AWS erweitern, ausführen:

1. Erstellen Sie das Transit-Gateway.
2. Erstellen Sie eine Transit Gateway Gateway-Routentabelle für jedes VRF.
3. Erstellen Sie die virtuellen Transitschnittstellen.
4. Erstellen Sie das Direct Connect-Gateway.
5. Erstellen Sie die virtuelle Direct Connect-Gateway-Schnittstelle und die Gateway-Zuordnungen mit zulässigen Präfixen.
6. Erstellen Sie den Transit Gateway Connect-Anhang.
7. Erstellen Sie die Transit Gateway Connect-Peers.
8. Ordnen Sie den Transit Gateway Connect-Anhang der Routentabelle zu.
9. Kündigen Sie Routen zu den Routern an.

Tools

AWS-Services

- AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- AWS Transit Gateway ist ein zentraler Hub, der virtuelle private Clouds (VPCs) und lokale Netzwerke verbindet.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Plane die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerdefinierte Architekturdiagramme.	1. Laden Sie im Abschnitt Anlagen die Schemavorlage herunter. 2. Öffnen Sie das angehängte Diagramm in Microsoft Office PowerPoint. 3. Passen Sie auf der Folie mit der Architekturübersicht das Architekturdiagramm an Ihre Umgebung an. Identifizieren Sie die lokalen VRFs, die auf Ihre AWS-Umgebung erweitert werden müssen. 4. Passen Sie auf der Transit VIF-Folie das Architekturdiagramm an. Identifizieren Sie die AS-Nummer	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n der Router, des Direct Connect-Gateways und des Transit-Gateways. Identifiz ieren Sie die IP-Adressen an jedem Ende der Transit-VIF. 5. Passen Sie auf der Folie Transit Gateway Connect ein Architekturdiagramm für jedes VRF an. Identifiz ieren Sie alle erforderlichen IP-Adressen, die für die Konfiguration der Router und der Transit Gateway Connect-Peers erforderlich sind.	

Erstellen Sie die Transit Gateway Gateway-Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Transit-G ateway.	1. Melden Sie sich beim Netzwerk-Hub-Konto an. 2. Folgen Sie den Anweisung en unter Ein Transit-G ateway erstellen. Beachten Sie für dieses Muster Folgendes: • Geben Sie für Amazon Side Autonomous System Number (ASN) eine eindeutige ASN ein. Für die Zwecke dieses	Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispiels lautet die ASN. `64600` • Wählen Sie DNS-Unterstützung aus. • Für diese Beispielarchitektur sind VPN-ECMP-Unterstützung, Standardroutentabellenzuweisung, Standardroutentabellenverlängerung und Multicast-Unterstützung nicht erforderlich. • Geben Sie für CIDR-Blöcke des Transit-Gateways die IPv4-CIDR-Blöcke für Ihr Transit-Gateway ein. Für die Zwecke dieses Beispiels lautet der CIDR-Block. `10.100.254.0/24`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routentabelle des Transit-Gateways.	Folgen Sie den Anweisungen unter Erstellen einer Transit-Gateway-Routentabelle. Beachten Sie für dieses Muster Folgendes: • Geben Sie im Feld Name Tag einen Namen für die Transit-Gateway-Routentabelle ein. Wir empfehlen, einen Namen zu verwenden, der dem VRF entspricht, z. B. `routetable-dev-vrf` • Wählen Sie als Transit-Gateway-ID das Transit-Gateway aus, das Sie zuvor erstellt haben.	Cloud-Architekt, Netzwerkadministrator

Erstellen Sie die virtuellen Transitschnittstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die virtuellen Transitschnittstellen.	1. Melden Sie sich beim Direct Connect-Konto an. 2. Folgen Sie den Anweisungen unter Erstellen einer virtuellen Transitschnittstelle zum Direct Connect-Gateway. Beachten Sie Folgendes für dieses Muster: • Geben Sie unter Name der virtuellen Schnittst	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	elle einen Namen für die Transit-VIF ein. Wir empfehlen, einen Namen zu verwenden, der dem Router entspricht, z. B. `transit-vif-router 01` • Wählen Sie unter Verbindung den Router aus, z. `router-01` B. • Geben Sie für Besitzer der virtuellen Schnittst elle die Konto-ID des Netzwerk-Hub-Kontos ein. Anweisungen finden Sie unter Ihre AWS-Konto -ID anzeigen. • Treffen Sie für Direct Connect Gateway keine Auswahl. In einem nachfolgenden Schritt fügen Sie das Direct Connect-Gateway hinzu. • Geben Sie für VLAN das VLAN des Routers ein, z. B. `60` • Geben Sie für BGP ASN die ASN des Routers ein, z. B. `65534` • Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie IPv4 aus. • Geben Sie für Ihre Router-Peer-IP die Router-Peer-IP-Adresse ein, z. B. `169.254.100.1` • Geben Sie für Amazon-Router-Peer-IP die Amazon-Router-Peer-IP ein, z. `169.254.100.2` B. • Für den BGP-Authentifizierungsschlüssel ist ein Passwort erforderlich. Wenn dieses Feld leer gelassen wird, erstellt AWS einen Schlüssel, auf den nur in diesem Konto zugegriffen werden kann. 3. Wiederholen Sie diese Anweisungen, um alle Transit-VIFs für die VRF zu erstellen.	

Erstellen Sie die Direct Connect-Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Direct Connect-Gateway.	1. Melden Sie sich beim Netzwerk-Hub-Konto an.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Folgen Sie den Anweisungen unter Erstellen eines Direct Connect-Gateways. Beachten Sie für dieses Muster Folgendes: • Geben Sie für ASN auf Amazon-Seite die ASN des Direct Connect-Gateways ein, z. B. `64601` • Wählen Sie kein virtuelles privates Gateway.	
Schließen Sie das Direct Connect-Gateway an die Transit-VIFs an.	1. Öffnen Sie im Netzwerk-Hub-Konto die AWS Direct Connect Connect-Konsole unter https://console.aws.amazon.com/directconnect/v2/. 2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus. 3. Wählen Sie eine neue Transit-VIF aus und klicken Sie dann auf Akzeptieren. 4. Wählen Sie das Direct Connect-Gateway aus, das Sie erstellt haben. 5. Wiederholen Sie diese Anweisungen für jedes Transit-VIF.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Direct Connect-Gateway-Verknüpfungen mit zulässigen Präfixen.	Folgen Sie im Netzwerk-Hub-Konto den Anweisungen unter So ordnen Sie ein Transit-Gateway zu. Beachten Sie für dieses Muster Folgendes: • Wählen Sie für Gateways das Transit-Gateway aus, das Sie zuvor erstellt haben. • Geben Sie unter Zulässige Präfixe den CIDR-Block ein, der dem Transit-Gateway zugewiesen ist, z. B. **`10.100.254.0/24`** Durch das Erstellen dieser Zuordnung wird automatisch ein Transit Gateway Gateway-Anhang mit einem Direct Connect Gateway-Ressourcentyp erstellt. Dieser Anhang muss keiner Transit-Gateway-Routentabelle zugeordnet werden.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Transit Gateway Connect-Anhang.	1. Öffnen Sie im Netzwerk-Hub-Konto die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. 2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge). 3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus. 4. Geben Sie unter Namenstag einen Namen für den Anhang ein. Wir empfehlen, einen Namen zu verwenden, der dem VRF entspricht, z. B. `PROD-VRF` 5. Wählen Sie als Transit-Gateway-ID das Transit-Gateway aus, das Sie zuvor erstellt haben. 6. Wählen Sie bei Attachment type (Anhangstyp) die Option Connect aus. 7. Wählen Sie für Transport Attachment ID das Direct Connect-Gateway aus, das Sie zuvor erstellt haben. 8. Wählen Sie Create Transit Gateway Attachment	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Transit-Gateway-Anhang erstellen) aus. 9. Wiederholen Sie diesen Schritt für jedes VRF, das Sie erweitern möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Transit Gateway Connect-Peers.	1. Folgen Sie im Netzwerk-Hub-Konto den Anweisungen unter Erstellen eines Transit Gateway Connect-Peers (GRE-Tunnel). Beachten Sie Folgendes für dieses Muster: • Geben Sie unter Namenstag einen Namen für den Transit Gateway Connect-Peer ein. Wir empfehlen, einen Namen zu verwenden, der dem Router entspricht, z. B. `connectpeer-router01` • Geben Sie für die GRE-Adresse des Transit-Gateways die zugewiesene IP-Adresse aus dem CIDR-Block des Transit-Gateways ein, z. B. `10.100.254.1` • Geben Sie als Peer-GRE-Adresse die IP-Adresse ein, die dem VLAN zugewiesen ist, das auf dem Router für die Transit-VIF erstellt wurde, z. B. `169.254.100.1` Vorausgesetzt, dass AWS die IP-Adresse erreichen kann, können Sie eine beliebige	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schnittstelle wie VLAN oder Loopback für die Peer-GRE-Adresse verwenden. • Geben Sie für BGP Inside CIDR Blocks (IPv4) die IP-Adresse des BGP inside CIDR-Blocks ein, z. B. `169.254.101.16/29` • Geben Sie für Peer ASN die ASN des Routers ein, z. B. `65534` 2. Wiederholen Sie diese Anweisungen, um für jeden Router einen GRE-Tunnel zu erstellen.	

Kündigen Sie Routen zu den Routern an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Werben Sie für die Routen.	Ordnen Sie den neuen Transit Gateway Connect-Anhang der Routentabelle zu, die Sie zuvor für diese VRF erstellt haben. Ordnen Sie beispielsweise den Connect-Anhang des Production Transit Gateway der `Production-VRF` Routentabelle zu.	Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellen Sie eine statische Route für das Präfix, das den Routern angekündigt wird. 1. Melden Sie sich beim Netzwerk-Hub-Konto an. 2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. 3. Wählen Sie im Navigationsbereich unter Transit Gateways die Option Transit Gateway-Routentabellen aus. 4. Wählen Sie die `Production-VRF` -Routing-Tabelle aus. 5. Wählen Sie im Menü Aktionen die Option Statische Route erstellen aus. 6. Geben Sie für CIDR den CIDR-Block für die angekündigte Route zum Transit-Gateway-Anhang in der Ziel-VPC ein, z. B. `10.100.1.0/24` 7. Wählen Sie für Choose Attachment den entsprechenden Transit Gateway Connect-Anhang aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie Create static route (Statische Route erstellen) aus.	

Zugehörige Ressourcen

AWS-Dokumentation

- Direct Connect-Dokumentation
  - Arbeiten mit Direct Connect-Gateways
  - Transit-Gateway-Verknüpfungen
  - Virtuelle Schnittstellen von AWS Direct Connect
- Transit Gateway Gateway-Dokumentation
  - Arbeiten mit Transit-Gateways
  - Transit-Gateway-Anlagen an ein Direct Connect-Gateway
  - Transit Gateway Connect-Anlagen und Transit Gateway Connect-Peers
  - Einen Transit Gateway Connect-Anhang erstellen

AWS-Blogbeiträge

- Segmentierung hybrider Netzwerke mit AWS Transit Gateway Connect
- Verwenden von AWS Transit Gateway Connect zur Erweiterung von VRFs und zur Erhöhung der IP-Präfix-Advertising

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Amazon SNS-Benachrichtigungen abrufen, wenn sich der Schlüsselstatus eines AWS KMS-Schlüssels ändert

Erstellt von Shubhamsora (AWS), Boll Raj Jayarajan (AWS) und Navdeep Pareek (AWS)

Code-Repository: aws-kms-deletion-notification	Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; Cloudnativ; DevOpsSicherheit, Identität, Compliance
Workload: Alle anderen Workloads	AWS-Services: Amazon EventBridge; AWS KMS; Amazon SNS	

Übersicht

Die einem AWS Key Management Service (AWS KMS)-Schlüssel zugeordneten Daten und Metadaten gehen verloren, wenn dieser Schlüssel gelöscht wird. Das Löschen ist irreversibel und Sie können verlorene Daten (einschließlich verschlüsselter Daten) nicht wiederherstellen. Sie können Datenverlust verhindern, indem Sie ein Benachrichtigungssystem einrichten, das Sie über Statusänderungen der Schlüsselstatus Ihrer AWS KMS-Schlüssel informiert.

Dieses Muster zeigt Ihnen, wie Sie Statusänderungen an AWS KMS-Schlüsseln überwachen, indem Sie Amazon EventBridge und Amazon Simple Notification Service (Amazon SNS) verwenden, um automatisierte Benachrichtigungen auszugeben, wenn sich der Schlüsselstatus eines AWS KMS-Schlüssels in `Disabled` oder ändert`PendingDeletion`. Wenn ein Benutzer beispielsweise versucht, einen AWS KMS-Schlüssel zu deaktivieren oder zu löschen, erhalten Sie eine E-Mail-Benachrichtigung mit Details über die versuchte Statusänderung. Sie können dieses Muster auch verwenden, um das Löschen von AWS KMS-Schlüsseln zu planen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einem AWS Identity and Access Management (IAM)-Benutzer
- Ein AWS KMS-Schlüssel

Architektur

Technologie-Stack

- Amazon EventBridge
- AWS Key Management Service (AWS KMS)
- Amazon Simple Notification Service (Amazon SNS)

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur zum Erstellen eines automatisierten Überwachungsprozesses und eines Benachrichtigungsprozesses zur Erkennung von Änderungen am Status eines AWS KMS-Schlüssels.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer deaktiviert oder plant das Löschen eines AWS KMS-Schlüssels.
2. Eine - EventBridge Regel wertet das geplante - `Disabled` oder -`PendingDeletion`Ereignis aus.
3. Die EventBridge Regel ruft das Amazon SNS-Thema auf.
4. Amazon SNS sendet eine E-Mail-Benachrichtigung an die Benutzer.

Hinweis: Sie können die E-Mail-Nachricht an die Anforderungen Ihrer Organisation anpassen. Wir empfehlen, Informationen zu den Entitäten einzufügen, in denen der AWS KMS-Schlüssel verwendet wird. Dies kann Benutzern helfen, die Auswirkungen des Löschens des AWS KMS-Schlüssels zu verstehen. Sie können auch eine Erinnerungs-E-Mail-Benachrichtigung planen, die ein oder zwei Tage vor dem Löschen des AWS KMS-Schlüssels gesendet wird.

Automatisierung und Skalierung

Der AWS- CloudFormation Stack stellt alle erforderlichen Ressourcen und Services bereit, damit dieses Muster funktioniert. Sie können das Muster unabhängig in einem einzigen Konto implementieren oder indem Sie AWS CloudFormation StackSets für mehrere unabhängige Konten oder Organisationseinheiten in AWS Organizations verwenden.

Tools

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen hinweg zu verwalten. Die CloudFormation Vorlage für dieses Muster beschreibt alle gewünschten AWS-Ressourcen und stellt diese Ressourcen für Sie CloudFormation bereit und konfiguriert sie.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen und AWS-Services bereit und leitet diese Daten an Ziele wie AWS Lambda weiter. EventBridge vereinfacht den Prozess der Erstellung ereignisgesteuerter Architekturen.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.

Code

Der Code für dieses Muster ist im GitHub Repository AWS KMS-Schlüssel überwachen, deaktivieren und geplantes Löschen verfügbar.

Sekunden

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das GitHub AWS KMS-Schlüssel überwachende Deaktivierungs-Repository und das geplante Löschen auf Ihren lokalen Computer, indem Sie den folgenden Befehl ausführen:	AWS-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/aws-kms-deletion-notification`	
Aktualisieren Sie die Parameter der Vorlage.	Öffnen Sie in einem Code-Editor die `Alerting-KMS-Events.yaml` CloudFormation Vorlage, die Sie aus dem Repository geklont haben, und aktualisieren Sie dann die folgenden Parameter: • `DestinationEmailAddress` Geben Sie für eine aktive E-Mail-Adresse ein, die Sie für den Empfang der SNS-Benachrichtigung verwenden möchten. • `SNSTopicName` Geben Sie für einen Namen für Ihr SNS-Thema ein.	AWS-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Wählen Sie im Navigationsbereich Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 4. Wählen Sie auf der Seite Vorlage angeben für Vorlagenquelle die Option Vorlagendatei hochladen aus. 5. Wählen Sie Datei auswählen, wählen Sie die `Alerting-KMS-Events.yaml` Datei aus Ihrem geklonten GitHub Repository aus und klicken Sie dann auf Weiter. 6. Geben Sie für Stack-Name Ihren Stack-Namen ein. 7. Wählen Sie Absenden aus.	AWS-Administrator, Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Abonnement-E-Mail.	Nachdem die CloudFormation Vorlage erfolgreich bereitges	AWS-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tellt wurde, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die E-Mail-Adresse, die Sie in der CloudFormation Vorlage angegeben haben. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen. Weitere Informationen finden Sie unter Bestätigen des Abonnements im Amazon SNS-Entwicklerhandbuch.	

Testen der Abonnementbenachrichtigung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie AWS KMS-Schlüssel.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS KMS-Konsole . 2. Um die Region zu ändern, wählen Sie den Namen der aktuell angezeigten Region und dann die Region aus, zu der Sie wechseln möchten. 3. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel. 4. Aktivieren Sie das Kontrollkästchen für den AWS	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	KMS-Schlüssel, den Sie aktivieren oder deaktivieren möchten. 5. Um den AWS KMS-Schlüssel zu deaktivieren, wählen Sie Schlüsselaktionen und dann Deaktivieren aus.	
Validieren Sie das Abonnement.	Bestätigen Sie, dass Sie die Amazon SNS-Benachrichtigungs-E-Mail erhalten haben.	AWS-Administrator

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den CloudFormation Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Klicken Sie im Navigationsbereich auf Stacks. 3. Wählen Sie den Stack aus, den Sie zuvor erstellt haben, und klicken Sie dann auf Löschen.	AWS-Administrator

Zugehörige Ressourcen

- AWS CloudFormation (AWS-Dokumentation)
- Erstellen eines Stacks in der AWS- CloudFormation Konsole (AWS- CloudFormation Dokumentation)

- Erstellen von ereignisgesteuerten Architekturen in AWS (Dokumentation zu AWS Workshop Studio)
- Bewährte Methoden für AWS Key Management Service (AWS-Whitepaper)
- Bewährte Sicherheitsmethoden für AWS Key Management Service (AWS KMS-Entwicklerhandbuch)

Zusätzliche Informationen

Amazon SNS bietet standardmäßig Verschlüsselung während der Übertragung. Um den bewährten Methoden für die Sicherheit gerecht zu werden, können Sie auch die serverseitige Verschlüsselung für Amazon SNS mithilfe eines vom Kunden verwalteten AWS KMS-Schlüssels aktivieren.

Mainframe-Modernisierung: DevOps auf AWS mit Micro Focus

Erstellt von Kevin Yung (AWS)

Quelle: IBM z/OS Mainframe	Ziel: AWS	R-Typ: N/A
Umgebung: PoC oder Pilotprojekt	Technologien: DevOps; Infrastruktur	AWS-Services: Amazon EC2; AWS CloudFormation; AWS CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS Systems Manager ; AWS CodePipeline

Übersicht

Herausforderungen für Kunden

Organisationen, die Kernanwendungen auf Mainframe-Hardware ausführen, stehen in der Regel vor einigen Herausforderungen, wenn die Hardware hochskaliert werden muss, um den Anforderungen digitaler Innovationen gerecht zu werden. Zu diesen Herausforderungen gehören die folgenden Einschränkungen.

- Mainframe-Entwicklungs- und Testumgebungen können aufgrund der Unflexibilität von Mainframe-Hardwarekomponenten und der hohen Änderungskosten nicht skaliert werden.
- Die Mainframe-Entwicklung steht vor Qualifikationsengpässen, da neue Entwickler nicht vertraut sind und nicht an den herkömmlichen Mainframe-Entwicklungstools interessiert sind. Moderne Technologie wie Container, Continuous Integration/Continuous Delivery (CI/CD)-Pipelines und moderne Test-Frameworks sind in der Mainframe-Entwicklung nicht verfügbar.

Musterergebnisse

Um diese Herausforderungen zu bewältigen, haben Amazon Web Services (AWS) und Micro Focus, ein AWS Partner Network (APN)-Partner, zusammengearbeitet, um dieses Muster zu erstellen. Die Lösung soll Ihnen helfen, die folgenden Ergebnisse zu erzielen.

- Die Produktivität der Entwickler wurde verbessert. Entwicklern können innerhalb weniger Minuten neue Mainframe-Entwicklungs-Instances zugewiesen werden.

- Verwenden Sie die AWS Cloud, um neue Mainframe-Testumgebungen mit praktisch unbegrenzter Kapazität zu erstellen.
- Schnelle Bereitstellung einer neuen Mainframe-CI/CD-Infrastruktur. Die Bereitstellung auf AWS kann innerhalb einer Stunde mithilfe von AWS CloudFormation und AWS Systems Manager abgeschlossen werden.
- Native Verwendung von AWS- DevOps Tools für die Mainframe-Entwicklung, einschließlich AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy, CodePipelineAWS und Amazon Elastic Container Registry (Amazon ECR).
- Wandeln Sie die traditionelle Wasserfallentwicklung in agile Entwicklung in Mainframe-Projekten um.

Zusammenfassung der Technologien

In diesem Muster enthält der Ziel-Stack die folgenden Komponenten.

Logische Komponenten	Implementierungslösungen	Beschreibung
Quellcode-Repositorys	Micro Focus AccuRev Server, CodeCommitAmazon ECR	Verwaltung von Quellcode – Die Lösung verwendet zwei Arten von Quellcode. • Mainframe-Quellcode, z. B. COBOL, JCL usw. • AWS-Infrastrukturvorlagen und Automatisierungsskripts Beide Arten von Quellcode benötigen Versionskontrolle, werden aber in verschiedenen SCMs verwaltet. Quellcode, der auf Mainframe- oder Micro Focus Enterprise Servers bereitgestellt wird, wird in Micro Focus AccuRev Server verwaltet. AWS-Vorlagen

		und Automatisierungsskripts werden in verwaltet CodeCommit. Amazon ECR wird für die Docker-Image-Repositorys verwendet.
Enterprise-Entwickler-Instances	Amazon Elastic Compute Cloud (Amazon EC2), Micro Focus Enterprise Developer für Eclipse	Mainframe-Entwickler können Code in Amazon EC2 entwickeln, indem sie Micro Focus Enterprise Developer für Eclipse verwenden. Dadurch entfällt die Notwendigkeit, sich zum Schreiben und Testen von Code auf Mainframe-Hardware zu verlassen.
Micro-Focus-Lizenzverwaltung	Micro Focus License Manager	Für eine zentrale Verwaltung und Verwaltung von Micro-Focus-Lizenzen verwendet die Lösung Micro Focus License Manager, um die erforderliche Lizenz zu hosten.
CI/CD-Pipelines	CodePipeline, CodeBuild, CodeDeploy, Micro Focus Enterprise Developer in einem Container, Micro Focus Enterprise Test Server in einem Container, Micro Focus Enterprise Server	Mainframe-Entwicklungsteams benötigen CI/CD-Pipelines, um Codekompilierung, Integrationstests und Regressionstests durchzuführen. In AWS CodeBuild kann CodePipeline und nativ mit Micro Focus Enterprise Developer und Enterprise Test Server in einem Container arbeiten.

Voraussetzungen und Einschränkungen

Voraussetzungen

Name	Beschreibung
py3270	py3270 ist eine Python-Schnittstelle zu x3270, einem IBM 3270-Terminal-Emulator. Es stellt eine API für einen x3270- oder s3270-Sub prozess bereit.
x3270	x3270 ist ein IBM 3270-Terminal-Emulator für das X Window System und Windows. Dies kann vom Entwickler für lokale Komponent entests verwendet werden.
Robot-Framework-Mainframe-3270-Library	Mainframe3270 ist eine Bibliothek für Robot Framework, die auf dem Projekt py3270 basiert.
Micro Focus Verastream	Micro Focus Verastream ist eine Integrati onsplattform, mit der Mainframe-Komponenten so getestet werden können, wie mobile Apps, Webanwendungen und SOA-Webservices getestet werden.
Micro Focus Unified Function Testing (UFT)-Ins tallationsprogramm und Lizenz	Micro Focus Unified Function Testing ist Software, die Funktions- und Regressio nstestautomatisierung für Softwareanwendunge n und -umgebungen bietet.
Installationsprogramm und Lizenz für Micro Focus Enterprise Server	Enterprise Server bietet die Laufzeitumgebung für Mainframe-Anwendungen.
Installationsprogramm und Lizenz für Micro Focus Enterprise Test Server	Micro Focus Enterprise Test Server ist eine Testumgebung für IBM Mainframe-Anwendun gen

Micro-Focus- AccuRev Installationsprogramm und -Lizenz für Server und Micro-Focus-AccuRev Installationsprogramm und -Lizenz für Windows- und Linux-Betriebssysteme	AccuRev bietet Quellcodeverwaltung (SCM). Das AccuRev System wurde für die Verwendung durch ein Team von Personen entwickelt, die eine Reihe von Dateien entwickeln.
Micro Focus Enterprise Developer für Eclipse – Installationsprogramm, Patch und Lizenz	Enterprise Developer bietet Mainframe-Entwicklern eine Plattform zur Entwicklung und Wartung der Kern-Mainframe-Online- und Batch-Anwendungen.

Einschränkungen

- Das Erstellen eines Windows-Docker-Images wird in nicht unterstützt CodeBuild. Dieses gemeldete Problem benötigt Unterstützung von Windows-Kernel/HCS- und Docker-Teams. Die Problemumgehung besteht darin, mithilfe von Systems Manager ein Docker-Image-Build-Runbook zu erstellen. Dieses Muster verwendet die Problemumgehung, um Micro Focus Enterpise Developer für Eclipse und Micro Focus Enterprise Test Server Container-Images zu erstellen.
- Die Virtual Private Cloud (VPC)-Konnektivität von CodeBuild wird in Windows noch nicht unterstützt, daher verwendet das Muster Micro Focus License Manager nicht, um Lizenzen in Containern von Micro Focus Enterprise Developer und Micro Focus Enterprise Test Server zu verwalten.

Produktversionen

- Micro Focus Enterprise Developer 5.5 oder höher
- Micro Focus Enterprise Test Server 5.5 oder höher
- Micro Focus Enterprise Server 5.5 oder höher
- Micro Focus AccuRev 7.x oder höher
- Windows Docker-Basis-Image für Micro Focus Enterprise Developer und Enterprise Test Server: Microsoft/dotnet-framework-4.7.2-runtime
- Linux-Docker-Basis-Image für AccuRev Client: amazonlinux:2

Architektur

Mainframe-Umgebung

Bei der herkömmlichen Mainframe-Entwicklung müssen die Entwickler Mainframe-Hardware verwenden, um Programme zu entwickeln und zu testen. Sie haben Kapazitätsbeschränkungen, z. B. eingeschränkte Millionen Anweisungen pro Sekunde (MIPS) für die Entwicklungs-/Testumgebung, und sie müssen sich auf die Tools verlassen, die auf den Mainframe-Computern verfügbar sind.

In vielen Organisationen folgt die Mainframe-Entwicklung der Wasserfallentwicklungsmethode, wobei sich Teams auf lange Zyklen verlassen, um Änderungen zu veröffentlichen. Diese Release-Zyklen sind in der Regel länger als die Entwicklung digitaler Produkte.

Das folgende Diagramm zeigt mehrere Mainframe-Projekte, die Mainframe-Hardware für ihre Entwicklung gemeinsam nutzen. Bei Mainframe-Hardware ist es teuer, eine Entwicklungs- und Testumgebung für mehr Projekte zu skalieren.

AWS-Architektur

Dieses Muster erweitert die Mainframe-Entwicklung auf die AWS Cloud. Zunächst verwendet es Micro Focus AccuRev SCM, um den Mainframe-Quellcode auf AWS zu hosten. Anschließend werden Micro Focus Enterprise Developer und Micro Focus Enterprise Test Server zum Erstellen und Testen des Mainframe-Codes auf AWS verfügbar.

In den folgenden Abschnitten werden die drei Hauptkomponenten des Musters beschrieben.

1. SCM

In AWS verwendet das Muster Micro Focus, AccuRev um eine Reihe von SCM-Workspaces und Versionskontrolle für den Mainframe-Quellcode zu erstellen. Die streambasierte Architektur ermöglicht die parallele Mainframe-Entwicklung für mehrere Teams. Um eine Änderung zusammenzuführen, AccuRev verwendet das Konzept Hochstufen. Um diese Änderung zu anderen Workspaces hinzuzufügen, AccuRev verwendet das Aktualisierungskonzept.

Auf Projektebene kann jedes Team einen oder mehrere Streams in erstellen AccuRev , um Änderungen auf Projektebene zu verfolgen. Diese werden als Projektstreams bezeichnet. Diese Projektstreams werden vom selben übergeordneten Stream geerbt. Der übergeordnete Stream wird verwendet, um die Änderungen aus verschiedenen Projektstreams zusammenzuführen.

Jeder Projektstream kann Code zu hochstufen AccuRev, und es wird ein Auslöser für die Hochstufung nach dem Start der AWS CI/CD-Pipeline eingerichtet. Der erfolgreiche Build für eine Projektstream-Änderung kann für weitere Regressionstests in den übergeordneten Stream hochgestuft werden.

Normalerweise wird der übergeordnete Stream als Systemintegrations-Stream bezeichnet. Wenn es eine Hochstufung von einem Projekt-Stream zu einem Systemintegrations-Stream gibt, initiiert ein Auslöser nach der Hochstufung eine andere CI/CD-Pipeline, um Regressionstests durchzuführen.

Zusätzlich zum Mainframe-Code enthält dieses Muster AWS- CloudFormation Vorlagen, Systems Manager Automation-Dokumente und Skripts. Gemäß den infrastructure-as-code bewährten Methoden sind sie in AWS versionsgesteuert CodeCommit.

Wenn Sie Mainframe-Code für die Bereitstellung wieder mit einer Mainframe-Umgebung synchronisieren müssen, bietet Micro Focus die Enterprise-Sync-Lösung, die Code aus dem AccuRev SCM wieder mit dem Mainframe-SCM synchronisiert.

2. Entwickler- und Testumgebungen

In einer großen Organisation ist es schwierig, mehr als einhundert oder sogar mehr als eintausend Mainframe-Entwickler zu skalieren. Um diese Einschränkung zu beheben, verwendet das Muster Amazon EC2 Windows-Instances für die Entwicklung. Auf den Instances sind die Tools Micro Focus Enterprise Developer für Eclipse installiert. Der Entwickler kann alle Mainframe-Codetests und Debuggings lokal auf der Instance durchführen.

AWS Systems Manager State Manager- und Automation-Dokumente werden verwendet, um die Bereitstellung der Entwickler-Instance zu automatisieren. Die durchschnittliche Zeit zum Erstellen einer Entwickler-Instance beträgt 15 Minuten. Die folgenden Software und Konfigurationen werden vorbereitet.

- AccuRev Windows-Client zum Auschecken und Übergeben von Quellcode in AccuRev
- Micro Focus Enterprise Developers for Eclipse Tool zum lokalen Schreiben, Testen und Debuggen von Mainframe-Code
- Open-Source-Testframeworks Python-Testframework für verhaltensgesteuerte Entwicklung (BDD) Verhalten, py3270 und den x3270-Emulator zum Erstellen von Skripts zum Testen von Anwendungen
- Ein Docker-Entwickler-Tool zum Erstellen des Docker-Images für Enterprise Test Server und zum Testen der Anwendung im Docker-Container für Enterprise Test Server

Im Entwicklungszyklus verwenden Entwickler die EC2-Instance, um Mainframe-Code lokal zu entwickeln und zu testen. Wenn die lokalen Änderungen erfolgreich getestet wurden, stufen Entwickler die Änderung auf den AccuRev Server hoch.

3. CI/CD-Pipelines

Im Muster werden CI/CD-Pipelines für Integrationstests und Regressionstests vor der Bereitstellung in der Produktionsumgebung verwendet.

Wie im Abschnitt SCM erläutert, AccuRev verwendet zwei Arten von Streams: einen Projektstream und einen Integrationsstream. Jeder Stream ist mit CI/CD-Pipelines verbunden. Um die Integration zwischen dem AccuRev Server und AWS durchzuführen CodePipeline, verwendet das Muster AccuRev ein Skript nach der Hochstufung, um ein Ereignis zu erstellen, das CI/CD initiiert.

Wenn ein Entwickler beispielsweise eine Änderung an einem Projekt-Stream in hochstuft AccuRev, initiiert er ein Skript nach der Hochstufung, das in AccuRev Server ausgeführt wird. Anschließend lädt das Skript die Metadaten der Änderung in einen Amazon Simple Storage Service (Amazon S3)-Bucket hoch, um ein Amazon S3-Ereignis zu erstellen. Dieses Ereignis initiiert die Ausführung einer CodePipeline konfigurierten Pipeline.

Derselbe Mechanismus zur Ereignisinitiierung wird für den Integrations-Stream und die zugehörigen Pipelines verwendet.

In der CI/CD-Pipeline CodePipeline verwendet CodeBuild mit dem Micro Focus AccuRev Linux-Client-Container, um den neuesten Code aus den AccuRev Streams anzuzeigen. Dann beginnt die Pipeline CodeBuild , den Windows-Container des Micro Focus Enterprise Developer zu verwenden, um den Quellcode zu kompilieren, und den Windows-Container des Micro Focus Enterprise Test Servers in zu verwenden, um Mainframe-Anwendungen CodeBuild zu testen.

Die CI/CD-Pipelines werden mithilfe von AWS- CloudFormation Vorlagen erstellt und der Blueprint wird für neue Projekte verwendet. Durch die Verwendung der Vorlagen dauert es weniger als eine Stunde, bis ein Projekt eine neue CI/CD-Pipeline in AWS erstellt.

Um Ihre Mainframe-Testfunktionen auf AWS zu skalieren, baut das Muster die Micro Focus- DevOps Testsuite, Micro Focus Verastream und Micro Focus UFT-Server auf. Mit den modernen DevOps Tools können Sie so viele Tests in AWS ausführen, wie Sie benötigen.

Ein Beispiel für eine Mainframe-Entwicklungsumgebung mit Micro Focus in AWS ist im folgenden Diagramm dargestellt.

Zieltechnologie-Stack

Dieser Abschnitt bietet einen genaueren Überblick über die Architektur jeder Komponente im Muster.

1. Quellcode-Repository – AccuRev SCM

Micro Focus AccuRev SCM ist für die Verwaltung von Mainframe-Quellcodeversionen eingerichtet. Für hohe Verfügbarkeit AccuRev unterstützt Primär- und Replikatmodi. Operatoren können ein Failover auf das Replikat durchführen, wenn sie Wartungsarbeiten am Primärknoten durchführen.

Um die Antwort der CI/CD-Pipeline zu beschleunigen, verwendet das Muster Amazon CloudWatch Events, um Quellcodeänderungen zu erkennen und den Start der Pipeline zu initiieren.

1. Die CodePipeline ist für die Verwendung einer Amazon S3-Quelle eingerichtet.
2. Eine CloudWatch Ereignisregel ist eingerichtet, um S3-Ereignisse aus einem S3-Quell-Bucket zu erfassen.
3. Die CloudWatch Ereignisregel legt ein Ziel für die Pipeline fest.
4. AccuRev SCM ist so konfiguriert, dass ein Skript nach der Hochstufung lokal ausgeführt wird, nachdem die Hochstufung abgeschlossen ist.
5. AccuRev SCM generiert eine XML-Datei, die die Metadaten der Hochstufung enthält, und das Skript lädt die XML-Datei in den S3-Quell-Bucket hoch.
6. Nach dem Upload sendet der S3-Quell-Bucket Ereignisse, die der CloudWatch Ereignisregel entsprechen, und die CloudWatch Ereignisregel initiiert CodePipeline die Ausführung von .

Wenn die Pipeline ausgeführt wird, startet sie ein CodeBuild Projekt, um einen AccuRev Linux-Client-Container zu verwenden, um den neuesten Mainframe-Code aus einem zugehörigen AccuRev Stream anzuzeigen.

Das folgende Diagramm zeigt eine - AccuRev Server-Einrichtung.

2. Enterprise-Entwicklervorlage

Das Muster verwendet Amazon EC2-Vorlagen, um die Erstellung der Entwickler-Instance zu vereinfachen. Durch die Verwendung von State Manager können Software- und Lizenzeinstellungen konsistent auf EC2-Instances angewendet werden.

Die Amazon EC2-Vorlage baut ihre VPC-Kontexteinstellungen und Standard-Instance-Einstellungen auf und erfüllt die Anforderungen an Unternehmens-Tagging. Mithilfe einer Vorlage kann ein Team seine eigenen neuen Entwicklungs-Instances erstellen.

Wenn eine Entwickler-Instance gestartet wird, indem sie Tags zuordnet, verwendet Systems Manager State Manager, um die Automatisierung anzuwenden. Die Automatisierung umfasst die folgenden allgemeinen Schritte.

1. Installieren Sie die Software Micro Focus Enterprise Developer und installieren Sie Patches.
2. Installieren Sie den Micro Focus- AccuRev Client für Windows.
3. Installieren Sie das vorkonfigurierte Skript, mit dem Entwickler dem AccuRev Stream beitreten können. Initialisieren Sie Eclipse-Workspaces.
4. Installieren Sie Entwicklungstools, einschließlich x3270, py3270 und Docker.
5. Konfigurieren Sie die Lizenzeinstellungen so, dass sie auf einen Micro Focus License Manager Load Balancer verweisen.

Das folgende Diagramm zeigt eine Enterprise-Entwickler-Instance, die von der Amazon EC2-Vorlage erstellt wurde, wobei Software und Konfiguration von State Manager auf die Instance angewendet werden. Enterprise-Entwickler-Instances stellen eine Verbindung zu Micro Focus License Manager her, um ihre Lizenz zu aktivieren.

3. CI/CD-Pipelines

Wie im Abschnitt AWS-Architektur erläutert, gibt es im Muster CI/CD-Pipelines auf Projektebene und Systemintegrations-Pipelines. Jedes Mainframe-Projektteam erstellt eine Pipeline oder mehrere CI/CD-Pipelines zum Erstellen der Programme, die es in einem Projekt entwickelt. Diese Projekt-CI/CD-Pipelines überprüfen den Quellcode aus einem zugehörigen AccuRev Stream.

In einem Projektteam stufen Entwickler ihren Code im zugehörigen AccuRev Stream hoch. Dann initiiert die Hochstufung die Projektpipeline, um den Code zu erstellen und - und -Integrationstests auszuführen.

Jede Projekt-CI/CD-Pipeline verwendet CodeBuild Projekte mit dem Micro Focus Enterprise Developer-Tool Amazon ECR-Image und dem Micro Focus Enterprise Test Server-Tool Amazon ECR-Image.

CodePipeline und CodeBuild werden verwendet, um die CI/CDs-Pipelines zu erstellen. Da CodeBuild und keine Vorabgebühren oder Verpflichtungen CodePipeline haben, zahlen Sie nur für das, was Sie tatsächlich nutzen. Im Vergleich zu Mainframe-Hardware reduziert die AWS-Lösung die Vorlaufzeit für die Hardwarebereitstellung erheblich und senkt die Kosten für Ihre Testumgebung.

In der modernen Entwicklung werden mehrere Testmethoden verwendet. Zum Beispiel testgesteuerte Entwicklung (TDD), BDD und Robot Framework. Mit diesem Muster können Entwickler diese modernen Tools für Mainframe-Tests verwenden. Mit x3270, py3270 und dem Python-Testtool Behave können Sie beispielsweise das Verhalten einer Online-Anwendung definieren. Sie können auch Build Mainframe 3270 Roboter-Framework in diesen CI/CD-Pipelines verwenden.

Das folgende Diagramm zeigt die CI/CD-Pipeline für den Teamstream.

Das folgende Diagramm zeigt den CI/CD-Testbericht des Projekts, der von CodePipeline im Mainframe3270 Robot Framework erstellt wurde.

Das folgende Diagramm zeigt den CI/CD-Testbericht des Projekts, der von CodePipeline in Py3270 und Behave BDD erstellt wurde.

Nachdem Tests auf Projektebene erfolgreich bestanden wurden, wird der getestete Code manuell in den Integrations-Stream in AccuRev SCM hochgestuft. Sie können diesen Schritt automatisieren, nachdem sich die Teams auf die Testabdeckung ihrer Projektpipeline verlassen haben.

Wenn Code hochgestuft wird, überprüft die CI/CD-Pipeline der Systemintegration den zusammengeführten Code und führt Regressionstests durch. Der zusammengeführte Code wird aus allen parallelen Projektstreams hochgestuft.

Je nachdem, wie genau die Testumgebung erforderlich ist, können Kunden mehr CI/CD-Pipelines für die Systemintegration in verschiedenen Umgebungen haben, z. B. UAT, Pre-Production.

In dem Muster sind die in der Systemintegrationspipeline verwendeten Tools Micro Focus Enterprise Test Server, Micro Focus UFT Server und Micro Focus Verastream. All diese Tools können im Docker-Container bereitgestellt und mit verwendet werden CodeBuild.

Nach erfolgreichem Testen der Mainframe-Programme wird das Artefakt mit Versionskontrolle in einem S3-Bucket gespeichert.

Das folgende Diagramm zeigt eine CI/CD-Pipeline für die Systemintegration.

Nachdem das Artefakt erfolgreich in den CI/CD-Pipelines der Systemintegration getestet wurde, kann es für die Produktionsbereitstellung hochgestuft werden.

Wenn Sie Quellcode wieder auf dem Mainframe bereitstellen müssen, bietet Micro Focus die Enterprise-Sync-Lösung, um Quellcode von AccuRev zurück zu Mainframe Endeavour zu synchronisieren.

Das folgende Diagramm zeigt eine CI/CD-Produktionspipeline, die das Artefakt in Micro Focus Enterprise Servers bereitstellt. In diesem Beispiel CodeDeploy orchestriert die Bereitstellung des getesteten Mainframe-Artefakts in Micro Focus Enterprise Server.

Zusätzlich zur Architektur-Anleitung der CI/CD-Pipeline können Sie auch den AWS- DevOps Blogbeitrag Automatisieren von Tausenden von Mainframe-Tests in AWS mit der Micro Focus Enterprise Suite lesen, um weitere Informationen zum Testen von Mainframe-Anwendungen in CodeBuild und zu erhalten CodePipeline. Im Blogbeitrag finden Sie die bewährten Methoden und Details zur Durchführung von Mainframe-Tests in AWS.

Tools

Tools

AWS-Automatisierungstools

- AWS CloudFormation
- Amazon CloudWatch -Ereignisse
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline
- Amazon ECR
- Amazon S3
- AWS Secrets Manager

- AWS Systems Manager

Micro-Focus-Werkzeuge

- Micro Focus Enterprise Developer für Eclipse
- Micro Focus Enterprise Test Server
- Micro Focus Enterprise Server (Produktionsbereitstellung)
- Micro Focus AccuRev
- Micro Focus License Manager
- Micro Focus Verastream Host Integrator
- Micro Focus UFT One

Andere Tools

- x3270
- py3270
- Robot-Framework-Mainframe-3270-Library

Polen

Erstellen der AccuRev SCM-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen primären AccuRev SCM-Server mithilfe von AWS bereit CloudForm ation.		AWS CloudFormation
Erstellen Sie den AccuRev Administratorbenutzer.	Melden Sie sich bei AccuRev SCM Server an und führen Sie den CLI-Befehl aus, um einen Administratorbenutzer zu erstellen.	AccuRev SCM-Serveradminist rator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie AccuRev Streams.	Erstellen Sie AccuRev Streams, die nacheinander von den oberen Streams geerbt werden: Produktion, Systemintegration, Teamstreams.	AccuRev SCM-Administrator
Erstellen Sie die Entwickler AccuRev -Anmeldekonten.	Verwenden Sie AccuRev SCM-CLI-Befehle, um AccuRev Benutzer-Anmeldekonten für Mainframe-Entwickler zu erstellen.	AccuRev SCM-Administrator

Erstellen der Amazon EC2-Startvorlage für Enterprise Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Amazon EC2-Startvorlage mithilfe von AWS bereit CloudFormation.	Verwenden Sie AWS CloudFormation , um eine Amazon EC2-Startvorlage für Micro Focus Enterprise Developer-Instances bereitzustellen. Die Vorlage enthält ein Systems Manager Automation-Dokument für die Micro Focus Enterprise Developer-Instance.	AWS CloudFormation
Erstellen Sie die Enterprise Developer-Instance aus der Amazon EC2-Vorlage.		AWS-Konsolenanmeldung und Mainframe-Entwicklerfähigkeiten

Erstellen des Docker-Images des Micro Focus Enterprise Developer-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Docker-Image des Micro Focus Enterprise Developer-Tools.	Verwenden Sie den Docker-Befehl und das Micro Focus Enterprise Developer-Tool Dockerfile, um das Docker-Image zu erstellen.	Docker
Erstellen Sie das Docker-Repository in Amazon ECR.	Erstellen Sie in der Amazon-ECR-Konsole das Repository für das Micro Focus Enterprise Developer Docker-Image.	Amazon ECR
Verschieben Sie das Docker-Image des Micro Focus Enterprise Developer-Tools zu Amazon ECR.	Führen Sie den Docker-Push-Befehl aus, um das Docker-Image des Enterprise Developer-Tools zu pushen und es im Docker-Repository in Amazon ECR zu speichern.	Docker

Erstellen des Docker-Images von Micro Focus Enterprise Test Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Docker-Image von Micro Focus Enterprise Test Server.	Verwenden Sie den Docker-Befehl und die Docker-Datei des Micro Focus Enterprise Test Server, um das Docker-Image zu erstellen.	Docker
Erstellen Sie das Docker-Repository in Amazon ECR.	Erstellen Sie in der Amazon-ECR-Konsole das Amazon-ECR-Repository für das Docker-Image von Micro Focus Enterprise Test Server.	Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie das Docker-Image des Micro Focus Enterprise Test Servers an Amazon ECR.	Führen Sie den Docker-Push-Befehl aus, um das Docker-Image von Enterprise Test Server in Amazon ECR zu pushen und zu speichern.	Docker

Erstellen der CI/CD-Pipeline für den Team-Stream

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das AWS-CodeCommit Repository.	Erstellen Sie in der -CodeCommit Konsole ein Git-basiertes Repository für Infrastruktur und AWS-CloudFormation Code.	AWS CodeCommit
Laden Sie die AWS-CloudFormation Vorlage und den Automatisierungscode in das CodeCommit Repository hoch.	Führen Sie den Git-Push-Befehl aus, um AWS-CloudFormation Vorlagen- und Automatisierungscode in das Repository hochzuladen.	Git
Stellen Sie die CI/CD-Pipeline des Team-Streams über bereit CloudFormation.	Verwenden Sie die vorbereitete AWS- CloudFormation Vorlage, um eine CI/CD-Pipeline für den Team-Stream bereitzustellen.	AWS CloudFormation

Erstellen der CI/CD-Pipeline für die Systemintegration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Micro Focus UFT Docker-Image.	Verwenden Sie den Docker-Befehl und die Micro Focus	Docker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	UFT Dockerfile, um das Micro Focus Docker-Image zu erstellen.	
Erstellen Sie das Docker-Repository in Amazon ECR für das Micro Focus UFT-Image.	Erstellen Sie in der Amazon ECR-Konsole das Docker-Repository für das Micro Focus UFT-Image.	Amazon ECR
Verschieben Sie das Micro Focus UFT Docker-Image zu Amazon ECR.	Führen Sie den Docker-Push-Befehl aus, um das Docker-Image von Enterprise Test Server in Amazon ECR zu pushen und zu speichern.	Docker
Erstellen Sie das Micro Focus Verastream Docker-Image.	Verwenden Sie den Docker-Befehl und die Micro Focus Verastream Dockerfile, um das Docker-Image zu erstellen .	Docker
Erstellen Sie das Docker-Repository in Amazon ECR für das Micro Focus Verastream-Image.	Erstellen Sie in der Amazon-ECR-Konsole das Docker-Repository für das Micro-Focus-Verastream-Image.	Amazon ECR
Stellen Sie die CI/CD-Pipeline für die Systemintegration über bereit CloudFormation.	Verwenden Sie die vorbereitete AWS- CloudFormation Vorlage, um eine CI/CD-Pipeline für die Systemintegration bereitzustellen.	AWS CloudFormation

CI/CD-Pipeline für die Produktionsbereitstellung erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Micro Focus Enterprise Server mithilfe des AWS-Schnellstarts bereit.	Um Micro Focus Enterpris e Server mithilfe von AWS bereitzustellen CloudForm ation, starten Sie Micro Focus Enterprise Server auf AWS Quick Start.	AWS CloudFormation
Stellen Sie eine CI/CD-Pipeline für die Produktio nsbereitstellung bereit.	Verwenden Sie in der AWS-CloudFormation Konsole die AWS- CloudFormation Vorlage, um eine CI/CD-Pipeline für die Produktio nsbereitstellung bereitzus tellen.	AWS CloudFormation

Zugehörige Ressourcen

Referenzen

- AWS DevOps Blog – Automatisieren Sie Tausende von Mainframe-Tests in AWS mit der Micro Focus Enterprise Suite
- py3270/py3270 GitHub -Repository
- Altran-PT-GDC/Robot-Framework-Mainframe-3270-Library GitHub -Repository
- Willkommen beim Verhalten!
- APN-Partner-Blog – Tag: Micro Focus
- Starten einer Instance über eine Startvorlage

AWS Marketplace

- Micro Focus UFT One

AWS-Schnellstart

- Micro Focus Enterprise Server auf AWS

Aufbewahren von routbarem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze, die keine Workload sind

Erstellt von A Spicer (AWS)

Code-Repository: Nicht weiterleitbares sekundäres CIDRs-Muster	Umgebung: Produktion	Technologien: Infrastruktur; DevOpsManagement und Governance; Netzwerk
AWS-Services: AWS Transit Gateway; Amazon VPC; Elastic Load Balancing (ELB)		

Übersicht

Amazon Web Services (AWS) hat bewährte Methoden veröffentlicht, die die Verwendung dedizierter Subnetze in einer Virtual Private Cloud (VPC) sowohl für Transit-Gateway-Anfügungen als auch für Gateway Load Balancer-Endpunkte (zur Unterstützung von AWS Network Firewall oder Drittanbieter-Appliances) empfehlen. Diese Subnetze werden verwendet, um Elastic Network-Schnittstellen für diese Services zu enthalten. Wenn Sie sowohl AWS Transit Gateway als auch einen Gateway Load Balancer verwenden, werden zwei Subnetze in jeder Availability Zone für die VPC erstellt. Aufgrund der Art und Weise, wie VPCs konzipiert sind, können diese zusätzlichen Subnetze nicht kleiner als eine /28-Mask sein und viel routbaren IP-Speicher belegen, der andernfalls für routbare Workloads verwendet werden könnte. Dieses Muster zeigt, wie Sie einen sekundären, nicht routingfähigen CIDR-Bereich (Classless Inter-Domain Routing) für diese dedizierten Subnetze verwenden können, um routbaren IP-Speicherplatz beizubehalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Multi-VPC-Strategie für routingfähigen IP-Speicherplatz
- Ein nicht weiterleitbarer CIDR-Bereich für die von Ihnen verwendeten Services (Transit-Gateway-Anfügungen und Gateway Load Balancer- oder Network-Firewall-Endpunkte)

Architektur

Zielarchitektur

Dieses Muster umfasst zwei Referenzarchitekturen: eine Architektur hat Subnetze für Transit-Gateway-Anfügungen (TGW) und einen Gateway Load Balancer-Endpunkt (GWLBe) und die zweite Architektur hat nur Subnetze für TGW-Anfügungen.

Architektur 1 angefügte VPC mit eingehendem Routing an eine Appliance

Das folgende Diagramm stellt eine Referenzarchitektur für eine VPC dar, die sich über zwei Availability Zones erstreckt. Beim Eingang verwendet die VPC ein Eingangs-Routing-Muster, um den für das öffentliche Subnetz bestimmten Datenverkehr zur Firewall-Inspektion an eine bump-in-the-wire Appliance weiterzuleiten. Eine TGW-Anfügung unterstützt den Ausgang von privaten Subnetzen zu einer separaten VPC.

Dieses Muster verwendet einen nicht routingfähigen CIDR-Bereich für das TGW-Anhangssubnetz und das GWLBe-Subnetz. In der TGW-Routing-Tabelle wird dieses nicht routbare CIDR mit einer Blackhole-Route (statisch) konfiguriert, indem eine Reihe spezifischerer Routen verwendet wird. Wenn die Routen an die TGW-Routing-Tabelle weitergegeben werden sollen, gelten diese spezifischen Blackhole-Routen.

In diesem Beispiel ist das routbare CIDR /23 unterteilt und vollständig routbaren Subnetzen zugewiesen.

Architektur 2 – angefügte VPC mit TGW

Das folgende Diagramm stellt eine weitere Referenzarchitektur für eine VPC dar, die sich über zwei Availability Zones erstreckt. Eine TGW-Anfügung unterstützt ausgehenden Datenverkehr (Ausgang) von den privaten Subnetzen zu einer separaten VPC. Es verwendet einen nicht routbaren CIDR-Bereich nur für das Subnetz der TGW-Anfügungen. In der TGW-Routing-Tabelle wird dieses nicht routbare CIDR mit einer Blackhole-Route konfiguriert, indem eine Reihe spezifischerer Routen verwendet wird. Wenn die Routen an die TGW-Routing-Tabelle weitergegeben werden sollen, gelten diese spezifischen Blackhole-Routen.

In diesem Beispiel ist das routbare CIDR /23 unterteilt und vollständig routbaren Subnetzen zugewiesen.

Tools

AWS-Services und -Ressourcen

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS. In diesem Muster werden sekundäre VPC-CIDRs verwendet, um routbaren IP-Speicherplatz in Workload-CIDRs beizubehalten.
- Internet-Gateway-Eingangs-Routing (Edge-Zuordnungen) kann zusammen mit Gateway Load Balancer-Endpunkten für dedizierte nicht routingfähige Subnetze verwendet werden.
- AWS Transit Gateway ist ein zentraler Hub, der VPCs und On-Premises-Netzwerke miteinander verbindet. In diesem Muster werden VPCs zentral an ein Transit-Gateway angefügt, und die Transit-Gateway-Anhänge befinden sich in einem dedizierten nicht routingfähigen Subnetz.
- Gateway-Load Balancer ermöglichen Ihnen die Bereitstellung, Skalierung und Verwaltung virtueller Geräte, wie Firewalls, Systeme zur Angriffserkennung und -Abwehr und Deep-Packet-Inspection-Systeme. Das Gateway dient als einziger Eingangs- und Ausgangspunkt für den gesamten Verkehr. In diesem Muster können Endpunkte für einen Gateway Load Balancer in einem dedizierten nicht routingfähigen Subnetz verwendet werden.
- AWS Network Firewall ist eine zustandsbehaftete, verwaltete Netzwerk-Firewall sowie ein Service zur Erkennung und Verhinderung von Eindringlingen für VPCs in der AWS Cloud. In diesem Muster können Endpunkte für eine Firewall in einem dedizierten nicht routingfähigen Subnetz verwendet werden.

Code-Repository

Ein Runbook und AWS- CloudFormation Vorlagen für dieses Muster sind im Repository GitHub Nicht routingfähige sekundäre CIDR-Muster verfügbar. Sie können die Beispieldateien verwenden, um eine Arbeitsumgebung in Ihrer Umgebung einzurichten.

Bewährte Methoden

AWS Transit Gateway

- Verwenden Sie für jeden Transit-Gateway-VPC-Anhang ein separates Subnetz.

- Weisen Sie ein /28-Subnetz aus dem sekundären nicht routingfähigen CIDR-Bereich für die Transit-Gateway-Anfügungssubnetze zu.
- Fügen Sie in jeder Transit-Gateway-Routing-Tabelle eine statische, spezifischere Route für den nicht routingfähigen CIDR-Bereich als Blackhole hinzu.

Gateway Load Balancer und Ingress-Routing

- Verwenden Sie Ingress-Routing, um den Datenverkehr aus dem Internet an die Gateway Load Balancer-Endpunkte weiterzuleiten.
- Verwenden Sie für jeden Gateway Load Balancer-Endpunkt ein separates Subnetz.
- Weisen Sie ein /28-Subnetz aus dem sekundären nicht routbaren CIDR-Bereich für die Gateway Load Balancer-Endpunktsubnetze zu.

Sekunden

Erstellen von VPCs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie den nicht routbaren CIDR-Bereich.	Bestimmen Sie einen nicht routbaren CIDR-Bereich, der für das Transit-Gateway-Anfügungssubnetz und (optional) für alle Gateway Load Balancer- oder Network Firewall-Endpunktsubnetze verwendet wird. Dieser CIDR-Bereich wird als sekundäres CIDR für die VPC verwendet . Sie darf nicht aus dem primären CIDR-Bereich der VPC oder dem größeren Netzwerk routbar sein.	Cloud-Architekt
Bestimmen Sie routingfähige CIDR-Bereiche für VPCs.	Bestimmen Sie eine Reihe von routingfähigen CIDR-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereichen, die für Ihre VPCs verwendet werden. Dieser CIDR-Bereich wird als primäres CIDR für Ihre VPCs verwendet.	
Erstellen Sie VPCs .	Erstellen Sie Ihre VPCs und fügen Sie sie an das Transit Gateway an. Jede VPC sollte einen primären CIDR-Bere ich haben, der routingfähig ist, und einen sekundären CIDR-Bereich, der nicht routingfä hig ist, basierend auf den Bereichen, die Sie in den beiden vorherigen Schritten festgelegt haben.	Cloud-Architekt

Konfigurieren von Transit-Gateway-Blackhole-Routen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie spezifischere, nicht routingfähige CIDRs als Blackholes.	Jede Transit-Gateway-Ro uting-Tabelle muss über eine Reihe von Blackhole-Routen verfügen, die für die nicht routingfähigen CIDRs erstellt wurden. Diese sind so konfiguriert, dass der gesamte Datenverkehr vom sekundäre n VPC-CIDR nicht routbar bleibt und nicht in das größere Netzwerk gelangt. Diese Routen sollten spezifischer sein als das nicht routingfä	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hige CIDR, das als sekundäre s CIDR auf der VPC festgelegt ist. Wenn das sekundäre nicht routingfähige CIDR beispiels weise 100.64.0.0/26 ist, sollten die Blackhole-Routen in der Transit-Gateway-Routing-Tabelle 100.64.0.0/27 und 100.64.0.32/27 sein.	

Zugehörige Ressourcen

- Bewährte Methoden für die Bereitstellung von Gateway Load Balancer
- Verteilte Inspektionsarchitekturen mit Gateway Load Balancer
- Networking Immersion Day Internet zu VPC Firewall Lab
- Bewährte Methoden für das Transit-Gateway-Design

Zusätzliche Informationen

Der nicht routingfähige sekundäre CIDR-Bereich kann auch nützlich sein, wenn Sie mit größeren skalierten Containerbereitstellungen arbeiten, die eine große Menge von IP-Adressen benötigen. Sie können dieses Muster mit einem privaten NAT-Gateway verwenden, um ein nicht routingfähiges Subnetz zum Hosten Ihrer Container-Bereitstellungen zu verwenden. Weitere Informationen finden Sie im Blog-Beitrag So lösen Sie private IP-Erschöpfung mit privater NAT-Lösung .

Bereitstellen eines Terraform-Produkts in AWS Service Catalog mithilfe eines Code-Repositorys

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) und Tamilselvan P (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; DevOps	Arbeitslast: Alle anderen Workloads
AWS-Services: AWS Service Catalog; Amazon EC2		

Übersicht

AWS Service Catalog unterstützt Self-Service-Bereitstellung mit Steuerung für Ihre HashiCorp Terraform-Konfigurationen. Wenn Sie Terraform verwenden, können Sie Service Catalog als einziges Tool verwenden, um Ihre Terraform-Konfigurationen innerhalb von AWS in großem Umfang zu organisieren, zu verwalten und zu verteilen. Sie können auf die wichtigsten Funktionen von Service Catalog zugreifen, darunter die Katalogisierung standardisierter und vorab genehmigter IaC-Vorlagen (Infrastructure as Code), Zugriffskontrolle, Bereitstellung von Cloud-Ressourcen mit geringsten Zugriffsrechten, Versionierung, gemeinsame Nutzung für Tausende von AWS-Konten und Tagging. Endbenutzer, wie Techniker, Datenbankadministratoren und Datenwissenschaftler, sehen eine Liste der Produkte und Versionen, auf die sie Zugriff haben, und können diese mit einer einzigen Aktion bereitstellen.

Dieses Muster hilft Ihnen bei der Bereitstellung von AWS-Ressourcen mithilfe von Terraform-Code. Auf den Terraform-Code im GitHub Repository wird über Service Catalog zugegriffen. Mit diesem Ansatz integrieren Sie die Produkte in Ihre bestehenden Terraform-Workflows. Administratoren können mithilfe von Terraform Service Catalog-Portfolios erstellen und ihnen AWS Launch Wizard Wizard-Produkte hinzufügen.

Im Folgenden sind die Vorteile dieser Lösung aufgeführt:

- Aufgrund der Rollback-Funktion in Service Catalog können Sie das Produkt auf eine frühere Version zurücksetzen, wenn während der Bereitstellung Probleme auftreten.
- Sie können die Unterschiede zwischen den Produktversionen leicht erkennen. Dies hilft Ihnen, Probleme bei der Bereitstellung zu lösen.

- Sie können eine Repository-Verbindung in Service Catalog konfigurieren, z. B. zu GitHub GitLab, oder AWS CodeCommit. Sie können Produktänderungen direkt über das Repository vornehmen.

Informationen zu den allgemeinen Vorteilen von AWS Service Catalog finden Sie unter Was ist Service Catalog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein GitHub BitBucket, oder ein anderes Repository, das Terraform-Konfigurationsdateien im ZIP-Format enthält.
- AWS Serverless Application Model Command Line Interface (AWS SAM CLI), installiert.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert.
- Los, installiert.
- Python-Version 3.9, installiert. AWS SAM CLI erfordert diese Version von Python.
- Berechtigungen zum Schreiben und Ausführen von AWS Lambda Lambda-Funktionen sowie Berechtigungen für den Zugriff auf und die Verwaltung von Service Catalog-Produkten und -Portfolios.

Architektur

Zieltechnologie-Stack

- AWS Service Catalog
- AWS Lambda

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Wenn eine Terraform-Konfiguration fertig ist, erstellt ein Entwickler eine ZIP-Datei, die den gesamten Terraform-Code enthält. Der Entwickler lädt die ZIP-Datei in das Code-Repository hoch, das mit Service Catalog verbunden ist.

2. Ein Administrator ordnet das Terraform-Produkt einem Portfolio im Service Catalog zu. Der Administrator erstellt außerdem eine Startbeschränkung, die es Endbenutzern ermöglicht, das Produkt bereitzustellen.
3. In Service Catalog starten Endbenutzer AWS-Ressourcen mithilfe der Terraform-Konfiguration. Sie können wählen, welche Produktversion bereitgestellt werden soll.

Tools

AWS-Services und -Tools

- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Mit AWS Service Catalog können Sie Kataloge von IT-Services, die für AWS zugelassen sind, zentral verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Andere Dienste

- Go ist eine Open-Source-Programmiersprache, die Google unterstützt.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Wenn Sie Terraform-Beispielkonfigurationen benötigen, die Sie über Service Catalog bereitstellen können, können Sie die Konfigurationen im GitHub Amazon Macie Organization Setup Using Terraform Repository verwenden. Die Verwendung der Codebeispiele in diesem Repository ist nicht erforderlich.

Bewährte Methoden

- Anstatt die Werte für Variablen in der Terraform-Konfigurationsdatei (`terraform.tfvars`) bereitzustellen, konfigurieren Sie Variablenwerte, wenn Sie das Produkt über Service Catalog starten.
- Gewähren Sie nur bestimmten Benutzern oder Administratoren Zugriff auf das Portfolio.

- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Richten Sie Ihre lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Installieren Sie Docker.	Wenn Sie die AWS Lambda Lambda-Funktionen in Ihrer Entwicklungsumgebung ausführen möchten, installieren Sie Docker. Weitere Informationen finden Sie unter Installieren der Docker-Engine in der Docker-Dokumentation.	DevOps Ingenieur
Installieren Sie die AWS Service Catalog Engine für Terraform.	1. Geben Sie den folgenden Befehl ein, um das AWS Service Catalog Engine for Terraform-Repository zu klonen. `git clone https://github.com/aws-samples/service-catalog-engine-for-terraform-os.git` 2. Navigieren Sie zum Stammverzeichnis des geklonten Repositorys. 3. Geben Sie den folgenden Befehl ein. Dadurch wird die Engine installiert.	DevOps Ingenieur, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`run ./bin/bash/ deploy-tre.sh -r` Die in Ihrem Standardprofil festgelegte AWS-Region wird während der automatisierten Installation nicht verwendet. Stattdessen geben Sie die Region an, wenn Sie diesen Befehl ausführen.	

Connect das GitHub Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung zum GitHub Repository her.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die Developer Tools-Konsole. Sie können auf die Developer Tools-Konsole zugreifen, indem Sie einen Service wie AWS CodePipeline CodeCommit, AWS oder AWS auswählen CodeDeploy. 2. Wählen Sie im linken Navigationsbereich Einstellungen und dann Verbindungen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Create Connection (Verbindung erstellen) aus. 4. Wählen Sie das Repository aus, in dem Sie den Terraform-Quellcode verwalten. Sie können beispielsweise Bitbucket oder GitHub Enterprise Server GitHubwählen. 5. Geben Sie einen Namen für die Verbindung ein, und wählen Sie dann Connect. 6. Wenn Sie dazu aufgefordert werden, authentifizieren Sie das Repository. Nach Abschluss der Authentifizierung wird die Verbindung hergestellt und der Status wechselt zu aktiv.	

Erstellen Sie ein Terraform-Produkt im Service Catalog

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Service Catalog-Produkt.	1. Öffnen Sie die AWS Service Catalog-Konsole. 2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Produktliste aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Produkt erstellen aus. 4. Wählen Sie auf der Seite Produkt erstellen im Abschnitt Produktdetails den externen Produktty p aus. Service Catalog verwendet diesen Produktty p zur Unterstützung von Terraform Community Edition-Produkten. 5. Geben Sie einen Namen und Besitzer für das Service Catalog-Produkt ein. 6. Wählen Sie Geben Sie Ihr Code-Repository mithilfe eines CodeStar Anbieters an. 7. Geben Sie die folgenden Informationen für Ihr Repository ein: • Connect zu Ihrem Anbieter her über AWS CodeConnections — Wählen Sie die Verbindung aus, die Sie zuvor erstellt haben. • Repository — Wählen Sie das Repository aus. • Zweig — Wählen Sie den Zweig aus. • Pfad der Vorlagendatei — Wählen Sie den Pfad,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in dem die Codevorla gendatei gespeichert ist. Der Dateiname sollte mit enden `tar.gz`. 8. Geben Sie unter Versionsn ame und Beschreib ung Informationen zur Produktversion an. 9. Wählen Sie Produkt erstellen aus.	
Erstellen Sie ein Portfolio.	1. Öffnen Sie die AWS Service Catalog-Konsole. 2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Portfolios aus. 3. Wählen Sie Portfolio erstellen 4. Geben Sie die folgenden Werte ein: • Portfolio-Name – `Sample terraform` • Beschreibung des Portfolios — `Sample portfolio for Terraform configura tions` • Eigentümer — Ihre Kontaktinformationen, z. B. E-Mail 5. Wählen Sie Erstellen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Terraform-Produkt dem Portfolio hinzu.	1. Öffnen Sie die AWS Service Catalog-Konsole. 2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Produktliste aus. 3. Wählen Sie das Terraform-Produkt aus, das Sie zuvor erstellt haben. 4. Wählen Sie Aktionen und dann Produkt zum Portfolio hinzufügen. 5. Wählen Sie das `Sample terraform` Portfolio aus. 6. Wählen Sie Produkt zum Portfolio hinzufügen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zugriffsr ichtlinie.	1. Öffnen Sie die AWS Identity and Access Management (IAM) -Konsole. 2. Wählen Sie im Navigatio nsbereich Policies. 3. Wählen Sie im Inhaltsbe reich die Option Create policy (Richtlinie erstellen). 4. Wählen Sie die JSON-Opti on. 5. Geben Sie die JSON-Beis pielrichtlinie unter Zugriffsr ichtlinie im Abschnitt Zusätzliche Informationen dieses Musters ein. 6. Wählen Sie Weiter aus. 7. Geben Sie auf der Seite Überprüfen und erstellen im Feld Richtlinienname den Text ein `TerraformResourceCreationAndArtifactAccessPolicy` . 8. Wählen Sie Richtlinie erstellen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine benutzerdefinierte Vertrauensrichtlinie.	1. Öffnen Sie die AWS Identity and Access Management (IAM) -Konsole. 2. Wählen Sie im Navigationsbereich Rollen aus. 3. Wählen Sie Rolle erstellen aus. 4. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus. 5. Geben Sie im JSON-Richtlinieneditor die JSON-Beispielrichtlinie unter Vertrauensrichtlinie im Abschnitt Zusätzliche Informationen dieses Musters ein. 6. Wählen Sie Weiter aus. 7. Wählen Sie unter Berechtigungsrichtlinien die aus`TerraformResourceCreationAndArtifactAccessPolicy` , die Sie zuvor erstellt haben. 8. Wählen Sie Weiter aus. 9. Geben Sie unter Rollendetails in das Feld Rollenname den Text ein`SCLaunch-product` .	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Der Rollenname muss mit beginnen`SCLaunch`. 10. Wählen Sie Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie dem Service Catalog-Produkt eine Startbeschränkung hinzu.	1. Melden Sie sich als Benutzer mit Administratorberechtigungen bei der AWS-Managementkonsole an. 2. Öffnen Sie die AWS Service Catalog-Konsole. 3. Wählen Sie im Navigationsbereich Portfolios aus. 4. Wählen Sie das Portfolio aus, das Sie zuvor erstellt haben. 5. Wählen Sie auf der Seite mit den Portfoliodetails die Registerkarte Einschränkungen und dann Einschränkung erstellen aus. 6. Wählen Sie unter Produkt das Terraform-Produkt aus, das Sie zuvor erstellt haben. 7. Wählen Sie unter Startbeschränkung für Methode die Option Rollennamen eingeben aus. 8. Geben Sie in das Feld Rollenname den Text ein`SCLaunch-product` . 9. Wählen Sie Erstellen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff auf das Produkt.	1. Öffnen Sie die AWS Service Catalog-Konsole. 2. Wählen Sie im Navigationsbereich Portfolios aus. 3. Wählen Sie das Portfolio aus, das Sie zuvor erstellt haben. 4. Wählen Sie die Registerkarte Zugriff und anschließend Zugriff gewähren aus. 5. Wählen Sie die Registerkarte Rollen und dann die Rolle aus, die Zugriff auf die Bereitstellung dieses Produkts haben soll. 6. Wählen Sie Zugriff gewähren.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie das Produkt.	1. Melden Sie sich bei der AWS-Managementkonsole als Benutzer mit Berechtigungen zur Bereitstellung des Service Catalog-Produkts an. 2. Öffnen Sie die AWS Service Catalog-Konsole. 3. Wählen Sie im Navigationsbereich Produkte aus. 4. Wählen Sie das Produkt aus, das Sie zuvor erstellt haben, und klicken Sie dann auf Produkt starten. 5. Geben Sie einen Produktnamen ein und definieren Sie alle erforderlichen Parameter. 6. Wählen Sie Produkt starten.	DevOps Ingenieur

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	Es gibt zwei AWS Step Functions Functions-Zustandsmaschinen für den Service Catalog-Bereitstellungsworkflow: • `ManageProvisionedProductStateMachine` —Service Catalog ruft	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	diese Zustandsmaschine auf, wenn ein neues Terraform-Produkt bereitgestellt wird und wenn ein vorhandenes von Terraform bereitgestelltes Produkt aktualisiert wird. • `TerminateProvisionedProductStateMachine` —Service Catalog ruft diese Zustandsmaschine auf, wenn ein vorhandenes, von Terraform bereitgestelltes Produkt beendet wird. Sie überprüfen die Protokolle für den `ManageProvisionedProductStateMachine` State Machine, um zu bestätigen, dass das Produkt bereitgestellt wurde. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Step Functions-Konsole. 2. Wählen Sie im linken Navigationsbereich State Machines aus. 3. `ManageProvisionedProductStateMachine` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Geben Sie in der Liste Ausführungen die bereitgestellte Produkt-ID ein, um nach der Ausführung zu suchen. Hinweis: Die Namen der Backend-Buckets für die Statusdatei beginnen mit. `sc-terraform-engine-state-` 5. Stellen Sie sicher, dass alle erforderlichen Ressourcen im Konto erstellt wurden.	

Infrastruktur aufräumen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie bereitgestellte Produkte.	1. Melden Sie sich bei der AWS-Managementkonsole als Benutzer mit Berechtigungen zur Bereitstellung des Service Catalog-Produkts an. 2. Öffnen Sie die AWS Service Catalog-Konsole. 3. Wählen Sie in der linken Navigationsleiste Bereitgestellte Produkte aus. 4. Wählen Sie das Produkt aus, das Sie erstellt haben.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie in der Liste Aktionen die Option Beenden aus. 6. Geben Sie `terminate` in das Bestätigungsfeld den Text ein und wählen Sie dann Bereitgestelltes Produkt beenden aus. 7. Wiederholen Sie diese Schritte, um alle bereitgestellten Produkte zu beenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS Service Catalog Engine für Terraform.	1. Melden Sie sich als Benutzer mit Administr atorberechtigungen bei der AWS-Managementkonsole an. 2. Öffnen Sie die Amazon S3-Konsole. 3. Wählen Sie im Navigatio nsbereich die Option Buckets aus. 4. Wählen Sie den `sc-terraform-engine-logging-XXXX` Bucket aus. 5. Wählen Sie Leer. 6. Wiederholen Sie die Schritte 4—5 für die folgenden Buckets: • `sc-terraform-engine-state-XXXX` • `terraform-engine-bootstrap-XXXX` 7. Öffnen Sie die CloudFormation AWS-Konsole und überprüfen Sie dann, ob Sie sich in der richtigen AWS-Region befinden. 8. Wählen Sie in der linken Navigationsleiste Stacks aus. 9. Wählen Sie `SAM-TRE` und wählen Sie dann Löschen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Warten Sie, bis der Stapel gelöscht wurde. 10. Wählen Sie `Bootstrap-TRE` und wählen Sie dann Löschen. Warten Sie, bis der Stapel gelöscht wurde.	

Zugehörige Ressourcen

AWS-Dokumentation

- Erste Schritte mit einem Terraform-Produkt

Terraform-Dokumentation

- Terraform-Installation
- Terraform-Backend-Konfiguration
- Terraform AWS-Provider-Dokumentation

Zusätzliche Informationen

Richtlinie für den Zugriff

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
```

```
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Vertrauensrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GivePermissionsToServiceCatalog",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

Registrieren mehrerer AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES

Erstellt von Joe Wozniak (AWS) und Shubhangi Vishwakarma (AWS)

Code-Repository: GitHub aws-account-factory-email	Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; Management und Governance; Messaging und Kommunikation
AWS-Services: AWS Lambda ;Amazon SES; Amazon DynamoDB		

Übersicht

Dieses Muster beschreibt, wie Sie echte E-Mail-Adressen von der E-Mail-Adresse entkoppeln können, die einem AWS-Konto zugeordnet ist. AWS-Konten erfordern, dass zum Zeitpunkt der Kontoerstellung eine eindeutige E-Mail-Adresse angegeben wird. In einigen Organisationen muss das Team, das AWS-Konten verwaltet, die Last übernehmen, viele eindeutige E-Mail-Adressen mit seinem Messaging-Team zu verwalten. Dies kann für große Organisationen, die viele AWS-Konten verwalten, schwierig sein.

Dieses Muster bietet eine eindeutige Lösung für den E-Mail-Adressverkauf, mit der AWS-Kontoinhaber eine E-Mail-Adresse mehreren AWS-Konten zuordnen können. Die echten E-Mail-Adressen der AWS-Kontoinhaber werden dann diesen generierten E-Mail-Adressen in einer Tabelle zugeordnet. Die Lösung verarbeitet alle eingehenden E-Mails für die eindeutigen E-Mail-Konten, sucht den Besitzer jedes Kontos und leitet dann alle empfangenen Nachrichten an den Eigentümer weiter.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Administrativer Zugriff auf ein AWS-Konto.

- Zugriff auf eine Entwicklungsumgebung. Wir empfehlen, AWS Cloud9 zu verwenden, um zu vermeiden, dass Sie die erforderlichen Tools und Zugriffsschlüssel selbst einrichten müssen.
- (Optional) Vertrautheit mit AWS Cloud Development Kit (AWS CDK)-Workflows und der Programmiersprache Python hilft Ihnen bei der Behebung von Problemen oder Änderungen.

Einschränkungen

- Gesamtlänge der verkauften E-Mail-Adresse beträgt 64 Zeichen. Weitere Informationen finden SieCreateAccount unter in der AWS Organizations-API-Referenz.

Produktversionen

- Node.js Version 12.7.0 oder höher
- Python 3.9 oder höher
- Python-Pakete pip und virtualenv
- AWS-CDK-Version 2.23.0 oder höher
- Docker 20.10.x oder höher

Architektur

Zieltechnologie-Stack

- AWS- CloudFormation Stack
- Funktionen von AWS Lambda
- Regel und Regelsatz für Amazon Simple Email Address (Amazon SES)
- AWS Identity and Access Management (IAM)-Rollen und -Richtlinien
- Bucket- und Bucket-Richtlinie für Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS)-Schlüssel und Schlüsselrichtlinie
- Thema und Themenrichtlinie von Amazon Simple Notification Service (Amazon SNS)
- Amazon-DynamoDB-Tabelle.

Zielarchitektur

Dieses Diagramm zeigt zwei Flows:

- Ablauf beim Verkauf von E-Mail-Adressen: Im Diagramm beginnt der Ablauf beim Verkauf von E-Mail-Adressen (unterster Abschnitt) in der Regel mit einer Kontoverkaufslösung oder einer externen Automatisierung oder wird manuell aufgerufen. In der Anforderung wird eine Lambda-Funktion mit einer Nutzlast aufgerufen, die die erforderlichen Metadaten enthält. Die Funktion verwendet diese Informationen, um einen eindeutigen Kontonamen und eine eindeutige E-Mail-Adresse zu generieren, sie in einer DynamoDB-Datenbank zu speichern und die Werte an den Aufrufer zurückzugeben. Diese Werte können dann verwendet werden, um ein neues AWS-Konto zu erstellen (in der Regel mithilfe von AWS Organizations).
- E-Mail-Weiterleitungsablauf: Dieser Flow wird im oberen Abschnitt des vorherigen Diagramms dargestellt. Wenn ein AWS-Konto mithilfe der Konto-E-Mail erstellt wird, die aus dem E-Mail-Adressvergabeablauf generiert wurde, sendet AWS verschiedene E-Mails, z. B. Kontoregistrierungsbestätigung und regelmäßige Benachrichtigungen, an diese E-Mail-Adresse. Indem Sie die Schritte in diesem Muster ausführen, konfigurieren Sie Ihr AWS-Konto bei Amazon SES so, dass es E-Mails für die gesamte Domain empfängt. Diese Lösung konfiguriert Weiterleitungsregeln, die es Lambda ermöglichen, alle eingehenden E-Mails zu verarbeiten, zu überprüfen, ob sich die T0 Adresse in der DynamoDB-Tabelle befindet, und stattdessen die Nachricht an die E-Mail-Adresse des Kontoinhabers weiterzuleiten. Durch diesen Prozess können Kontoinhaber mehrere Konten einer E-Mail-Adresse zuordnen.

Automatisierung und Skalierung

Dieses Muster verwendet das AWS-CDK, um die Bereitstellung vollständig zu automatisieren. Die Lösung verwendet von AWS verwaltete Services, die automatisch skaliert werden (oder so konfiguriert werden können), um Ihren Anforderungen gerecht zu werden. Die Lambda-Funktionen erfordern möglicherweise eine zusätzliche Konfiguration, um Ihre Skalierungsanforderungen zu erfüllen. Weitere Informationen finden Sie unter Lambda-Funktionsskalierung in der Lambda-Dokumentation.

Tools

AWS-Services

- AWS Cloud9 ist eine integrierte Entwicklungsumgebung (IDE), mit der Sie Software programmieren, erstellen, ausführen, testen und debuggen können. Es hilft Ihnen auch, Software in der AWS Cloud zu veröffentlichen.

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Email Service (Amazon SES) hilft Ihnen beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domänen.
- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Für die Bereitstellung benötigte Tools

- Entwicklungsumgebung mit der AWS CLI und dem IAM-Zugriff auf Ihr AWS-Konto. Einzelheiten finden Sie unter den Links im Abschnitt Verwandte Ressourcen. Wir empfehlen Ihnen, AWS Cloud9 zu verwenden, um den Einrichtungsprozess zu vereinfachen.
- Wenn Sie AWS Cloud9 verwenden, wird Folgendes für Sie konfiguriert. Wenn Sie AWS Cloud9 nicht verwenden möchten, müssen Sie Folgendes installieren:
  - Die AWS CLI zum Konfigurieren von Anmeldeinformationen für das AWS-CDK. Weitere Informationen finden Sie in der AWS CLI-Dokumentation.
  - Python Version 3.9 oder höher
  - Python-Pakete pip und virtualenv
  - Node.js Version 12.7.0 oder höher

- AWS-CDK-Version 2.23.0 oder höher
- Docker-Version 20.10.x oder höher

Code

Der Code für dieses Muster ist im GitHub AWS-Account-Factory-E-Mail-Repository verfügbar.

Polen

Zuweisen einer Zielbereitstellungsumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren oder erstellen Sie ein AWS-Konto.	Identifizieren Sie ein vorhandenes oder neues AWS-Konto, auf das Sie vollen Administratorzugriff haben, um die E-Mail-Lösung bereitzustellen.	AWS-Administrator, Cloud-Administrator
Richten Sie eine Bereitstellungsumgebung ein.	Konfigurieren Sie eine benutzerfreundliche Bereitstellungsumgebung und richten Sie Abhängigkeiten ein, indem Sie die folgenden Schritte ausführen: 1. Stellen Sie eine Instance von AWS Cloud9 als dedizierte Bereitstellungsumgebung bereit. Anweisungen finden Sie unter Erste Schritte mit AWS Cloud9. 2. Klonen Sie die E GitHub -Mail-Repository-Codebasis des AWS-Kontos in die	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Cloud9-Instance, indem Sie den Befehl verwenden: `git clone https://github.com/aws-samples/aws-account-factory-email` 3. Aktualisieren Sie in der `requirements.txt` Datei (im Stammverzeichnis des Repositorys) die Zeile, die mit beginnt`aws-cdk-lib==` , so, dass sie mit der Version des AWS-CDK übereinstimmt, das in Ihrer Umgebung ausgeführt wird. Verwenden Sie den `cdk --version` Befehl , um die Version zu identifizieren.	

Einrichten einer verifizierten Domain

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren und Zuweisen einer Domain.	Die E-Mail-Weiterleitungsfunktion erfordert eine dedizierte Domain. Identifizieren und weisen Sie eine Domäne oder Subdomäne zu, die Sie mit Amazon SES verifizieren können. Diese Domain sollte für den Empfang eingehender E-Mails innerhalb des AWS-	Cloud-Administrator, Netzwerkadministrator, DNS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kontos verfügbar sein, in dem die E-Mail-Weiterleitungslösung bereitgestellt wird. Domänenanforderungen: • Die Domain sollte eine Standarddomain oder Subdomain sein. • Die Domain sollte extern DNS-lösbar sein, da sie zum Empfangen von E-Mails von außerhalb der Organisation verwendet wird.	
Überprüfen Sie die Domain.	Stellen Sie sicher, dass die identifizierte Domain verwendet werden kann, um eingehende E-Mails zu akzeptieren. Befolgen Sie die Anweisungen unter Verifizieren Ihrer Domain für Amazon SES-E-Mail-Empfang in der Amazon SES-Dokumentation. Dies erfordert die Koordination mit der Person oder dem Team, die/das für die DNS-Datensätze der Domain verantwortlich ist.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie MX-Datensätze ein.	Richten Sie Ihre Domain mit MX-Datensätzen ein, die auf die Amazon SES-Endpunkte in Ihrem AWS-Konto und Ihrer Region verweisen. Weitere Informationen finden Sie unter Veröffentlichen eines MX-Datensatzes für den Amazon SES-E-Mail-Empfang in der Amazon SES-Dokumentation.	Cloud-Administrator, Netzwerkadministrator, DNS-Administrator

Bereitstellen der E-Mail-Vertriebs- und Weiterleitungslösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Standardwerte in cdk.json.	Bearbeiten Sie einige der Standardwerte in der `cdk.json` Datei (im Stammverzeichnis des Repositorys), damit die Lösung nach der Bereitstellung ordnungsgemäß funktioniert. 1. Ändern Sie den `SES_DOMAIN_NAME` Wert so, dass er mit dem Domänennamen übereinstimmt, den Sie zuvor verifiziert haben. 2. Ändern Sie den `ADDRESS_FROM` Wert so, dass er dieselbe Domain enthält, die sich	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in befindet`SES_DOMAIN_NAME` . Der lokale Teil der Adresse sollte von Ihrem Cloud-Team bestimmt werden. Diese Adresse wird die `FROM` Adresse für jede E-Mail, die über die Lösung weitergeleitet wird. 3. Ändern Sie den `ADDRESS_ADMIN` Wert so, dass er mit der E-Mail-Adresse übereinstimmt, an die nicht übereinstimmende eingehende Nachrichten weitergeleitet werden. Dieser Wert muss eine gültige und funktionierende E-Mail-Adresse sein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die E-Mail-Vertriebs- und Weiterleitungslösung bereit.	1. Erstellen Sie eine virtuelle Python-Umgebung:
	`python -m venv .venv`
	2. Aktivieren Sie die virtuelle Python-Umgebung:
	`source .venv/bin/activate`
	Oder verwenden Sie auf der Windows-Plattform:
	`% .venv\Scripts\activate.bat`
	3. Installieren Sie alle Python-Anforderungen ohne Fehler:
	`pip install -r requirements.txt`
	4. Synthetisieren Sie die CloudFormation Vorlage:
	`cdk synth`
	Vergewissern Sie sich, dass keine Fehler vorliegen und dass die vollständige CloudFormation Vorlage die erwartete Ausgabe enthält.
	5. (Optional) Wenn Sie den AWS-CDK-Code zum ersten Mal im aktuellen
		App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	AWS-Konto oder in der aktuellen Region bereitstellen, bootstrappen Sie die Umgebung. Weitere Informationen finden Sie unter Bootstrapping in der AWS-CDK-Dokumentation.
	`cdk bootstrap aws://AWS-ACCOUNT-NUMBER/REGION`
	Ersetzen Sie `AWS-ACCOUNT-NUMBER` und `REGION` durch tatsächliche Werte.
	6. Stellen Sie die Lösung bereit:
	`cdk bootstrap`
	`cdk deploy`
	Die Befehle sollten fehlerfrei abgeschlossen werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lösung bereitgestellt wurde.	Stellen Sie sicher, dass die Lösung erfolgreich bereitgestellt wurde, bevor Sie mit dem Testen beginnen: 1. Öffnen Sie die AWS-CloudFormation Konsole und suchen Sie nach einem CloudFormation Stack, der den Namen enthält`AwsMailFwdStack` . 2. Vergewissern Sie sich, dass dieser `AwsMailFwdStack` Stack über die folgenden Ressourcen verfügt: • Lambda-Funktionen • Amazon SES-Regel und Regelsatz • IAM-Rollen und -Richtlinien • Amazon S3-Bucket und Bucket-Richtlinie • AWS KMS-Schlüssel und Schlüsselrichtlinie • Amazon SNS-Thema und Themenrichtlinie • DynamoDB-Tabelle	App-Entwickler, AWS DevOps

Stellen Sie sicher, dass der E-Mail-Versand und die Weiterleitung wie erwartet funktionieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die API funktioniert.	In diesem Schritt übermitte ln Sie Testdaten an die API der Lösung und bestätige n, dass die Lösung die erwartete Ausgabe erzeugt und Backend-Operationen wie erwartet ausgeführt wurden. Führen Sie die Funktion Vend Email Lambda mithilfe der Testeingabe manuell aus. (Ein Beispiel finden Sie in der Datei sample_vend_request.json.) `OwnerAddress` Verwenden Sie für eine gültige E-Mail-Ad resse. Die API sollte einen Kontonamen und eine Konto-E-Mail mit den erwarteten Werten zurückgeben.	App-Entwickler, AWS DevOps
Stellen Sie sicher, dass die E-Mail weitergeleitet wird.	In diesem Schritt senden Sie eine Test-E-Mail über das System und überprüfen, ob die E-Mail an den erwarteten Empfänger weitergeleitet wird. 1. Rufen Sie die Konto-E-Mail aus dem letzten Schritt ab. 2. Senden Sie eine E-Mail mit einem Betreff und Text an diese Adresse. 3. Vergewissern Sie sich, dass Sie die E-Mail an die E-	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mail-Adresse des Kontoinhabers erhalten haben. 4. Vergewissern Sie sich, dass die E-Mail, die Sie erhalten haben, eine `FROM` Adresse hat, die der `ADDRESS_FROM` Einstellung in entsprichtcdk.json. 5. Vergewissern Sie sich, dass der Betreff und der Text der empfangenen E-Mail mit der ursprünglich gesendeten Nachricht übereinstimmen.	

Fehlerbehebung

Problem	Lösung
Das System leitet E-Mails nicht wie erwartet weiter.	Überprüfen Sie, ob Ihre Einrichtung korrekt ist: 1. Sie sollten den Amazon SES-Verifizierungsprozess für Ihre Domain abgeschlossen haben. 2. Ihre Domain sollte ordnungsgemäß eingerichtet sein, wobei MX-Datensätze auf die Amazon SES-Endpunkte in Ihrem AWS-Konto und Ihrer Region verweisen. Weitere Informationen finden Sie unter Veröffentlichen eines MX-Datensatzes für den Amazon SES-E-Mail-Empfang in der Amazon SES-Dokumentation.

Problem	Lösung
	Nachdem Sie Ihre Domäneneinrichtung überprüft haben, gehen Sie wie folgt vor: 1. Öffnen Sie die AWS- CloudWatch Konsole für das Konto und die Region, in der Sie die Lösung bereitgestellt haben, und navigiere n Sie im Navigationsbereich zu CloudWatch Protokollgruppen. 2. Suchen Sie in der Liste der Protokollgruppen nach `SesMailForwardLogGroup` . 3. Untersuchen Sie die Protokolle in dieser Gruppe, um festzustellen, ob während des E-Mail-Vertriebs- und Weiterleitungsproz esses Fehler generiert werden.

Problem	Lösung
Wenn Sie versuchen, den AWS-CDK-Stack bereitzustellen, erhalten Sie eine Fehlermeldung ähnlich wie: „Fehler im Vorlagenformat: Nicht erkannte Ressourcentypen“	In den meisten Fällen bedeutet diese Fehlermeldung, dass die gewünschte Region nicht über alle verfügbaren AWS-Services verfügt. Wenn Sie AWS Cloud9 zur Bereitstellung der Lösung verwenden, richten Sie sich möglicherweise an eine Region, die sich von der Region unterscheidet, in der die AWS Cloud9-Instance ausgeführt wird. Hinweis: Standardmäßig wird das AWS-CDK für die Region und das Konto bereitgestellt, die Sie in der AWS CLI konfiguriert haben. Mögliche Lösungen: 1. Untersuchen Sie, ob sich alle für diese Lösung erforderlichen Services (siehe Abschnitt Zieltechnologie-Stack weiter oben in diesem Muster) in der AWS-Region befinden, auf die Sie abzielen, indem Sie AWS-Services nach Region überprüfen. 2. Wenn Sie AWS Cloud9 verwenden und auf eine Region abzielen, die sich von der Region unterscheidet, in der Ihre AWS Cloud9-Instance ausgeführt wird, stellen Sie sicher, dass Sie die `AWS_DEFAULT_REGION` Umgebungsvariable oder eine Region mit der AWS CLI festlegen, bevor Sie die Lösung bereitstellen. Weitere Informationen finden Sie in den Umgebungsvariablen zur Konfiguration der AWS CLI in der AWS CLI-Dokumentation. Alternativ können Sie die `app.py` Datei im Stammverzeichnis des Repositorys so ändern, dass sie eine fest codierte Konto-ID und Region

Problem	Lösung
	enthält, indem Sie den Anweisungen in der AWS-CDK-Dokumentation für Umgebungen folgen.
Wenn Sie die Lösung bereitstellen, erhalten Sie die Fehlermeldung: „Bereitstellung fehlgeschlagen: Fehler: AwsMailFwdStack: SSM-Parameter /cdk-bootstrap/hnb659fds/version nicht gefunden. Wurde die Umgebung gestartet? Bitte führen Sie „cdk bootstrap“ aus	Wenn Sie noch nie AWS-CDK-Ressourcen für das AWS-Konto und die AWS-Region bereitgestellt haben, die Sie anvisieren, müssen Sie zuerst den `cdk bootstrap` Befehl ausführen, wie der Fehler anzeigt. Wenn Sie diesen Fehler nach dem Ausführen des Bootstrap ping-Befehls weiterhin erhalten, versuchen Sie möglicherweise, die Lösung in einer Region bereitzustellen, die sich von der Region unterscheidet, in der Ihre AWS Cloud9-Instance ausgeführt wird. Um dieses Problem zu lösen, legen Sie die `AWS_DEFAULT_REGION` Umgebungsvariable oder eine Region mit der AWS CLI fest, bevor Sie die Lösung bereitstellen. Alternativ können Sie die `app.py` Datei im Stammverzeichnis des Repositorys so ändern, dass sie eine fest codierte Konto-ID und Region enthält, indem Sie den Anweisungen in der AWS-CDK-Dokumentation für Umgebungen folgen.

Zugehörige Ressourcen

- Hilfe bei der Installation der AWS CLI finden Sie unter Installieren oder Aktualisieren der neuesten Version der AWS CLI.
- Weitere Informationen zum Einrichten der AWS CLI mit IAM-Anmeldeinformationen finden Sie unter Konfigurieren der AWS CLI.
- Hilfe zum AWS-CDK finden Sie unter Erste Schritte mit dem AWS-CDK.

Zusätzliche Informationen

Kosten

Wenn Sie diese Lösung bereitstellen, können dem AWS-Kontoinhaber Kosten entstehen, die mit der Nutzung der folgenden Services verbunden sind. Es ist wichtig, dass Sie verstehen, wie diese Services in Rechnung gestellt werden, damit Sie über mögliche Gebühren informiert sind. Preisinformationen finden Sie auf den folgenden Seiten:

- Amazon SES-Preise
- Amazon S3 – Preise
- AWS Cloud9 – Preise
- AWS KMS – Preise
- AWS Lambda – Preise
- Amazon DynamoDB – Preise

Einrichten der DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit mehreren Konten

Erstellt von Amir Durrani

Umgebung: Produktion	Technologien: Infrastruktur; Netzwerk	AWS-Services: AWS RAM; Amazon Route 53; AWS Control Tower

Übersicht

Dieses Muster beschreibt, wie Sie On-Premises-DNS-Services (Domain Name System) mit Amazon Route 53-Resolver-Regeln und ausgehenden Resolver-Endpunkten zur Namensauflösung verwenden können.

DNS ist für den Aufbau und die Aufrechterhaltung der Kommunikation zwischen Netzwerkumgebungen von grundlegender Bedeutung. Wenn Sie über eine hybride Netzwerkkonnektivitätsumgebung verfügen, können Sie kritische Netzwerkservices wie DNS und Active Directory gemeinsam nutzen, ohne den betrieblichen Aufwand für die Verwaltung einer verteilten Umgebung über -Konten und Virtual Private Clouds (VPCs). Dieser Ansatz hilft Ihnen beim Erstellen und Unterstützen von Anwendungen, die sich über eine große Anzahl von Konten erstrecken. Wenn Sie beispielsweise über Hunderte oder Tausende von Konten mit Hybrid-Konnektivitätsanforderungen in mehreren Regionen verfügen, können Sie DNS-Services sicher und effizient in allen verbundenen Umgebungen innerhalb Ihrer AWS-Organisation freigeben.

DNS ist für das IP-Netzwerk zwischen allen Ebenen (Web, Anwendung und Datenbank) einer Anwendung von entscheidender Bedeutung. Es hat sich bewährt, nur dem Team von DNS-Experten vollen Zugriff auf die Konfiguration, den Betrieb und die Unterstützung dieser Ressource zu gewähren. In einer Hybrid-Konnektivitätsumgebung können Sie Ihr On-Premises-DNS weiterhin für Anforderungen zur Namensauflösung verwenden, die von Ressourcen stammen, die sich in verschiedenen Konten befinden, indem Sie die bedingte Weiterleitung verwenden.

Dieses Muster behandelt die hybride DNS-Auflösung in einer AWS-Umgebung mit mehreren Konten. Informationen zu einzelnen Konten finden Sie im Muster DNS-Auflösung für hybride Netzwerke in einer AWS-Umgebung mit einem einzigen Konto einrichten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine AWS-Umgebung mit mehreren Konten, die auf bewährten Methoden basiert und mit AWS Control Tower erstellt wurde. Das Diagramm im nächsten Abschnitt zeigt die typische Architektur einer solchen Umgebung.
- Skalierbare Routing-Infrastruktur zwischen den Konten und VPCs mithilfe von AWS Transit Gateway .
- Ausgehende Resolver-Endpunkte und Resolver-Regeln mithilfe von Amazon Route 53.
- Ressourcenfreigaben für ausgehende Resolver-Regeln mithilfe von AWS Resource Access Manager (AWS RAM).

Architektur

AWS-Architektur mit mehreren Konten

Zieltechnologie-Stack

- Eine vorhandene On-Premises-DNS-Infrastruktur für die Auflösung ausgehender Namen für eine große Anzahl von AWS-Prinzipalen
- Route 53-Resolver-Regel und ausgehende Resolver-Endpunkte
- AWS RAM zum Freigeben von Route 53 Resolver-Regeln für andere AWS-Prinzipale innerhalb und außerhalb der AWS-Organisation

Zielarchitektur

Das folgende Diagramm zeigt die Schritte zur Konfiguration der end-to-end Hybrid-DNS-Auflösung. AWS RAM wird verwendet, um die Route 53 Resolver-Regeln und Resolver-Endpunkte gemeinsam zu nutzen, die über das zentrale Shared Services-Konto konfiguriert und verwaltet werden. Route 53-Resolver-Endpunkte sind für jede Availability Zone so konfiguriert, dass sie die ausgehenden Namensauflösungsanforderungen für die Ressourcen empfängt, die sich im On-Premises-Rechenzentrum befinden, und diese Anforderungen dann an die On-Premises-DNS-Resolver weiterleitet. Die On-Premises-DNS-Resolver senden die Antworten auf die Namensauflösung an die

ausgehenden Endpunkte, die die Antworten dann an den VPC-Resolver weiterleiten. Diese Schritte richten die end-to-end Kommunikation mithilfe von Hostnamen anstelle von IP-Adressen ein.

Das folgende Diagramm zeigt die Architektur detaillierter.

Automatisierung und Skalierung

Sie können Route 53 Resolver-Regeln über AWS RAM konfigurieren und freigeben, indem Sie AWS-CloudFormation Vorlagen verwenden.

Tools

AWS-Services

- AWS Control Tower unterstützt Sie bei der Einrichtung und Verwaltung einer AWS-Umgebung mit mehreren Konten gemäß den vorgeschrieben bewährten Methoden.
- Mit AWS Resource Access Manager (AWS RAM) können Sie Ihre Ressourcen sicher über AWS-Konten hinweg freigeben, um den betrieblichen Aufwand zu reduzieren und Transparenz und Überprüfbarkeit zu gewährleisten.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Zusätzliche Tools

- nslookup und dig sind Hilfsprogramme für die Abfrage von DNS-Datensätzen.

Polen

Konfigurieren der Resolver-Endpunkte und -Regeln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie ausgehende Route 53-Resolver-Endpunkte und -Regeln.	1. Melden Sie sich bei der AWS-Managementkonsole für das AWS-Konto an, von dem aus Sie die ausgehend	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e Route 53-Resolver-Regel konfigurieren und freigeben möchten. 2. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/. 3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den Resolver-Endpunkt konfigurieren möchten. 4. Wählen Sie im Navigationsbereich Ausgehende Endpunkte und dann Endpunkte konfigurieren aus. 5. Geben Sie allgemeine Einstellungen, IP-Adressen und optionale Tag-Informationen an und wählen Sie dann Weiter aus. 6. Erstellen Sie eine oder mehrere Regeln, um die Domänennamen der DNS-Abfragen anzugeben, die Sie an Ihr Netzwerk weiterleiten möchten, und wählen Sie dann Speichern aus. Weitere Informationen finden Sie unter Weiterleiten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausgehender DNS-Abfragen an Ihr Netzwerk in der Route 53-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ausgehende Route 53-Resolver-Regeln und geben Sie sie für AWS-Prinzipale frei.	1. Öffnen Sie die AWS RAM-Konsole unter https://console.aws.amazon.com/ram/. 2. Wählen Sie im Navigationsbereich Ressourcenfreigaben und dann Ressourcenfreigabe erstellen aus. 3. Geben Sie einen Freigabenamen an. 4. Wählen Sie als Ressourcentyp Resolver-Regeln aus. 5. Wählen Sie die Resolver-Regel aus, die Sie freigeben möchten, geben Sie optionale Tag-Schlüssel- und Wertinformationen an und wählen Sie dann Weiter aus. 6. Wählen Sie die Prinzipale aus, für die Sie die Resolver-Regelressource freigeben möchten. Prinzipale können sich innerhalb oder außerhalb Ihrer AWS-Organisation befinden. Sie können beispielsweise Ihre AWS-Organisation, eine bestimmte Organisationseinheit (OU) innerhalb der Organisation oder	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein bestimmtes Konto auswählen. 7. Überprüfen und erstellen Sie die Ressourcenfreigabe . Nachdem die Ressource erstellt und freigegeben wurde, wird sie im Abschnitt Mit mir geteilt im Navigationsbereich für die Prinzipale angezeigt, für die sie freigegeben wurde. 8. Ordnen Sie die VPCs im (Prinzipal-)Konto der Resolver-Regel zu, die von den freigegebenen Services oder dem Netzwerkkonto freigegeben wurde. Weitere Informationen finden Sie unter Freigeben Ihrer AWS-Ressourcen in der AWS RAM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die ausgehende DNS-Namensauflösung.	Testen Sie die Namensauf lösung, indem Sie das Dienstprogramm nslookup oder dig auf Instances in einer VPC in einem Konto verwenden, für das Sie die Resolver-Regel freigegeben haben. Die Abfrage sollte in die IP-Adresse einer Ressource in Ihrem On-Premises-Rechen zentrum aufgelöst werden.	Allgemeines AWS

Zugehörige Ressourcen

- Auflösen von On-Premises-DNS in Hybridumgebungen (Video)
- Weiterleiten ausgehender DNS-Abfragen an Ihr Netzwerk (Dokumentation zu Route 53)
- Freigeben Ihrer AWS-Ressourcen (AWS RAM-Dokumentation)

Einrichten der DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit einem einzigen Konto

Erstellt von Abdullahi Olaoye (AWS)

Umgebung: Produktion	Technologien: Infrastruktur	AWS-Services: Amazon Route 53; Amazon VPC

Übersicht

Dieses Muster beschreibt, wie Sie eine vollständig hybride DNS-Architektur (Domain Name System) einrichten, die die end-to-end DNS-Auflösung von On-Premises-Ressourcen, AWS-Ressourcen und Internet-DNS-Abfragen ohne Verwaltungsaufwand ermöglicht. Das Muster beschreibt, wie Amazon Route 53 Resolver-Weiterleitungsregeln eingerichtet werden, die bestimmen, wohin eine DNS-Abfrage gesendet werden soll, die von AWS stammt, basierend auf dem Domänennamen. DNS-Abfragen für On-Premises-Ressourcen werden an On-Premises-DNS-Resolver weitergeleitet. DNS-Abfragen für AWS-Ressourcen und Internet-DNS-Abfragen werden von Route 53 Resolver aufgelöst.

Dieses Muster behandelt die hybride DNS-Auflösung in einer AWS-Umgebung mit einem einzigen Konto. Informationen zum Einrichten ausgehender DNS-Abfragen in einer AWS-Umgebung mit mehreren Konten finden Sie im Muster DNS-Auflösung für Hybrid-Netzwerke in einer AWS-Umgebung mit mehreren Konten einrichten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto
- Eine Virtual Private Cloud (VPC) in Ihrem AWS-Konto
- Eine Netzwerkverbindung zwischen der On-Premises-Umgebung und Ihrer VPC über AWS Virtual Private Network (AWS VPN) oder AWS Direct Connect
- IP-Adressen Ihrer On-Premises-DNS-Resolver (erreichbar von Ihrer VPC)
- Domänen-/Subdomänenname, der an On-Premises-Resolver weitergeleitet werden soll (z. B. onprem.mydc.com)

- Domänen-/Subdomänenname für die privat gehostete AWS-Zone (z. B. myvpc.cloud.com)

Architektur

Zieltechnologie-Stack

- Privat gehostete Zone von Amazon Route 53
- Amazon Route 53 Resolver
- Amazon VPC
- AWS VPN oder Direct Connect

Zielarchitektur

Tools

- Amazon Route 53 Resolver erleichtert Unternehmenskunden die Hybrid-Cloud, indem es eine nahtlose DNS-Abfrageauflösung in Ihrer gesamten Hybrid-Cloud ermöglicht. Sie können DNS-Endpunkte und Regeln für die bedingte Weiterleitung erstellen, um DNS-Namespaces zwischen Ihrem On-Premises-Rechenzentrum und Ihren VPCs aufzulösen.
- Die privat gehostete Zone von Amazon Route 53 ist ein Container, der Informationen darüber enthält, wie Route 53 auf DNS-Abfragen für eine Domäne und ihre Subdomänen innerhalb einer oder mehrerer VPCs antworten soll, die Sie mit dem Amazon-VPC-Service erstellen.

Polen

Konfigurieren einer privat gehosteten Zone

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine privat gehostete Route 53-Zone für einen reservierten	Diese Zone enthält die DNS-Datensätze für AWS-Ressourcen, die aus der On-Premises-Umgebung aufgelöst	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
AWS-Domänennamen wie myvpc.cloud.com.	werden sollen. Anweisungen finden Sie unter Erstellen einer privat gehosteten Zone in der Route 53-Dokumentation.	
Ordnen Sie die privat gehostete Zone Ihrer VPC zu.	Damit Ressourcen in Ihrer VPC DNS-Datensätze in dieser privat gehosteten Zone auflösen können, müssen Sie Ihre VPC der gehosteten Zone zuordnen. Anweisungen finden Sie unter Erstellen einer privat gehosteten Zone in der Route 53-Dokumentation.	Netzwerkadministrator, Systemadministrator

Route 53 Resolver-Endpunkte einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen eingehend en Endpunkt.	Route 53 Resolver verwendet den eingehenden Endpunkt, um DNS-Abfragen von On-Premises-DNS-Resolvern zu empfangen. Anweisungen finden Sie unter Weiterleiten eingehender DNS-Abfragen an Ihre VPCs in der Route 53-Dokumentation. Notieren Sie sich die IP-Adresse des eingehenden Endpunkts.	Netzwerkadministrator, Systemadministrator
Erstellen Sie einen ausgehend en Endpunkt.	Route 53 Resolver verwendet den ausgehenden Endpunkt, um DNS-Abfragen an On-Premises-DNS-Resolver	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zu senden. Anweisungen finden Sie unter Weiterleiten ausgehender DNS-Abfragen an Ihr Netzwerk in der Route 53-Dokumentation. Notieren Sie sich die Ausgabeen dpunkt-ID.	

Richten Sie eine Weiterleitungsregel ein und verknüpfen Sie sie mit Ihrer VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Weiterlei tungsregel für die On-Premis es-Domain.	Diese Regel weist Route 53 Resolver an, alle DNS-Abfra gen für On-Premises-Domain s (z. B. onprem.mydc.com) an On-Premises-DNS-Resolver weiterzuleiten. Um diese Regel zu erstellen, benötigen Sie die IP-Adressen der On-Premises-DNS-Resolver und die ID des ausgehend en Endpunkts für Route 53 Resolver. Anweisungen finden Sie unter Verwalten von Weiterleitungsregeln in der Route 53-Dokumentation.	Netzwerkadministrator, Systemadministrator
Ordnen Sie die Weiterlei tungsregel Ihrer VPC zu.	Damit die Weiterleitungsrege l wirksam wird, müssen Sie die Regel Ihrer VPC zuordnen. Route 53 Resolver berücksic htigt dann die Regel beim Auflösen einer Domain. Anweisungen finden Sie	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Verwalten von Weiterleitungsregeln in der Route 53-Dokumentation.	

Konfigurieren von On-Premises-DNS-Resolvern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die bedingte Weiterleitung in den On-Premises-DNS-Resolvern.	Damit DNS-Abfragen von der On-Premises-Umgebung an die privat gehostete Route 53-Zone gesendet werden, müssen Sie die bedingte Weiterleitung in den On-Premises-DNS-Resolvern konfigurieren. Dadurch werden die DNS-Resolver angewiesen, alle DNS-Abfragen für die AWS-Domain (z. B. für myvpc.cloud.com) an die eingehende Endpunkt-IP-Adresse für Route 53 Resolver weiterzuleiten.	Netzwerkadministrator, Systemadministrator

Testen der end-to-end DNS-Auflösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die DNS-Auflösung von AWS in die On-Premises-Umgebung.	Führen Sie von einem Server in der VPC aus eine DNS-Abfrage für eine On-Premises-Domain durch (z. B. server1.onprem.mydc.com).	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die DNS-Auflösung von der On-Premises-Umgebung zu AWS.	Führen Sie von einem On-Premises-Server aus die DNS-Auflösung für eine AWS-Domäne durch (z. B. server1.myvpc.cloud.com).	Netzwerkadministrator, Systemadministrator

Zugehörige Ressourcen

- Zentralisierte DNS-Verwaltung von Hybrid Cloud mit Amazon Route 53 und AWS Transit Gateway (Blog AWS Networking & Content Delivery)
- Vereinfachen der DNS-Verwaltung in einer Umgebung mit mehreren Konten mit Route 53 Resolver (AWS-Sicherheitsblog)
- Arbeiten mit privat gehosteten Zonen (Dokumentation zu Route 53)
- Erste Schritte mit Route 53 Resolver (Dokumentation zu Route 53)

Automatisches Einrichten von UiPath Bol-Bots auf Amazon EC2 mithilfe von AWS CloudFormation

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) undilsel Bol P (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; DevOps	Workload: Alle anderen Workloads
AWS-Services: Amazon CloudWatch; Amazon EC2 Image Builder; AWS Systems Manager; AWS CloudFormation		

Übersicht

In diesem Muster wird erläutert, wie Sie Bots zur Roboterprozessautomatisierung (Robotic Process Automation, RPA) auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances bereitstellen können. Es verwendet eine EC2 Image Builder-Pipeline, um ein benutzerdefiniertes Amazon Machine Image (AMI) zu erstellen. Ein AMI ist ein vorkonfiguriertes VM-Image (Virtual Machine), das das Betriebssystem (OS) und vorinstallierte Software zur Bereitstellung von EC2-Instances enthält. Dieses Muster verwendet AWS- CloudFormation Vorlagen, um die UiPath Studio Community Edition auf dem benutzerdefinierten AMI zu installieren. UiPath ist ein microSD-Tool, mit dem Sie Roboter zur Automatisierung Ihrer Aufgaben einrichten können.

Im Rahmen dieser Lösung werden EC2-Windows-Instances mit dem Basis-AMI gestartet und die UiPath Studio-Anwendung wird auf den Instances installiert. Das Muster verwendet das Microsoft System Preparation (Sysprep)-Tool, um die benutzerdefinierte Windows-Installation zu duplizieren. Danach werden die Hostinformationen entfernt und ein endgültiges AMI aus der Instance erstellt. Anschließend können Sie die Instances bei Bedarf starten, indem Sie das endgültige AMI mit Ihren eigenen Namenskonventionen und Überwachungseinstellungen verwenden.

> Hinweis: Dieses Muster enthält keine Informationen zur Verwendung von Bots. Diese Informationen finden Sie in der UiPath -Dokumentation. Sie können dieses Muster auch verwenden, um

andere Bot-Anwendungen einzurichten, indem Sie die Installationsschritte an Ihre Anforderungen anpassen.

Dieses Muster bietet die folgenden Automatisierungen und Vorteile:

- Bereitstellung und Freigabe von Anwendungen: Sie können Amazon EC2-AMIs für die Anwendungsbereitstellung erstellen und diese über eine EC2 Image Builder-Pipeline für mehrere Konten freigeben, die AWS- CloudFormation Vorlagen als Infrastructure as Code (IaC)-Skripts verwendet.
- Amazon EC2-Vorlagen für Bereitstellung und Skalierung: CloudFormation IaC bieten benutzerdefinierte Computernamensequenzen und Active-Directory-Join-Automatisierung.
- Beobachtbarkeit und Überwachung: Das Muster richtet Amazon- CloudWatch Dashboards ein, um Sie bei der Überwachung von Amazon EC2-Metriken (wie CPU- und Festplattennutzung) zu unterstützen.
- Zuverlässige Vorteile für Ihr Unternehmen: Zulässige Ergebnisse verbessern die Genauigkeit, da Roboter zugewiesene Aufgaben automatisch und konsistent ausführen können. Außerdem erhöht sich die Geschwindigkeit und Produktivität, da Vorgänge entfernt werden, die keinen Mehrwert bieten, und wiederholte Aktivitäten verarbeitet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Identity and Access Management (IAM)-Berechtigungen für die Bereitstellung von CloudFormation Vorlagen
- IAM-Richtlinien zum Einrichten einer kontoübergreifenden AMI-Verteilung mit EC2 Image Builder

Architektur

1. Der Administrator stellt das Basis-Windows-AMI in der `-ec2-image-builder.yaml`Datei bereit und stellt den Stack in der - CloudFormation Konsole bereit.

2. Der CloudFormation Stack stellt die EC2 Image Builder-Pipeline bereit, die die folgenden Ressourcen enthält:
   - `Ec2ImageInfraConfiguration`
   - `Ec2ImageComponent`
   - `Ec2ImageRecipe`
   - `Ec2AMI`
3. Die EC2 Image Builder-Pipeline startet eine temporäre Windows EC2-Instance mithilfe des Basis-AMI und installiert die erforderlichen Komponenten (in diesem Fall UiPath Studio).
4. Der EC2 Image Builder entfernt alle Hostinformationen und erstellt ein AMI von Windows Server.
5. Sie aktualisieren die `ec2-provisioning yaml` Datei mit dem benutzerdefinierten AMI und starten eine Reihe von EC2-Instances, die Ihren Anforderungen entsprechen.
6. Sie stellen das Count-Makro mithilfe einer CloudFormation Vorlage bereit. Dieses Makro bietet eine Count-Eigenschaft für CloudFormation Ressourcen, sodass Sie auf einfache Weise mehrere Ressourcen desselben Typs angeben können.
7. Sie aktualisieren den Namen des Makros in der CloudFormation `ec2-provisioning.yaml` Datei und stellen den Stack bereit.
8. Der Administrator aktualisiert die `ec2-provisioning.yaml` Datei basierend auf den Anforderungen und startet den Stack.
9. Die Vorlage stellt EC2-Instances mit der UiPath Studio-Anwendung bereit.

Tools

AWS-Services

- AWS CloudFormation unterstützt Sie bei der automatisierten und sicheren Modellierung und Verwaltung von Infrastrukturressourcen.
- Amazon CloudWatch hilft Ihnen, Ressourcen und Anwendungen in AWS, On-Premises und in anderen Clouds zu beobachten und zu überwachen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet sichere und anpassbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- EC2 Image Builder vereinfacht das Erstellen, Testen und Bereitstellen virtueller Maschinen und Container-Images für die Verwendung in AWS oder On-Premises.

- Amazon EventBridge hilft Ihnen, ereignisgesteuerte Anwendungen in großem Umfang über AWS, vorhandene Systeme oder Software-as-a-Service (SaaS)-Anwendungen hinweg zu erstellen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf AWS-Ressourcen sicher steuern. Mit IAM können Sie zentral Berechtigungen verwalten, die steuern, auf welche AWS-Ressourcen Benutzer zugreifen können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- AWS Lambda ist ein serverloser, ereignisgesteuerter Datenverarbeitungsservice, mit dem Sie Code für praktisch jeden Anwendungs- oder Backend-Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Sie können Lambda-Funktionen von über 200 AWS-Services und SaaS-Anwendungen aufrufen und nur für das bezahlen, was Sie tatsächlich nutzen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, mit dem Sie beliebige Datenmengen speichern, schützen und abrufen können.
- AWS Systems Manager Agent (SSM Agent) unterstützt Systems Manager bei der Aktualisierung, Verwaltung und Konfiguration von EC2-Instances, Edge-Geräten, On-Premises-Servern und virtuellen Maschinen (VMs).

Code-Repositorys

Der Code für dieses Muster ist in der GitHub UiPath Einrichtung des Bol-Bots mithilfe CloudFormation des Repositorys verfügbar. Das Muster verwendet auch ein Makro, das im AWS CloudFormation Makros-Repository verfügbar ist.

Bewährte Methoden

- AWS veröffentlicht jeden Monat neue Windows-AMIs. Diese enthalten die neuesten Betriebssystem-Patches, Treiber und Startagenten. Wir empfehlen Ihnen, das neueste AMI zu verwenden, wenn Sie neue Instances starten oder eigene benutzerdefinierte Images erstellen.
- Wenden Sie alle verfügbaren Windows- oder Linux-Sicherheitspatches während Image-Builds an.

Polen

Bereitstellen einer Image-Pipeline für das Basis-Image

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine EC2 Image Builder-Pipeline ein.	1. Klonen Sie die UiPath Einrichtung des Bol-Bots mithilfe CloudFormation des Repositorys oder laden Sie die `ec2-image-builder.yaml` Vorlage aus dem Repository herunter. 2. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-CloudFormation Konsole . 3. Wählen Sie Stack erstellen aus. 4. Wählen Sie im Abschnitt Specify template (Vorlage angeben) die Option Upload a template file (Vorlagen datei hochladen) aus. 5. Suchen und laden Sie die `ec2-image-builder.yaml` Vorlage von Ihrem Computer hoch und wählen Sie dann Weiter aus. 6. Geben Sie Eingabepa rameter für Ihren Stack an oder akzeptieren Sie die Standardwerte. Wählen Sie Weiter aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Die Anzahl und die Werte der Parameter können je nach Eingabewert variieren. 7. Konfigurieren Sie optional Stack-Optionen und wählen Sie dann Weiter aus. 8. Überprüfen Sie Ihre Stack-Details. 9. Aktivieren Sie am Ende des Bildschirms das Kontrollkästchen, um die Funktionen zu bestätigen, und wählen Sie dann Absenden aus. 10. Überwachen Sie den Fortschritt des Stacks. Wenn der Status lautet `CREATE_COMPLETE`, ist die Bereitstellung bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Anzeigen der EC2 Image Builder-Einstellungen.	Zu den EC2 Image Builder-Einstellungen gehören Infrastrukturkonfiguration, Verteilungseinstellungen und Sicherheitsscaneinstellungen. So zeigen Sie die Einstellungen an: 1. Öffnen Sie die EC2 Image Builder-Konsole . 2. Navigieren Sie im Navigationsbereich zu verschiedenen Image-Builder-Einstellungen. Hinweis: Als bewährte Methode sollten Sie EC2 Image Builder nur über die CloudFormation Vorlage aktualisieren.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie die Image-Pipeline an.	So zeigen Sie die bereitgestellte Image-Pipeline an: 1. Wählen Sie in der EC2 Image Builder-Konsole im Navigationsbereich Image-Pipelines aus. 2. Wählen Sie die Image-Pipeline aus, die Sie erstellt haben. 3. Zeigen Sie die Konfigurationsdetails der Ausgabeabbilder, des Image-Rezepts, der Infrastrukturkonfiguration, der Verteilungseinstellungen, der Amazon- EventBridge Regeln und der Tags an.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Image-Builder-Protokolle anzeigen.	EC2 Image Builder-Protokolle werden in CloudWatch Protokollgruppen aggregiert. So zeigen Sie die Protokolle in an CloudWatch: 1. Öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigatio nsbereich Logs (Protokol le), Log groups (Protokol lgruppen) aus. 3. Wählen Sie den Namen der Protokollgruppe aus. EC2 Image Builder-Protokolle werden in der Protokoll gruppe aggregiert `/aws/imagebuilder/XXX` . 4. Überprüfen Sie die neuesten Protokolle im jeweiligen Protokollstream auf Fehler, die beim Ausführen der Image-Pip eline auftreten. EC2 Image Builder-Protokolle werden auch in einem S3-Bucket gespeichert. So zeigen Sie die Protokolle im Bucket an: 1. Öffnen Sie die Amazon S3-Konsole.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie in der Liste Buckets den Namen des Buckets aus. Die Protokolle werden im S3-Bucket aggregiert<stack-name>-XXXXXX .	
Laden Sie die UiPath Datei in einen S3-Bucket hoch.	1. Laden Sie die `.msi` Datei für UiPath Studio vom Speicherort https://download.uipath.com/UiPathStudioCommunity.msi herunter. 2. Laden Sie die Datei zu einem S3-Bucket hoch. 3. Aktualisieren Sie den Bucket-Namen und den Dateischlüssel in der `ec2-image-builder.yaml` Vorlage im Abschnitt Benutzerdaten Zeile 310.	AWS DevOps

Bereitstellen und Testen des Count-Makros

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Count-Makro bereit.	1. Klonen oder laden Sie das Count- CloudFormation Makro herunter. 2. Navigieren Sie zum Verzeichnis `Count`. 3. Sie benötigen einen S3-Bucket, um die CloudFormation Artefakte zu speichern	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	. Wenn Sie noch keinen S3-Bucket haben, erstellen Sie einen mit dem Namen `aws s3 mb s3://<bucket name>`.
	4. Verpacken Sie die Zählen-Makrovorlage. Die Vorlage verwendet das AWS Serverless Application Model (SAM), daher muss es transformiert werden, bevor Sie es bereitstellen können.
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket <your bucket name here> \ --output-template-file packaged.yaml`
	Beispielsweise:
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket count-macro-ec2 \ --output-template-file packaged.yaml`
	5. Stellen Sie die verpackte Vorlage bereit, um einen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudFormation Stack zu erstellen. `aws cloudformation deploy \ --stack-name Count-macro \ --template-file packaged.yaml \ --capabilities CAPABILITY_IAM` Wenn Sie die Konsole verwenden möchten, folgen Sie den Anweisungen im vorherigen Epi oder in der CloudFormation Dokumentation .	
Testen Sie das Count-Makro.	Um die Funktionen des Makros zu testen, versuchen Sie, die Beispielvorlage zu starten, die mit dem Makro bereitgestellt wird. `aws cloudformation deploy \ --stack-name Count-test \ --template-file test.yaml \ --capabilities CAPABILITY_IAM`	DevOps Techniker

Stellen Sie den CloudFormation Stack bereit, um Instances mit dem benutzerdefinierten Image bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Amazon EC2-Bereitstellungsvorlage bereit.	So stellen Sie EC2 Image Pipeline mithilfe von bereit CloudFormation: 1. Laden Sie die `ec2-provisioning.yaml` Vorlage aus dem GitHub Repository herunter oder suchen Sie sie auf Ihrem Computer, wenn Sie das Repository geklont haben. 2. Öffnen Sie die CloudFormation -Konsole. 3. Wiederholen Sie die Schritte aus dem ersten Epic (oder folgen Sie den Anweisungen in der CloudFormation Dokumentation), um bereitzustellen`ec2-provisioning.yaml` .	AWS DevOps
Anzeigen der Amazon EC2-Einstellungen.	Zu den Amazon EC2-Einstellungen gehören Sicherheits-, Netzwerk-, Speicher-, Statusprüfungen, Überwachung und Tag-Konfigurationen. So zeigen Sie diese Konfigurationen an: 1. Öffnen Sie die Amazon EC2-Konsole.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigationsbereich Instances und dann die EC2-Instance aus, die von der Amazon EC2-Bereitstellungsvorlage erstellt wurde. 3. Wählen Sie in der Instance-Zusammenfassung die Registerkarten aus, um die entsprechenden Amazon EC2-Einstellungen anzuzeigen.	
Zeigen Sie das CloudWatch Dashboard an.	1. Öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigationsbereich Dashboards aus. 3. Wählen Sie das Dashboard mit Ihrem Stack-Namen aus. Hinweis: Nachdem Sie den Stack bereitgestellt haben, dauert es einige Zeit, bis das Dashboard mit Metriken gefüllt ist. Das Dashboard stellt diese Metriken bereit: `CPUUtilization` , `DiskUtilization` , `MemoryUtilization` , `NetworkIn` , `NetworkOut` , `StatusCheckFailed` .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie benutzerdefinierte Metriken für die Speicher- und Festplattennutzung an.	1. Wählen Sie in der CloudWatch Konsole Dashboards aus. 2. Wählen Sie im Navigationsbereich Metrics (Metriken) All metrics (Alle Metriken) aus. 3. Wählen Sie Benutzerdefinierte Namespaces, CWAgent aus.	AWS DevOps
Anzeigen von Alarmen für die Speicher- und Festplattennutzung.	1. Wählen Sie im Navigationsbereich der CloudWatch Konsole Dashboards aus. 2. Wählen Sie All alarms (Alle Warnungen) aus.	AWS DevOps
Überprüfen Sie die Snapshot-Lebenszyklusregel.	1. Öffnen Sie die Amazon EC2-Konsole. 2. Wählen Sie im Navigationsbereich Lifecycle Manager aus. 3. Überprüfen Sie die Einstellungen für den AMI-Lebenszyklus.	AWS DevOps

Löschen der Umgebung (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Stacks.	Wenn Ihr PoC- oder Pilotprojekt abgeschlossen ist, empfehlen wir Ihnen, die von Ihnen erstellten Stacks zu	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	löschen, um sicherzustellen, dass Ihnen diese Ressourcen nicht in Rechnung gestellt werden. 1. Öffnen Sie die AWS-CloudFormation Konsole . 2. Wählen Sie im Navigationsbereich Stacks und dann einen oder beide Stacks aus, die Sie zuvor erstellt haben und die Sie löschen möchten. Der Stack muss aktuell ausgeführt werden. 3. Wählen Sie im Stack-Detailbereich Delete (Löschen) aus. 4. Wählen Sie bei Aufforderung Delete stack (Stack löschen) aus. Wichtig: Der Stack-Löschvorgang kann nach Beginn nicht mehr gestoppt werden. Der Stack wird in den Status `DELETE_IN_PROGRESS` versetzt. Wenn der Löschvorgang fehlschlägt, befindet sich der Stack im `DELETE_FAILED` Status . Lösungen finden Sie unter Delete stack fail in der AWS-Dokumentation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zur CloudFormation Fehlerbehebung. Informationen zum Schutz von Stacks vor versehentlichem Löschen finden Sie unter Schutz eines Stacks vor dem Löschen in der AWS-CloudFormation Dokumentation.	

Fehlerbehebung

Problem	Lösung
Wenn Sie die Amazon EC2-Bereitstellungsvorlage bereitstellen, erhalten Sie die Fehlermeldung: Fehlerhafte Antwort von Transformation 123xxxx::Count .	Dies ist ein bekanntes Problem. (Siehe die benutzerdefinierte Lösung und PR im AWS-CloudFormation Makro-Repository .) Um dieses Problem zu beheben, öffnen Sie die AWS Lambda-Konsole und aktualisieren Sie `index.py` mit dem Inhalt aus dem GitHub Repository .

Zugehörige Ressourcen

GitHub -Repositorys

- UiPath Einrichtung eines microSD-Bots mit CloudFormation
- CloudFormation Makro zählen

AWS-Referenzen

- Erstellen eines Stacks in der AWS- CloudFormation Konsole (CloudFormation Dokumentation)

- Fehlerbehebung CloudFormation (CloudFormation Dokumentation)
- Überwachen von Arbeitsspeicher- und forAmazonEC2-Instances (Amazon EC2Dokumentation)
- Wie kann ich den CloudWatch Agenten verwenden, um Metriken für Performance Monitor auf einem Windows-Server anzuzeigen? (AWS re:Post-Artikel)

Zusätzliche Referenzen

- UiPath -Dokumentation
- Festlegen des Hostnamens in einem SysPreped AMI (Blogbeitrag von Brian)
- Wie kann ich Cloudformation eine Vorlage mit einem Makro erneut verarbeiten, wenn sich die Parameter ändern? (Stack-Überlauf)

Einrichten der Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery

Erstellt von Thanigaivelrumalai (AWS)

Umgebung: Produktion	Technologien: Infrastruktur; Migration; Netzwerk	Workload: Oracle
AWS-Services: AWS Elastic Disaster Recovery; Amazon EC2		

Übersicht

Katastrophen, die durch natürliche Katastrophen, Anwendungsausfälle oder Störungen der -Services ausgelöst werden, beeinträchtigen den Umsatz und führen zu Ausfallzeiten für Unternehmensanwendungen. Um die Auswirkungen solcher Ereignisse zu reduzieren, ist die Planung für die Notfallwiederherstellung (DR) für Unternehmen von entscheidender Bedeutung, die Enterprise EnterpriseOne Resource Planning (ERP)-Systeme von JD Edwards und andere geschäftskritische und geschäftskritische Software einsetzen.

Dieses Muster erklärt, wie Unternehmen AWS Elastic Disaster Recovery als DR-Option für ihre JD Edwards- EnterpriseOne Anwendungen verwenden können. Es beschreibt auch die Schritte zur Verwendung von Elastic Disaster Recovery-Failover und -Failback, um eine regionsübergreifende DR-Strategie für Datenbanken zu erstellen, die auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance in der AWS Cloud gehostet werden.

Hinweis: Für dieses Muster müssen die primären und sekundären Regionen für die regionsübergreifende DR-Implementierung in AWS gehostet werden.

Oracle JD Edwards EnterpriseOne ist eine integrierte Bol-Softwarelösung für mittelgroße bis große Unternehmen in einer Vielzahl von Branchen.

AWS Elastic Disaster Recovery minimiert Ausfallzeiten und Datenverluste mit schneller, zuverlässiger Wiederherstellung von On-Premises- und Cloud-basierten Anwendungen, indem kostengünstiger Speicher, minimale Rechenleistung und point-in-time Wiederherstellung verwendet werden.

AWS bietet vier zentrale DR-Architekturmuster. Dieses Dokument konzentriert sich auf Einrichtung, Konfiguration und Optimierung mithilfe der Pilot-Light-Strategie . Diese Strategie hilft Ihnen, eine kostengünstigere DR-Umgebung zu erstellen, in der Sie zunächst einen Replikationsserver für die Replikation von Daten aus der Quelldatenbank bereitstellen und den tatsächlichen Datenbankserver nur bereitstellen, wenn Sie eine DR-Drossel und Wiederherstellung starten. Diese Strategie eliminiert die Kosten für die Wartung eines Datenbankservers in der DR-Region. Stattdessen zahlen Sie für eine kleinere EC2-Instance, die als Replikationsserver dient.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine JD Edwards- EnterpriseOne Anwendung, die auf Oracle Database oder Microsoft SQL Server mit einer unterstützten Datenbank ausgeführt wird, die sich im laufenden Zustand auf einer verwalteten EC2-Instance befindet. Diese Anwendung sollte alle JD Edwards- EnterpriseOne Basiskomponenten (Enterprise Server, HTML Server und Database Server) enthalten, die in einer AWS-Region installiert sind.
- Eine AWS Identity and Access Management (IAM)-Rolle zum Einrichten des Elastic Disaster Recovery-Services.
- Das Netzwerk für die Ausführung von Elastic Disaster Recovery, das gemäß den erforderlichen Konnektivitätseinstellungen konfiguriert ist.

Einschränkungen

- Sie können dieses Muster verwenden, um alle Ebenen zu replizieren, es sei denn, die Datenbank wird auf Amazon Relational Database Service (Amazon RDS) gehostet. In diesem Fall empfehlen wir Ihnen, die regionsübergreifende Kopierfunktion von Amazon RDS zu verwenden.
- Elastic Disaster Recovery ist nicht mit CloudEndure Disaster Recovery kompatibel, aber Sie können ein Upgrade von CloudEndure Disaster Recovery durchführen. Weitere Informationen finden Sie unter Häufig gestellte Fragen in der Elastic Disaster Recovery-Dokumentation.
- Amazon Elastic Block Store (Amazon EBS) begrenzt die Geschwindigkeit, mit der Sie Snapshots erstellen können. Sie können eine maximale Anzahl von 300 Servern in einem einzigen AWS-Konto replizieren, indem Sie Elastic Disaster Recovery verwenden. Um mehr Server zu replizieren, können Sie mehrere AWS-Konten oder mehrere AWS-Zielregionen verwenden. (Sie müssen Elastic Disaster Recovery für jedes Konto und jede Region separat einrichten.)

Weitere Informationen finden Sie unter Bewährte Methoden in der Elastic Disaster Recovery-Dokumentation.

- Die Quell-Workloads (die JD Edwards- EnterpriseOne Anwendung und -Datenbank) müssen auf EC2-Instances gehostet werden. Dieses Muster unterstützt keine Workloads, die sich On-Premises oder in anderen Cloud-Umgebungen befinden.
- Dieses Muster konzentriert sich auf die EnterpriseOne Komponenten von JD Edwards. Ein vollständiger DR- und Business Continuity Plan (BCP) sollte andere Kernservices enthalten, darunter:
  - Netzwerk (virtuelle private Cloud, Subnetze und Sicherheitsgruppen)
  - Active Directory
  - Amazon WorkSpaces
  - Elastic Load Balancing
  - Ein verwalteter Datenbankservice wie Amazon Relational Database Service (Amazon RDS)

Weitere Informationen zu Voraussetzungen, Konfigurationen und Einschränkungen finden Sie in der Elastic Disaster Recovery-Dokumentation.

Produktversionen

- Oracle JD Edwards EnterpriseOne (unterstützte Oracle- und SQL Server-Versionen, die auf den technischen Mindestanforderungen von Oracle basieren)

Architektur

Zieltechnologie-Stack

- Eine einzelne Region und eine einzelne Virtual Private Cloud (VPC) für Produktion und Nicht-Produktion sowie eine zweite Region für DR
- Einzelne Availability Zones zur Gewährleistung einer niedrigen Latenz zwischen Servern
- Ein Application Load Balancer, der den Netzwerkverkehr verteilt, um die Skalierbarkeit und Verfügbarkeit Ihrer Anwendungen über mehrere Availability Zones hinweg zu verbessern
- Amazon Route 53 zur Bereitstellung der DNS-Konfiguration (Domain Name System)
- Amazon WorkSpaces , um Benutzern ein Desktop-Erlebnis in der Cloud zu bieten
- Amazon Simple Storage Service (Amazon S3) zum Speichern von Backups, Dateien und Objekten

- Amazon CloudWatch für Anwendungsprotokollierung, Überwachung und Alarme
- Amazon Elastic Disaster Recovery für die Notfallwiederherstellung

Zielarchitektur

Das folgende Diagramm zeigt die regionsübergreifende Notfallwiederherstellungsarchitektur für JD Edwards EnterpriseOne mit Elastic Disaster Recovery.

Verfahren

Hier ist eine allgemeine Überprüfung des Prozesses. Weitere Informationen finden Sie im Abschnitt Echocs.

- Die Elastic-Disaster-Recovery-Replikation beginnt mit einer ersten Synchronisierung. Während der ersten Synchronisierung repliziert der AWS Replication Agent alle Daten von den Quelldatenträgern auf die entsprechende Ressource im Subnetz des Staging-Bereichs.
- Die kontinuierliche Replikation wird unbegrenzt fortgesetzt, nachdem die erste Synchronisierung abgeschlossen ist.
- Sie überprüfen die Startparameter, die servicespezifische Konfigurationen und eine Amazon EC2-Startvorlage enthalten, nachdem der Agent installiert und die Replikation gestartet wurde. Wenn der Quellserver als bereit für die Wiederherstellung angezeigt wird, können Sie Instances starten.
- Wenn Elastic Disaster Recovery eine Reihe von API-Aufrufen ausgibt, um den Startvorgang zu starten, wird die Wiederherstellungs-Instance gemäß Ihren Starteinstellungen sofort in AWS gestartet. Der Service startet beim Start automatisch einen Konvertierungsserver.
- Die neue Instance wird in AWS gestartet, nachdem die Konvertierung abgeschlossen ist und einsatzbereit ist. Der Quellserverstatus zum Zeitpunkt des Starts wird durch die Volumes dargestellt, die der gestarteten Instance zugeordnet sind. Der Konvertierungsprozess beinhaltet Änderungen an Treibern, Netzwerken und Betriebssystemlizenzen, um sicherzustellen, dass die Instance nativ in AWS gestartet wird.
- Nach dem Start werden die neu erstellten Volumes nicht mehr mit den Quellservern synchronisiert. Der AWS Replication Agent repliziert weiterhin routinemäßig Änderungen an Ihren Quellservern auf den Staging-Bereich-Volumes, aber die gestarteten Instances spiegeln diese Änderungen nicht wider.

- Wenn Sie eine neue Drill- oder Wiederherstellungs-Instance starten, spiegeln sich die Daten immer im neuesten Zustand wider, der vom Quellserver in das Subnetz des Staging-Bereichs repliziert wurde.
- Wenn der Quellserver als für die Wiederherstellung vorbereitet markiert ist, können Sie Instances starten.

Hinweis: Der Prozess funktioniert auf beide Arten: für Failover von einer primären AWS-Region zu einer DR-Region und für ein Failover zum primären Standort, wenn er wiederhergestellt wurde. Sie können sich auf ein Failback vorbereiten, indem Sie die Richtung der Datenreplikation vollständig orchestriert vom Zielcomputer zurück zum Quellcomputer umkehren.

Zu den Vorteilen dieses in diesem Muster beschriebenen Prozesses gehören:

- Flexibilität: Replikationsserver skalieren basierend auf Datensatz und Replikationszeit auf und ab, sodass Sie DR-Tests durchführen können, ohne Quell-Workloads oder Replikation zu unterbrechen.
- Zuverlässigkeit: Die Replikation ist robust, unterbrechungsfrei und kontinuierlich.
- Automatisierung: Diese Lösung bietet einen einheitlichen, automatisierten Prozess für Test, Wiederherstellung und Failback.
- Kostenoptimierung: Sie können nur die benötigten Volumes replizieren und dafür bezahlen und nur dann für Rechenressourcen am DR-Standort bezahlen, wenn diese Ressourcen aktiviert sind. Sie können eine kostenoptimierte Replikations-Instance (wir empfehlen, einen rechenoptimierten Instance-Typ zu verwenden) für mehrere Quellen oder eine einzelne Quelle mit einem großen EBS-Volume verwenden.

Automatisierung und Skalierung

Wenn Sie eine Notfallwiederherstellung in großem Umfang durchführen, sind die JD-Edwards-EnterpriseOne Server von anderen Servern in der Umgebung abhängig. Beispielsweise:

- JD Edwards- EnterpriseOne Anwendungsserver, die beim Booten eine Verbindung zu einer von JD Edwards EnterpriseOne unterstützten Datenbank herstellen, sind von dieser Datenbank abhängig.
- JD-Edwards- EnterpriseOne Server, die eine Authentifizierung erfordern und beim Booten eine Verbindung zu einem Domain-Controller herstellen müssen, um Services zu starten, sind vom Domain-Controller abhängig.

Aus diesem Grund empfehlen wir Ihnen, Failover-Aufgaben zu automatisieren. Sie können beispielsweise AWS Lambda oder AWS Step Functions verwenden, um die EnterpriseOne Startskripte von JD Edwards und Load Balancer-Änderungen zu automatisieren, um den end-to-end Failover-Prozess zu automatisieren. Weitere Informationen finden Sie im Blogbeitrag Erstellen eines skalierbaren Notfallwiederherstellungsplans mit AWS Elastic Disaster Recovery.

Tools

AWS-Services

- Amazon Elastic Block Store (Amazon EBS) bietet Volumes für die Speicherung auf Blockebene, die mit EC2-Instances verwendet werden.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Elastic Disaster Recovery minimiert Ausfallzeiten und Datenverluste mit schneller, zuverlässiger Wiederherstellung von On-Premises- und Cloud-basierten Anwendungen mit kostengünstigem Speicher, minimaler Rechenleistung und point-in-time Wiederherstellung.
- Amazon Virtual Private Cloud (Amazon VPC) bietet Ihnen die volle Kontrolle über Ihre virtuelle Netzwerkumgebung, einschließlich Ressourcenplatzierung, Konnektivität und Sicherheit.

Bewährte Methoden

Allgemeine bewährte Methoden

- Führen Sie einen eigenen Plan darüber durch, was im Falle eines realen Wiederherstellungsereignisses zu tun ist.
- Nachdem Sie Elastic Disaster Recovery korrekt eingerichtet haben, erstellen Sie bei Bedarf eine AWS- CloudFormation Vorlage, die die Konfiguration bei Bedarf erstellen kann. Bestimmen Sie die Reihenfolge, in der Server und Anwendungen gestartet werden sollen, und notieren Sie dies im Wiederherstellungsplan.
- Führen Sie einen regulären Drill durch (es gelten die Standardgebühren für Amazon EC2).
- Überwachen Sie den Zustand der laufenden Replikation mithilfe der Elastic Disaster Recovery-Konsole oder programmgesteuert.
- Schützen Sie die point-in-time Snapshots und bestätigen Sie dies, bevor Sie die Instances beenden.

- Erstellen Sie eine IAM-Rolle für die Installation von AWS Replication Agent.
- Aktivieren Sie den Beendigungsschutz für Wiederherstellungs-Instances in einem echten DR-Szenario.
- Verwenden Sie die Aktion Disconnect from AWS in der Elastic Disaster Recovery-Konsole nicht für Server, für die Sie Wiederherstellungs-Instances gestartet haben, auch nicht im Falle eines echten Wiederherstellungsereignisses. Durch das Durchführen einer Trennung werden alle Replikationsressourcen im Zusammenhang mit diesen Quellservern beendet, einschließlich Ihrer point-in-time (PIT)-Wiederherstellungspunkte.
- Ändern Sie die PIT-Richtlinie, um die Anzahl der Tage für die Snapshot-Aufbewahrung zu ändern.
- Bearbeiten Sie die Startvorlage in den Starteinstellungen von Elastic Disaster Recovery, um das richtige Subnetz, die richtige Sicherheitsgruppe und den richtigen Instance-Typ für Ihren Zielserver festzulegen.
- Automatisieren Sie den end-to-end Failover-Prozess, indem Sie Lambda oder Step Functions verwenden, um EnterpriseOne Startskripte von JD Edwards und Load Balancer-Änderungen zu automatisieren.

EnterpriseOne Optimierung und Überlegungen von JD Edwards

- Verschieben Sie PrintQueue in die Datenbank.
- Verschieben Sie MediaObjects in die Datenbank.
- Schließen Sie die Protokolle und den temporären Ordner von Batch- und Logikservern aus.
- Schließen Sie den temporären Ordner von Oracle aus WebLogic.
- Erstellen Sie Skripts für den Start nach dem Failover.
- Schließen Sie tempdb für SQL Server aus.
- Schließen Sie die temporäre Datei für Oracle aus.

Polen

Durchführen von ersten Aufgaben und Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Replikati onsnetzwerk ein.	Implementieren Sie Ihr JD Edwards- EnterpriseOne	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	System in der primären AWS-Region und identifizieren Sie die AWS-Region für DR. Führen Sie die Schritte im Abschnitt Anforderungen an das Replikationsnetzwerk der Elastic-Disaster-Recovery-Dokumentation aus, um Ihre Replikation und Ihr DR-Netzwerk zu planen und einzurichten.	
Bestimmen Sie RPO und RTO.	Identifizieren Sie das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für Ihre Anwendungsserver und Ihre Datenbank.	Cloud-Architekt, DR-Architekt
Aktivieren Sie die Replikation für Amazon EFS .	Aktivieren Sie gegebenenfalls die Replikation von der AWS-Primär- zur DR-Region für gemeinsam genutzte Dateisysteme wie Amazon Elastic File System (Amazon EFS), indem Sie AWS DataSync, rsync oder ein anderes geeignetes Tool verwenden.	Cloud-Administrator
Verwalten Sie DNS im Falle einer DR.	Identifizieren Sie den Prozess zum Aktualisieren des Domain Name System (DNS) während des DR-Drills oder der tatsächlichen DR.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für die Einrichtung.	Folgen Sie den Anweisungen im Abschnitt Initialisierung und Berechtigungen von Elastic Disaster Recovery in der Elastic Disaster Recovery-Dokumentation, um eine IAM-Rolle zur Initialisierung und Verwaltung des AWS-Services zu erstellen.	Cloud-Administrator
Richten Sie VPC-Peering ein.	Stellen Sie sicher, dass die Quell- und Ziel-VPCs durch Peering verbunden sind und miteinander zugänglich sind. Eine Konfigurationsanleitung finden Sie in der Amazon-VPC-Dokumentation.	AWS-Administrator

Konfigurieren der Elastic-Disaster-Recovery-Replikationseinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Elastic Disaster Recovery.	Öffnen Sie die Elastic Disaster Recovery-Konsole, wählen Sie die AWS-Zielregion aus (in der Sie Daten replizieren und Wiederherstellungs-Instances starten) und wählen Sie dann Standardreplikationseinstellungen festlegen aus.	AWS-Administrator
Richten Sie Replikationsserver ein.	1. Geben Sie im Bereich Replikationsserver einrichten das Stagingbereich-Subnetz und den Instance-Typ	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Replikationsservers ein. Standardmäßig ist der Instance-Typ `t3.small` ausgewählt. Konfiguri eren Sie diese Einstellu ng basierend auf Ihren Anforderungen und denken Sie daran, die Instance-Preise zu berücksichtigen. Weitere Informationen dazu finden Sie unter Amazon EC2 – Preise. 2. Wählen Sie im Abschnitt Servicezugriff die Option Details anzeigen aus, um die serviceverknüpfte Rolle und zusätzliche Richtlinien zu überprüfen, die während der Serviceinitialisierung erstellt wurden. 3. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Volumes und Sicherheitsgruppen.	1. Wählen Sie im Bereich Volumes und Sicherheitsgruppen den EBS-Volume-Typ für den Replikationsserver aus und legen Sie die Amazon-EBS-Verschlüsselung auf Standard fest. 2. Wählen Sie Immer die AWS Elastic Disaster Recovery-Sicherheitsgruppe verwenden aus, damit Elastic Disaster Recovery automatisch die Standardsicherheitsgruppe anfügt und überwacht. 3. Wählen Sie Weiter aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie zusätzliche Einstellungen.	1. Konfigurieren Sie im Bereich Zusätzliche Einstellungen Datenweit erleitung und -drosselung, PIT-Richtlinie und Tags. • Datenweiterleitung und Drosselung steuern, wie Daten vom externen Server zu den Replikati onsservern fließen. Wählen Sie Private IP für die Datenrepl ikation verwenden aus. Andernfalls wird Replikati onsservern automatis ch eine öffentliche IP zugewiesen und die Daten werden über das öffentliche Internet geleitet. • Konfigurieren Sie im Abschnitt Point-in-Time (PIT)-Richtlinie eine Aufbewahrungsricht linie, die die Dauer bestimmt, nach der keine Snapshots erforderlich sind. Der Standarda ufbewahrungszeitraum beträgt sieben Tage. • Fügen Sie im Abschnitt Tags benutzerdefinierte Tags zu Ressourcen hinzu, die von Elastic	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Disaster Recovery in Ihrem AWS-Konto erstellt wurden. 2. Wählen Sie Weiter, überprüfen Sie die Einstellungen im nächsten Bereich und wählen Sie dann Standard erstellen, um die Standardvorlage zu erstellen.	

Installieren des AWS Replication Agent

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Erstellen Sie eine IAM-Rolle, die die `AWSElasticDisasterRecoveryAgentInstallationPolicy` Richtlinie enthält. Aktivieren Sie im Abschnitt AWS-Zugriffstyp auswählen den programmgesteuerten Zugriff. Notieren Sie sich die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel. Sie benötigen diese Informationen während der Installation des AWS Replication Agent.	AWS-Administrator
Überprüfen Sie die Anforderungen.	Überprüfen und erfüllen Sie die Voraussetzungen in der Elastic Disaster Recovery-Dokumentation für die Installat	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ion des AWS Replication Agent.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den AWS Replication Agent.	Folgen Sie den Installationsanweisungen für Ihr Betriebssystem und installieren Sie den AWS Replication Agent. • Für Microsoft Windows: Laden Sie die Setup-Dateien herunter und führen Sie die .exe-Datei als Administrator aus. Antworten Sie auf die Eingabeaufforderungen, um die Installation abzuschließen. • Für Linux: Kopieren Sie die folgenden Befehle (in der angegebenen Reihenfolge) und fügen Sie sie in Ihre Secure Shell (SSH)-Sitzung ein. Der erste Befehl lädt das Installationsprogramm herunter und der zweite Befehl führt es aus. `wget -O ./aws-replication-installer-init.py https://aws-elastic-disaster-recovery-us-west-2.s3.amazonaws.com/latest/linux/aws-replication-installer-init.py`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Ändern Sie die URL so, dass sie Ihrer Region entspricht. `sudo python3 aws-replication-installer-init.py` Antworten Sie auf die Eingabeaufforderungen, um die Installation abzuschließen. Wiederholen Sie diese Schritte für den verbleibenden Server.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie die Replikation.	Kehren Sie zum Bereich Elastic-Disaster-Recovery-Quellserver zurück, um den Replikationsstatus zu überwachen. Die erste Synchronisierung dauert je nach Größe der Datenübertragung einige Zeit. Wenn der Quellserver vollständig synchronisiert ist, wird der Serverstatus auf Bereit aktualisiert. Das bedeutet, dass im Staging-Bereich ein Replikationsserver erstellt und die EBS-Volumes vom Quellserver in den Staging-Bereich repliziert wurden.	AWS-Administrator

Konfigurieren von Starteinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Starteinstellungen.	Um die Starteinstellungen für die Drill- und Wiederherstellungs-Instances zu aktualisieren, wählen Sie in der Elastic-Disaster-Recovery-Konsole den Quellserver und dann Aktionen, Starteinstellungen bearbeiten aus. Oder Sie können Ihre replizierenden Quellcomputer auf der	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Seite Quellserver und dann die Registerkarte Starteinstellungen auswählen. Diese Registerkarte besteht aus zwei Abschnitten: Allgemeine Starteinstellungen und EC2-Startvorlage .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie allgemeine Starteinstellungen.	Überarbeiten Sie die allgemeinen Starteinstellungen entsprechend Ihren Anforderungen. • Instance-Typ richtig dimensioniert: Wenn Sie Basic wählen, umgeht Elastic Disaster Recovery den Instance-Typ, den Sie in der Amazon EC2-Startvorlage ausgewählt haben, und wählt automatisch den Instance-Typ basierend auf Betriebssystem, CPU und RAM des Quellservers aus. • Private IP kopieren: Wählen Sie aus, ob Elastic Disaster Recovery sicherstellen soll, dass die private IP, die von der Drill- oder Wiederherstellungs-Instance verwendet wird, mit der privaten IP übereinstimmt, die vom Quellserver verwendet wird. Wenn Sie Ja ausgewählt haben, stellen Sie sicher, dass der IP-Bereich des Subnetzes, das Sie in der Amazon EC2-Startvorlage festgelegt haben, die private IP-Adresse enthält.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Allgemeine Starteinstellungen in der Elastic Disaster Recovery-Dokumentation.	
Konfigurieren Sie die Amazon EC2-Startvorlage.	Elastic Disaster Recovery verwendet Amazon EC2-Startvorlagen, um Drill- und Wiederherstellungs-Instances für jeden Quellserver zu starten. Die Startvorlage wird automatisch für jeden Quellserver erstellt, den Sie nach der Installation des AWS Replication Agent zu Elastic Disaster Recovery hinzufügen. Sie müssen die Amazon EC2-Startvorlage als Standardstartvorlage festlegen, wenn Sie sie mit Elastic Disaster Recovery verwenden möchten. Weitere Informationen finden Sie unter EC2-Startvorlage in der Elastic-Disaster-Recovery-Dokumentation.	AWS-Administrator

DR-Drosselung und Failover initiieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren von Drill	1. Öffnen Sie in der Elastic-Disaster-Recovery-Konsole die Seite Quellserver und überprüfen Sie, ob der Status des Quellservers Bereit lautet. 2. Wählen Sie alle Quellserver aus, für die Sie die DR-Drosselung durchführen möchten. 3. Wählen Sie im Menü Wiederherstellungsauftrag initiieren die Option Drill initiieren und wählen Sie den entsprechenden point-in-time Snapshot aus. Dadurch wird ein Wiederherstellungsauftrag für die ausgewählten Quellserver gestartet. Sie können den Status des Auftrags auf der Registerkarte Wiederherstellungsauftragsverlauf überwachen. Hinweis: Weitere Änderungen am Quellserver werden mit dem Replikationsserver synchronisiert, nicht mit der Drill-Instance. Die gestartete Drill-Instance wird auch auf der	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Seite Wiederherstellungs-Instances angezeigt. 4. Testen und überprüfen Sie die DR-Drill-Instance. 5. Wählen Sie auf der Seite Wiederherstellungs-Instances die Drill-Instance aus und wählen Sie dann Aktionen, Verbindung zu AWS trennen aus. Dadurch wird der AWS Replication Agent aus der Wiederher stellungs-Instance gelöscht und alle Ressourcen, die der Wiederherstellungs-Instance zugeordnet sind, werden aus Elastic Disaster Recovery entfernt. 6. Wählen Sie Wiederher stellungs-Instances löschen aus. Dadurch wird die Darstellung der Instance aus der Elastic Disaster Recovery-Konsole gelöscht und die Zuordnung der Instance zum Elastic Disaster Recovery-Service wird vollständig aufgehobe n. Die zugrunde liegende EC2-Instance wird nicht gelöscht. 7. Beenden Sie die DR-Drill-Instance über die Amazon EC2-Konsole.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Vorbereiten auf ein Failover in der Elastic-Disaster-Recovery-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie den Drill.	Im vorherigen Schritt haben Sie neue Ziel-Instances in der DR-Region gestartet. Die Ziel-Instances sind Replikate der Quellserver basierend auf dem Snapshot, der beim Start erstellt wurde. In diesem Verfahren stellen Sie eine Verbindung zu Ihren Amazon EC2-Zielcomputern her, um zu bestätigen, dass sie wie erwartet ausgeführt werden. 1. Öffnen Sie die Amazon EC2-Konsole. 2. Wählen Sie Instances (ausgeführt) aus. 3. Wählen Sie die Ziel-Instance aus und notieren Sie sich deren private IPv4-Adresse. 4. Stellen Sie sicher, dass Sie eine Verbindung mit der EC2-Instance herstellen können und dass die JD Edwards EnterpriseOne und die zugehörigen Komponenten wie erwartet repliziert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie ein Failover.	Ein Failover ist die Umleitung des Datenverkehrs von einem primären System zu einem sekundären System. Elastic Disaster Recovery unterstützt Sie bei der Durchführung eines Failovers, indem Wiederherstellungs-Instances in AWS gestartet werden. Wenn die Wiederherstellungs-Instances gestartet wurden, leiten Sie den Datenverkehr von Ihren Primärsystemen zu diesen Instances um. 1. Öffnen Sie auf der Elastic-Disaster-Recovery-Konsole die Seite Quellserver und überprüfen Sie, ob in der Spalte Bereit für die Wiederherstellung für den Quellserver Bereit und in der Spalte Status der Datenreplikation Zustand angezeigt wird. 2. Wählen Sie den Quellserver aus. Wählen Sie im Menü Wiederherstellungsauftrag initiieren die Option Wiederherstellung initiieren aus. 3. Wählen Sie den point-in-time Snapshot aus, aus dem die Wiederherstellungs	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-Instance gestartet werden soll, und wählen Sie dann Wiederherstellung initiieren aus. Dadurch wird ein Wiederherstellungsauftrag gestartet. Sie können den Status des Auftrags auf der Seite Wiederherstellungs-Instances überwachen. 4. Testen und überprüfen Sie die Wiederherstellungs-Instance. Passen Sie bei Bedarf die DNS-Konfiguration an und verbinden Sie Ihre JD Edwards-EnterpriseOne Anwendung mit der Datenbank. 5. Sie können jetzt den Quell-JD-Edwards- EnterpriseOne Server trennen und außer Betrieb nehmen, da alle Änderungen auf die neue Wiederherstellungs-Instance geschrieben wurden. 6. Registrieren Sie die Wiederherstellungs-Instance als Quellserver in der DR-Region, indem Sie den unter AWS Replication Agent installieren beschriebenen Prozess befolgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Durchführen eines Failovers in der Elastic-Disaster-Recovery-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie ein Failback.	Der Prozess zum Initiieren eines Failovers ähnelt dem Prozess zum Initiieren eines Failovers. 1. Öffnen Sie die Elastic Disaster Recovery-Konsole in der primären Region. Navigieren Sie zur Seite Wiederherstellungs-Instances, wählen Sie die Drill-Instance aus und wählen Sie dann Aktionen, Verbindung zu AWS trennen, Wiederherstellungs-Instances löschen aus. 2. Öffnen Sie die Elastic Disaster Recovery-Konsole in der DR-Region. Registrieren Sie Ihren neuen JD Edwards- EnterpriseOne Server als Quellserver in der DR-Region, indem Sie den AWS Replication Agent installieren. Die Daten werden mit einem neuen Replikationsserver synchronisiert, der im neuen Staging-Subnetz bereitgestellt wird. Hinweis: Wenn der neue JD Edwards- EnterpriseOne Server als Quellserver registriert ist, sehen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie möglicherweise zwei Quellserver in der Elastic-Disaster-Recovery-Konsole: einen Server, der aus der primären EC2-Instance erstellt wurde, und den neuen Server, der aus der Wiederherstellungs-Instance erstellt wurde. Wir empfehlen, die Server korrekt zu markieren, um Verwirrung zu vermeiden, und den neuen Server lieber zur Startvorlage hinzuzufügen. 3. Um die DR-Replikation von der primären Region neu zu starten, trennen Sie die gestartete Wiederherstellungs-Instance von der Elastic-Disaster-Recovery-Konsole in der DR-Region und registrieren Sie den Host als Quellserver in der primären Region. Weitere Informationen finden Sie unter Durchführen eines Failbacks in der Elastic-Disaster-Recovery-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Komponenten von JD Edwards EnterpriseOne .	1. Starten Sie die JD Edwards- EnterpriseOne Datenbank, indem Sie sich beim Datenbankserver anmelden. 2. Wenn die Datenbank ausgeführt wird, starten Sie die EnterpriseOne Logik und die Batchserver von JD Edwards. 3. Starten Sie WebLogic auf den Webservern und starten Sie eine JAS-Instance auf den JAS-Servern. 4. Starten Sie WebLogic auf dem Bereitstellungsserver und auf dem Server für die SM-Konsole. 5. Starten Sie SM Agent auf den Servern. 6. Vergewissern Sie sich, dass die Anmeldung bei JD Edwards ordnungsgemäß EnterpriseOne funktioniert. Sie müssen die Änderungen in Route 53 und Application Load Balancer integrieren, damit der EnterpriseOne Link JD Edwards funktioniert. Sie können diese Schritte automatisieren, indem Sie	JD Edwards EnterpriseOne Bol

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lambda, Step Functions und Systems Manager (Run Command) verwenden. Hinweis: Elastic Disaster Recovery führt eine Replikation der EBS-Quell-Volumes der EC2-Instance auf Blockebene durch, die das Betriebssystem und die Dateisysteme hosten. Freigegebene Dateisysteme, die mit Amazon EFS erstellt wurden, sind nicht Teil dieser Replikation. Sie können gemeinsam genutzte Dateisysteme mithilfe von AWS in die DR-Region replizieren DataSync, wie im ersten Epos erwähnt, und diese replizierten Dateisysteme dann im DR-System mounten.	

Fehlerbehebung

Problem	Lösung
Der Status der Quellserver-Datenreplikation lautet Verharrt und Replikationsverzögerungen. Wenn Sie Details überprüfen, zeigt der Datenreplikationsstatus Agent nicht angezeigt an.	Überprüfen Sie, ob der blockierte Quellserver ausgeführt wird. Hinweis: Wenn der Quellserver ausfällt, wird der Replikationsserver automatisch beendet. Weitere Informationen zu Verzögerungsproblemen finden Sie unter Probleme mit der

Problem	Lösung
	Replikationsverzögerung in der Elastic-Disaster-Recovery-Dokumentation.
Die Installation von AWS Replication Agent in der EC2-Quell-Instance schlägt nach dem Scannen der Datenträger in RHEL 8.2 fehl. `aws_replication_agent_installer.log` zeigt, dass Kernel-Header fehlen.	Führen Sie vor der Installation des AWS Replication Agent unter RHEL 8, CentOS 8 oder Oracle Linux 8 Folgendes aus: `sudo yum install elfutils-libelf-devel` Weitere Informationen finden Sie unter Linux-Installationsanforderungen in der Elastic Disaster Recovery-Dokumentation.
In der Elastic-Disaster-Recovery-Konsole sehen Sie den Quellserver als Bereit mit einer Verzögerung und den Datenreplikationsstatus als Veraltet. Je nachdem, wie lange der AWS Replication Agent nicht verfügbar ist, kann der Status auf eine hohe Verzögerung hinweisen, aber das Problem bleibt gleich.	Verwenden Sie einen Betriebssystembefehl, um zu bestätigen, dass der AWS Replication Agent in der EC2-Quell-Instance ausgeführt wird, oder um zu bestätigen, dass die Instance ausgeführt wird. Nachdem Sie Probleme behoben haben, startet Elastic Disaster Recovery das Scannen erneut. Warten Sie, bis alle Daten synchronisiert wurden und der Replikationsstatus Zustand ist, bevor Sie einen DR-Drossel starten.

Problem	Lösung
Anfängliche Replikation mit hoher Verzögerung. In der Elastic Disaster Recovery-Konsole können Sie sehen, dass der anfängliche Synchronisierungsstatus für einen Quellserver extrem langsam ist.	Überprüfen Sie die Probleme mit der Replikationsverzögerung, die im Abschnitt Probleme mit der Replikationsverzögerung der Elastic-Disaster-Recovery-Dokumentation dokumentiert sind. Der Replikationsserver kann die Last aufgrund intrinsischer Rechenvorgänge möglicherweise nicht bewältigen. Versuchen Sie in diesem Fall, den Instance-Typ zu aktualisieren, nachdem Sie sich an das AWS Technical Support Team wenden.

Zugehörige Ressourcen

- AWS Elastic Disaster Recovery-Benutzerhandbuch
- Erstellen eines skalierbaren Notfallwiederherstellungsplans mit AWS Elastic Disaster Recovery (AWS-Blogbeitrag)
- AWS Elastic Disaster Recovery – Eine technische Einführung (AWS Skill Builder-Schulung; erfordert Anmeldung)
- AWS Elastic Disaster Recovery-Schnellstartanleitung

Synchronisieren Sie Daten zwischen Amazon EFS-Dateisystemen in verschiedenen AWS-Regionen mithilfe von AWS DataSync

Erstellt von Sarat Chandra Pothula (AWS) und Aditya Ambati (AWS)

Code-Repository: aws-efs-crossregion-datasync	Umgebung: PoC oder Pilotprojekt	Technologien: Infrastruktur; Speicher und Backup
AWS-Dienste: AWS CDK; AWS DataSync; Amazon EFS		

Übersicht

Diese Lösung bietet ein robustes Framework für eine effiziente und sichere Datensynchronisierung zwischen Amazon Elastic File System (Amazon EFS) -Instances in verschiedenen AWS-Regionen. Dieser Ansatz ist skalierbar und ermöglicht eine kontrollierte, regionsübergreifende Datenreplikation. Diese Lösung kann Ihre Strategien zur Notfallwiederherstellung und Datenredundanz verbessern.

Durch die Verwendung des AWS Cloud Development Kit (AWS CDK) verwendet dieses Muster einen Infrastructure-as-Code-Ansatz (IaC) zur Bereitstellung der Lösungsressourcen. Die AWS CDK-Anwendung stellt die wesentlichen Ressourcen von AWS DataSync, Amazon EFS, Amazon Virtual Private Cloud (Amazon VPC) und Amazon Elastic Compute Cloud (Amazon EC2) bereit. Dieses IaC bietet einen wiederholbaren und versionskontrollierten Bereitstellungsprozess, der vollständig auf die bewährten AWS-Methoden abgestimmt ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2.9.11 oder höher, installiert und konfiguriert
- AWS CDK Version 2.114.1 oder höher, installiert und gebootet
- NodeJS Version 20.8.0 oder höher, installiert

Einschränkungen

- Die Lösung erbt Einschränkungen von DataSync Amazon EFS, wie z. B. Datenübertragungsraten, Größenbeschränkungen und regionale Verfügbarkeit. Weitere Informationen finden Sie unter DataSync AWS-Kontingente und Amazon EFS-Kontingente.
- Diese Lösung unterstützt nur Amazon EFS. DataSync unterstützt andere AWS-Services wie Amazon Simple Storage Service (Amazon S3) und Amazon FSx for Lustre. Diese Lösung erfordert jedoch Änderungen, um Daten mit diesen anderen Diensten zu synchronisieren.

Architektur

Diese Lösung stellt die folgenden AWS-CDK-Stacks bereit:

- Amazon VPC-Stack — Dieser Stack richtet Virtual Private Cloud (VPC) -Ressourcen ein, darunter Subnetze, ein Internet-Gateway und ein NAT-Gateway sowohl in der primären als auch in der sekundären AWS-Region.
- Amazon EFS-Stack — Dieser Stack stellt Amazon EFS-Dateisysteme in den primären und sekundären Regionen bereit und verbindet sie mit ihren jeweiligen VPCs.
- Amazon EC2 EC2-Stack — Dieser Stack startet EC2-Instances in der primären und sekundären Region. Diese Instances sind so konfiguriert, dass sie das Amazon EFS-Dateisystem mounten, wodurch sie auf den gemeinsam genutzten Speicher zugreifen können.
- DataSync Standort-Stack — Dieser Stack verwendet ein benutzerdefiniertes Konstrukt, das aufgerufen wird`DataSyncLocationConstruct`, um DataSync Standortressourcen in den primären und sekundären Regionen zu erstellen. Diese Ressourcen definieren Endpunkte für die Datensynchronisierung.
- DataSync Aufgabenstapel — Dieser Stapel verwendet ein benutzerdefiniertes Konstrukt`DataSyncTaskConstruct`, das aufgerufen wird, um eine DataSync Aufgabe in der primären Region zu erstellen. Diese Aufgabe ist so konfiguriert, dass Daten zwischen der primären und der sekundären Region mithilfe der DataSync Quell- und Zielorte synchronisiert werden.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.

- AWS DataSync ist ein Online-Datenübertragungs- und Erkennungsservice, mit dem Sie Dateien oder Objektdaten zu, von und zwischen AWS-Speicherservices verschieben können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Code-Repository

Der Code für dieses Muster ist im GitHub Amazon EFS Cross-Region DataSync Project Repository verfügbar.

Bewährte Methoden

Folgen Sie den unter Bewährte Methoden für die Verwendung des AWS-CDK bei der Erstellung von TypeScript IaC-Projekten beschriebenen bewährten Methoden.

Epen

Stellen Sie die AWS CDK-App bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Projekt-R epository.	Geben Sie den folgenden Befehl ein, um das Amazon EFS Cross-Region DataSync Project-Repository zu klonen. `git clone https://github.com/aws-samples/aws-efs-crossregion-datasync.git`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die NPM-Abhängigkeiten.	Geben Sie den folgenden Befehl ein. `npm ci`	AWS DevOps
Wählen Sie die primäre und die sekundäre Region aus.	Navigieren Sie im geklonten Repository zum `src/infra` Verzeichnis. Aktualisieren Sie in der `Launcher.ts` Datei die `SECONDARY_AWS_REGION` Werte `PRIMARY_AWS_REGION` und. Verwenden Sie die entsprechenden Regionalcodes. `const primaryRegion = { account: account, region: '<PRIMARY_AWS_REGION>' }; const secondaryRegion = { account: account, region: '<SECONDARY_AWS_REGION>' };`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrapping für die Umgebung.	Geben Sie den folgenden Befehl ein, um das AWS-Konto und die AWS-Region, die Sie verwenden möchten, zu booten. `cdk bootstrap <aws_account>/<aws_region>` Weitere Informationen finden Sie unter Bootstrapping in der AWS CDK-Dokumentation.	AWS DevOps
Listet die AWS CDK-Stacks auf.	Geben Sie den folgenden Befehl ein, um eine Liste der AWS CDK-Stacks in der App anzuzeigen. `cdk ls`	AWS DevOps
Synthetisieren Sie die AWS-CDK-Stacks.	Geben Sie den folgenden Befehl ein, um eine CloudFormation AWS-Vorlage für jeden in der AWS CDK-App definierten Stack zu erstellen. `cdk synth`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS CDK-App bereit.	Geben Sie den folgenden Befehl ein, um alle Stacks auf Ihrem AWS-Konto bereitzustellen, ohne dass eine manuelle Genehmigung für Änderungen erforderlich ist. `cdk deploy --all --require-approval never`	AWS DevOps

Validieren Sie die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der EC2-Instance in der primären Region an.	1. Melden Sie sich mit Session Manager, einer Funktion von AWS Systems Manager, bei der EC2-Instance in der primären Region an. Anweisungen finden Sie unter Stellen Sie mit AWS Systems Manager Session Manager eine Verbindung zu Ihrer Linux-Instance her. 2. Ändern Sie die Verzeichnisse in den Amazon EFS-Mountpfad. `cd /mnt/efs`	AWS DevOps
Erstellen Sie eine temporäre Datei.	Geben Sie den folgenden Befehl ein, um eine temporäre Datei im Amazon EFS-Mountpfad zu erstellen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`sudo dd if=/dev/zero \`
	`of=tmptst.dat \`
	`bs=1G \`
	`seek=5 \`
	`count=0`
	
	`ls -lrt tmptst.dat`	

Starten Sie die DataSync Aufgabe.	Geben Sie den folgenden Befehl ein, um die temporäre Datei von der primären Region in die sekundäre Region zu replizieren. Dabei `<ARN-task>` handelt es sich um den Amazon-Ressourcennamen (ARN) Ihrer DataSync Aufgabe.
	
	`aws datasync start-task-execution \`
	`--task-arn <ARN-task>`
	
	Der Befehl gibt den ARN der Aufgabenausführung im folgenden Format zurück.
	
	`arn:aws:datasync:<region>:<account-ID>:task/task-execution/<exec-ID>`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status der Datenübertragung.	Geben Sie den folgenden Befehl ein, um die DataSync Ausführungsaufgabe zu beschreiben. Dabei `<ARN-task-execution>` handelt es sich um den ARN der Aufgabenausführung. `aws datasync describe-task-execution \ --task-execution-arn <ARN-task-execution>` Die DataSync Aufgabe ist abgeschlossen`PrepareStatus` , wenn`TransferStatus` , und `VerifyStatus` alle den Wert haben`SUCCESS`.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der EC2-Instance in der sekundären Region an.	1. Melden Sie sich mit Session Manager, einer Funktion von AWS Systems Manager, bei der EC2-Instance in der sekundäre n Region an. Anweisungen finden Sie unter Stellen Sie mit AWS Systems Manager Session Manager eine Verbindung zu Ihrer Linux-Instance her. 2. Ändern Sie die Verzeichn isse in den Amazon EFS-Mountpfad. `cd /mnt/efs`	AWS DevOps
Validieren Sie die Replikation.	Geben Sie den folgenden Befehl ein, um zu überprüfe n, ob die temporäre Datei im Amazon EFS-Dateisystem vorhanden ist. `ls -lrt tmptst.dat`	AWS DevOps

Zugehörige Ressourcen

AWS-Dokumentation

- AWS-CDK-API-Referenz
- Konfiguration von DataSync AWS-Übertragungen mit Amazon EFS
- Behebung von Problemen mit DataSync AWS-Übertragungen

Andere AWS-Ressourcen

- DataSync Häufig gestellte Fragen zu AWS

Upgrade von SAP-Pacemaker-Clustern von ENSA1 auf ENSA2

Erstellt von Gergely Cserdi (AWS) und Balazs Sandor Skublics (AWS)

Umgebung: Produktion	Quelle: ENSA1-based Pacemaker-Cluster	Ziel: ENSA2-based Pacemaker-Cluster
R-Typ: Neuarchitektur	Workload: SAP	Technologien: Infrastruktur; Modernisierung
AWS-Services: Amazon EC2		

Übersicht

Dieses Muster erklärt die Schritte und Überlegungen zum Upgrade eines SAP-Pacemaker-Clusters, der auf dem eigenständigen Enqueue Server (ENSA1) basiert, auf ENSA2. Die Informationen in diesem Muster gelten sowohl für die Betriebssysteme SUSE Linux Enterprise Server (SLES) als auch Red Hat Enterprise Linux (RHEL).

Pacemaker-Cluster auf SAP NetWeaver 7.52 oder S/4HANA 1709 und früheren Versionen werden auf einer ENSA1-Architektur ausgeführt und sind speziell für ENSA1 konfiguriert. Wenn Sie Ihre SAP-Workloads auf Amazon Web Services (AWS) ausführen und zu ENSA2 wechseln möchten, stellen Sie möglicherweise fest, dass die SAP-, SUSE- und RHEL-Dokumentation keine umfassenden Informationen enthält. Dieses Muster beschreibt die technischen Schritte, die erforderlich sind, um SAP-Parameter und Pacemaker-Cluster neu zu konfigurieren, um von ENSA1 auf ENSA2 zu aktualisieren. Es enthält Beispiele für SUSE-Systeme, aber das Konzept ist für RHEL-Cluster dasselbe.

> Hinweise: ENSA1 und ENSA2 sind Konzepte, die sich nur auf SAP-Anwendungen beziehen. Daher gelten die Informationen in diesem Muster nicht für SAP HANA oder andere Arten von Clustern.
>
> Technisch gesehen kann ENSA2 mit oder ohne Enqueue Replicator 2 verwendet werden. Hochverfügbarkeit (HA) und Failover-Automatisierung (über eine Cluster-Lösung) erfordern jedoch Enqueue Replicator 2. Dieses Muster verwendet den Begriff ENSA2-Cluster, um auf Cluster mit eigenständigem Enqueue Server 2 und Enqueue Replicator 2 zu verweisen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein funktionierender ENSA1-based Cluster, der Pacemaker und Corosync auf SLES oder RHEL verwendet.
- Mindestens zwei Amazon Elastic Compute Cloud (Amazon EC2)-Instances, in denen die (ABAP) SAP Central Services (ASCS/SCS)- und Enqueue Replication Server (ERS)-Instances ausgeführt werden.
- Wissen über die Verwaltung von SAP-Anwendungen und -Clustern.
- Zugriff auf die Linux-Umgebung als Root-Benutzer.

Einschränkungen

- ENSA1-based Cluster unterstützen nur eine Architektur mit zwei Knoten.
- ENSA2-based Cluster können vor 7.52 nicht auf SAP- NetWeaver Versionen bereitgestellt werden.
- EC2-Instances in Clustern sollten sich in verschiedenen AWS Availability Zones befinden.

Produktversionen

- SAP- NetWeaver Version 7.52 oder höher
- Ab S/4HANA 2020 werden nur ENSA2-Cluster unterstützt
- Kernel 7.53 oder höher, der ENSA2 und Enqueue Replicator 2 unterstützt
- SLES für SAP-Anwendungen Version 12 oder höher
- RHEL für SAP mit Hochverfügbarkeit (HA) Version 7.9 oder höher

Architektur

Quelltechnologie-Stack

- SAP NetWeaver 7.52 mit SAP Kernel 7.53 oder höher
- SLES- oder RHEL-Betriebssystem

Zieltechnologie-Stack

- SAP NetWeaver 7.52 mit SAP Kernel 7.53 oder höher, einschließlich S/4HANA 2020 mit ABAP-Plattform
- SLES- oder RHEL-Betriebssystem

Zielarchitektur

Das folgende Diagramm zeigt eine HA-Konfiguration von ASCS/SCS- und ERS-Instances, die auf einem ENSA2-Cluster basieren.

Vergleich von ENSA1- und ENSA2-Clustern

SAP hat ENSA2 als Nachfolger von ENSA1 eingeführt. Ein ENSA1-based Cluster unterstützt eine Architektur mit zwei Knoten, bei der die ASCS/SCS-Instance ein Failover auf ERS durchführt, wenn ein Fehler auftritt. Diese Einschränkung ist darauf zurückzuführen, dass die ASCS/SCS-Instance nach dem Failover die Informationen der Sperrtabelle aus dem gemeinsam genutzten Speicher des ERS-Knotens zurückerhält. ENSA2-based Cluster mit Enqueue Replicator 2 beseitigen diese Einschränkung, da die ASCS/SCS-Instance die Sperrinformationen von der ERS-Instance über das Netzwerk erfassen kann. ENSA2-based Cluster können mehr als zwei Knoten haben, da die ASCS/SCS-Instance nicht mehr für ein Failover auf den ERS-Knoten erforderlich ist. (In einer ENSA2-Cluster-Umgebung mit zwei Knoten führt die ASCS/SCS-Instance jedoch weiterhin ein Failover auf den ERS-Knoten durch, da es keine anderen Knoten im Cluster gibt, auf die ein Failover durchgeführt werden kann.) ENSA2 wird ab SAP Kernel 7.50 mit einigen Einschränkungen unterstützt. Für die HA-Einrichtung, die Enqueue Replicator 2 unterstützt, beträgt die Mindestanforderung NetWeaver 7,52 (siehe SAP-OSS-Hinweis 2630416). S/4HANA 1809 wird standardmäßig mit der empfohlenen ENSA2-Architektur geliefert, während S/4HANA ab Version 2020 nur ENSA2 unterstützt.

Automatisierung und Skalierung

Der HA-Cluster in der Zielarchitektur sorgt dafür, dass ASCS automatisch ein Failover auf andere Knoten durchführt.

Szenarien für den Wechsel zu ENSA2-based Clustern

Es gibt zwei Hauptszenarien für das Upgrade auf ENSA2-based Cluster:

- Szenario 1: Sie entscheiden sich für ein Upgrade auf ENSA2 ohne ein zugehöriges SAP-Upgrade oder eine S/4HANA-Konvertierung, vorausgesetzt, dass Ihre SAP-Version und Kernel-Version ENSA2 unterstützen.

- Szenario 2: Sie wechseln im Rahmen eines Upgrades oder einer Konvertierung (z. B. zu S/4HANA 1809 oder höher) zu ENSA2, indem Sie SUM verwenden.

Der Abschnitt „PiCs“ behandelt die Schritte für diese beiden Szenarien. Im ersten Szenario müssen Sie SAP-bezogene Parameter manuell einrichten, bevor Sie die Clusterkonfiguration für ENSA2 ändern. Im zweiten Szenario werden die Binärdateien und SAP-bezogenen Parameter von SUM bereitgestellt, und Ihre einzige verbleibende Aufgabe besteht darin, die Clusterkonfiguration für HA zu aktualisieren. Wir empfehlen weiterhin, SAP-Parameter zu validieren, nachdem Sie SUM verwendet haben. In den meisten Fällen ist die S/4HANA-Konvertierung der Hauptgrund für ein Cluster-Upgrade.

Tools

- Für Betriebssystempaketmanager empfehlen wir die Tools Zypper (für SLES) oder YUM (für RHEL).
- Für die Clusterverwaltung empfehlen wir crm (für SLES)- oder pcs (für RHEL)-Shells.
- SAP-Instance-Management-Tools wie SAPControl .
- (Optional) SUM-Tool für S/4HANA-Konvertierungs-Upgrade.

Bewährte Methoden

- Bewährte Methoden für die Verwendung von SAP-Workloads in AWS finden Sie unter SAP Lens für das AWS Well-Architected Framework.
- Berücksichtigen Sie die Anzahl der Cluster-Knoten (Odd oder Even) in Ihrer ENSA2-Architektur mit mehreren Knoten.
- Richten Sie den ENSA2-Cluster für SLES 15 im Einklang mit dem SAP-S/4-HA-CLU-1.0-Zertifizierungsstandard ein.
- Speichern oder sichern Sie immer Ihren vorhandenen Cluster- und Anwendungsstatus, bevor Sie auf ENSA2 aktualisieren.

Polen

Manuelles Konfigurieren von SAP-Parametern für ENSA2 (nur Szenario 1)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Parameter im Standardprofil.	Wenn Sie ein Upgrade auf ENSA2 durchführen möchten, während Sie dieselbe SAP-Version verwenden , oder wenn Ihre Zielversi on standardmäßig ENSA1 verwendet, legen Sie die Parameter im Standardprofil (DEFAULT.PFL-Datei) auf die folgenden Werte fest.
	`enq/enable=TRUE`
	`enq/serverhost=sapas csvirt`
	`enq/serverinst=10`
	`(instance number of ASCS/SCS instance)`
	`enque/process_loc ation=REMOTESA`
	`enq/replicatorhost=sa persvirt`
	`enq/replicatorinst=11`
	`(instance number of ERS instance)`
	wobei `sapascsvirt` der virtuelle Hostname für die ASCS-Instances und der virtuelle Hostname für die ERS-Instances `sapersvirt` ist. Sie können diese an Ihre Zielumgebung anpassen.
		SAP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Um diese Upgrade-Option verwenden zu können, müssen Ihre SAP-Version und Kernel-Version ENSA2 und Enqueue Replicator 2 unterstützen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das ASCS/SCS-Instance-Profil.	Wenn Sie ein Upgrade auf ENSA2 durchführen möchten, während Sie dieselbe SAP-Version beibehalten, oder wenn Ihre Zielversion standardmäßig ENSA1 ist, legen Sie die folgenden Parameter im ASCS/SCS-Instance-Profil fest. Der Abschnitt des Profils, in dem ENSA1 definiert ist, sieht etwa wie folgt aus. `#------------------ ------------------ ------------------ --------- Start SAP enqueue server #------------------- ------------------ ------------------ ------- _EN = en.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_04 = local rm - f $(_EN) Execute_05 = local ln - s -f $(DIR_EXECUTABLE)/ enserver$(FT_EXE) $(_EN) Start_Program_01 = local $(_EN) pf=$(_PF)` So konfigurieren Sie diesen Abschnitt für ENSA2 neu:	SAP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Ändern Sie das `_EN` Programmpräfix auf `_ENQ` der Grundlage der neuesten Informationen von SAP in (OSS-Hinweis 2501860; erfordert ein SAP ONE Support Launchpad-Benutzerkonto).
	2. Ändern Sie die Binärdatei für den Enqueue-Server von `enserver` in `enq_server` .
	3. Legen Sie den neuen Parameter `enq/server/replication/enable` auf fest`TRUE`.
	4. Stellen Sie sicher, dass `Autostart = 0`.
	
	Dieser Profilabschnitt würde nach Ihren Änderungen etwa wie folgt aussehen.
	
	`#----------`
	`----------`
	`----------`
	`---------`
	`Start SAP enqueue server`
	`#----------`
	`----------`
	`----------`
	`-------`
	`_ENQ = enq.sap$(`
	`SAPSYSTEMNAME)$(IN`
	`STANCE_NAME)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Execute_04 = local rm -f $(_ENQ)`
	`Execute_05 = local ln -s -f $(DIR_EXECUTABLE)/enq_server$(FT_EXE) $(_ENQ)`
	`Start_Program_01 = local $(_ENQ) pf=$(_PF)`
	`...`
	`enq/server/replication/enable = TRUE`
	`Autostart = 0`
	
	Wichtig: _ENQ darf die Neustartoption nicht aktiviert haben. Wenn für festgelegt `RestartProgram_01` ist_ENQ, ändern Sie es in `StartProgram_01` . Dadurch wird verhindert, dass SAP den Service neu startet oder von Clustern verwaltete Ressourcen stört.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das ERS-Profil.	Wenn Sie ein Upgrade auf ENSA2 durchführen möchten, während Sie dieselbe SAP-Version verwenden , oder wenn Ihre Zielversi on standardmäßig ENSA1 verwendet, legen Sie die folgenden Parameter im ERS-Instance-Profil fest. Suchen Sie den Abschnitt, in dem der Enqueue-Replikator definiert ist. Es wird in etwa wie folgt aussehen. `#----------------- ------------------ ------------------- Start enqueue replicati on server #------------------- ------------------ ----------------- _ER = er.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_03 = local rm - f $(_ER) Execute_04 = local ln - s -f $(DIR_EXECUTABLE)/ enrepserver$(FT_EXE) $(_ER) Start_Program_00 = local $(_ER) pf=$(_PF) NR=$(SCSID)`	SAP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	So konfigurieren Sie diesen Abschnitt für Enqueue Replicator 2 neu:
	1. Ändern Sie das `_ER` Programmpräfix auf der `_ENQR` Grundlage der neuesten Hinweise von SAP in (OSS-Hinweis 2501860; erfordert ein SAP ONE Support Launchpad-Benutzerkonto).
	2. Ändern Sie die Binärdatei für den Enqueue-Replikator in `enq_replicator` anstelle von `enrepserver` .
	3. Stellen Sie sicher, dass `Autostart = 0`.
	
	Dieser Profilabschnitt sollte nach Ihren Änderungen etwa wie folgt aussehen.
	`#----------`
	`----------`
	`----------`
	`Start enqueue replicati`
	`on server`
	`#----------`
	`----------`
	`----------`
	`_ENQR = enqr.sap$`
	`(SAPSYSTEMNAME)$(I`
	`NSTANCE_NAME)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Execute_01 = local rm -f $(_ENQR)`
	`Execute_02 = local ln -s -f $(DIR_EXECUTABLE)/enq_replicator$(FT_EXE) $(_ENQR)`
	`Start_Program_00 = local $(_ENQR) pf=$(_PF) NR=$(SCSID)`
	`…`
	`Autostart = 0`
	
	Wichtig: `_ENQR` darf die Neustartoption nicht aktiviert haben. Wenn für festgeleg t `RestartProgram_01` ist`_ENQR`, ändern Sie es in `StartProgram_01` . Dadurch wird verhindert, dass SAP den Service neu startet oder von Clustern verwaltete Services stört.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie SAP Start Services neu.	Nachdem Sie die zuvor in dieser Übersicht beschrieb enen Profile geändert haben, starten Sie SAP Start Services sowohl für ASCS/SCS als auch für ERS neu.
	`sapcontrol -nr 10 -function RestartService SCT`
	`sapcontrol -nr 11 -function RestartService SCT`
	wobei sich auf die SAP-System-ID `SCT` bezieht und vorausgesetzt, dass 10 und 11 die Instance-Nummern für ASCS/SCS- bzw. ERS-Instances sind.
		SAP

Den Cluster für ENSA2 neu konfigurieren (erforderlich für beide Szenarien)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie Versionsnummern in SAP-Resourcenagenten.	Wenn Sie SUM verwenden , um SAP auf S/4HANA 1809 oder höher zu aktualisieren, übernimmt SUM die Parameteränderungen in den SAP-Profilen. Nur der Cluster erfordert eine manuelle Anpassung. Wir empfehlen jedoch, die Parametereinstellu	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ngen zu überprüfen, bevor Sie Änderungen am Cluster vornehmen. Hinweis: In den Beispielen in diesem Epos wird davon ausgegangen, dass Sie das SUSE-Betriebssystem verwenden. Wenn Sie RHEL verwenden, müssen Sie Tools wie YUM und die pcs-Shell anstelle von Zypper und crm verwenden. Überprüfen Sie beide Knoten in der Architektur, um sicherzustellen, dass das `resource-agents` Paket der von SAP empfohlenen Mindestversion entspricht. Überprüfen Sie für SLES den SAP-OSS-Hinweis 2641019. Überprüfen Sie für RHEL den SAP OSS-Hinweis 2641322. (SAP-Hinweise erfordern ein SAP ONE Support Launchpad -Benutzerkonto.) `sapers:sctadm 23>  zypper search -s -i  resource-agents Loading repository  data... Reading installed  packages...`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`S | Name | Type | Version | Arch | Repository --+------------ ----+---------+--- ----------+-- ------+---------- ---------- i | resource-agents | package | 4.8.0+git 30.d0077df0-150300 .8.28.1 | x86_64 | SLE-Product-HA15-SP3-Updates` Aktualisieren Sie die `resource-agents` Version bei Bedarf.	
Sichern Sie die Cluster-K onfiguration.	Sichern Sie die CRM-Clust erkonfiguration wie folgt. `crm configure show > /tmp/cluster_confi g_backup.txt`	AWS-Systemadministrator
Legen Sie den Wartungsm odus fest.	Setzen Sie den Cluster auf den Wartungsmodus. `crm configure property maintenance-mode=" true"`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Cluster-K onfiguration.	Überprüfen Sie die aktuelle Cluster-Konfiguration.
	`crm configure show`
	Hier ist ein Auszug aus der vollständigen Ausgabe:
	`node 1: sapascs`
	`node 2: sapers`
	`...`
	`primitive rsc_sap_S`
	`CT_ASCS10 SAPInstance`
	`\`
	`operations $id=rsc_s`
	`ap_SCT_ASCS10-oper`
	`ations \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
	`params InstanceN`
	`ame=SCT_ASCS10_sap`
	`ascsvirt START_PRO`
	`FILE="/sapmnt/SCT/`
	`profile/SCT_ASCS10`
	`_sapascsvirt" \`
	`AUTOMATIC_RECOVER=`
	`false \`
	`meta resource-stickines`
	`s=5000 failure-t`
	`imeout=60 migration-`
	`threshold=1 priority=`
	`10`
	`primitive rsc_sap_S`
	`CT_ERS11 SAPInstance \`
	`operations $id=rsc_s`
	`ap_SCT_ERS11-opera`
	`tions \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`params InstanceName=SCT_ERS11_sapersvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ERS11_sapersvirt" \ AUTOMATIC_RECOVER=false IS_ERS=true \ meta priority=1000 ... colocation col_sap_SCT_no_both -5000: grp_SCT_ERS11 grp_SCT_ASCS10 location loc_sap_SCT_failover_to_ers rsc_sap_SCT_ASCS10 \ rule 2000: runs_ers_SCT eq 1 order ord_sap_SCT_first_start_asc s Optional: rsc_sap_SCT_ASCS10:start rsc_sap_SCT_ERS11: stop symmetrical=false ...`  wobei `sapascsvirt` sich auf den virtuellen Hostnamen für die ASCS-Instances`sapersvirt` , auf den virtuellen Hostnamen für die ERS-Instances und auf die SAP-System-ID SCT bezieht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Failover-Colocation-Einschränkung.	Im vorherigen Beispiel `loc_sap_SCT_failover_to_ers` gibt die Standortbeschränkung an, dass das ENSA1-Feature von ASCS beim Failover immer der ERS-Instance folgen soll. Mit ENSA2 sollte ASCS in der Lage sein, ein Failover frei auf alle teilnehmenden Knoten durchzuführen, sodass Sie diese Einschränkung entfernen können. `crm configure delete loc_sap_SCT_failover_to_ers`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Passen Sie die Primitive an.	Sie müssen auch geringfügige Änderungen an den ASCS- und ERS SAPInstance-Primitiven vornehmen.
	
	Hier ist ein Beispiel für ein ASCS-SAPInstance-Primitive, das für ENSA1 konfiguriert ist.
	
	`primitive rsc_sap_SCT_ASCS10 SAPInstance \`
	`operations $id=rsc_sap_SCT_ASCS10-operations \`
	`op monitor interval=120 timeout=60 on-fail=restart \`
	`params InstanceName=SCT_ASCS10_sapascsvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ASCS10_sapascsvirt" \`
	`AUTOMATIC_RECOVER=false \`
	`meta resource-stickiness=5000 failure-timeout=60 migration-threshold=1 priority=10`
	
	Um auf ENSA2 zu aktualisieren, ändern Sie diese Konfiguration wie folgt.
	
	`primitive rsc_sap_SCT_ASCS10 SAPInstance \`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=3000 Dies ist ein Beispiel für ein ERS SAPInstance-Primitive, das für ENSA1 konfiguriert ist. primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \ meta priority=1000	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Um auf ENSA2 zu aktualisieren, ändern Sie diese Konfiguration wie folgt.
	
	`primitive rsc_sap_SCT_ERS11 SAPInstance \ operations $id=rsc_sap_SCT_ERS11-operations \ op monitor interval=120 timeout=60 on-fail=restart \ params InstanceName=SCT_ERS11_sapersvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ERS11_sapersvirt" \ AUTOMATIC_RECOVER=false IS_ERS=true`
	
	Sie können primitive Werte auf verschiedene Arten ändern. Sie können sie beispielsweise in einem Editor wie vi ändern, wie im folgenden Beispiel.
	
	`crm configure edit rsc_sap_SCT_ERS11`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie den Wartungsmodus.	Deaktivieren Sie den Wartungsmodus auf dem Cluster. `crm configure property maintenance-mode="false"` Wenn der Cluster nicht im Wartungsmodus ist, versucht er, die ASCS- und ERS-Instances mit den neuen ENSA2-Einstellungen online zu bringen.	AWS-Systemadministrator

(Optional) Hinzufügen von Cluster-Knoten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Informieren Sie sich über bewährte Methoden.	Bevor Sie weitere Knoten hinzufügen, stellen Sie sicher, dass Sie bewährte Methoden wie die Verwendung einer ungerade oder geraden Anzahl von Knoten verstehen.	AWS-Systemadministrator
Knoten hinzufügen.	Das Hinzufügen weiterer Knoten umfasst eine Reihe von Aufgaben, z. B. das Aktualisieren des Betriebssystems, das Installieren von Softwarepaketen, die den vorhandenen Knoten entsprechen, und das Bereitstellen von Mounts.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können die Option Additional Host vorbereiten in SAP Software Provisioning Manager (SWPM) verwenden , um eine SAP-spezifische Baseline des Hosts zu erstellen. Weitere Informati onen finden Sie in den SAP-Leitfäden, die im nächsten Abschnitt aufgeführt sind.	

Zugehörige Ressourcen

SAP- und SUSE-Referenzen

Für den Zugriff auf SAP Notes benötigen Sie ein SAP ONE Support Launchpad-Benutzerkonto. Weitere Informationen finden Sie auf der SAP-Supportwebsite.

- SAP Note 2501860 Dokumentation für SAP NetWeaver Application Server für ABAP 7.52
- SAP Note 2641019 Installation von ENSA2 und Aktualisierung von ENSA1 auf ENSA2 in der SUSE HA-Umgebung
- SAP Note 2641322 Installation von ENSA2 und Aktualisierung von ENSA1 auf ENSA2 bei Verwendung der Red Hat HA-Lösungen für SAP
- SAP Note 2711036 Verwendung des eigenständigen Enqueue Server 2 in einer HA-Umgebung
- Eigenständiger Enqueue Server 2 (SAP-Dokumentation)
- SAP S/4 HANA Enqueue Replication 2 – Cluster mit hoher Verfügbarkeit – Einrichtungshandbuch (SUSE-Dokumentation)

AWS-Referenzen

- SAP HANA in AWS: Konfigurationshandbuch für Hochverfügbarkeit für SLES und RHEL
- SAP Lens – AWS Well-Architected Framework

Verwenden konsistenter Availability Zones in VPCs über verschiedene AWS-Konten hinweg

Erstellt von A Spicer (AWS)

Code-Repository: Zuordnung von Availability Zones mit mehreren Konten	Umgebung: Produktion	Technologien: Infrastruktur
AWS-Services: AWS CloudFormation; Amazon VPC; AWS Lambda		

Übersicht

In der Amazon Web Services (AWS) Cloud hat eine Availability Zone einen Namen, der zwischen Ihren AWS-Konten variieren kann, und eine Availability Zone-ID (AZ-ID), die ihren Standort identifiziert. Wenn Sie AWS CloudFormation zum Erstellen von Virtual Private Clouds (VPCs) verwenden, müssen Sie beim Erstellen der Subnetze den Namen oder die ID der Availability Zone angeben. Wenn Sie VPCs in mehreren Konten erstellen, wird der Name der Availability Zone zufällig ermittelt, was bedeutet, dass Subnetze in jedem Konto unterschiedliche Availability Zones verwenden.

Um dieselbe Availability Zone für alle Konten zu verwenden, müssen Sie den Namen der Availability Zone in jedem Konto derselben AZ-ID zuordnen. Das folgende Diagramm zeigt beispielsweise, dass die `use1-az6` AZ-ID `us-east-1a` in AWS-Konto A und `us-east-1c` in AWS-Konto Z benannt ist.

Dieses Muster trägt dazu bei, die Zonenkonsistenz sicherzustellen, indem es eine kontoübergreifende, skalierbare Lösung für die Verwendung derselben Availability Zones in Ihren Subnetzen bietet. Die Zonenkonsistenz stellt sicher, dass Ihr kontoübergreifender Netzwerkverkehr Netzwerkpfade in der Availability Zone vermeidet, wodurch die Datenübertragungskosten gesenkt und die Netzwerklatenz zwischen Ihren Workloads verringert werden.

Dieses Muster ist ein alternativer Ansatz für die AWS- CloudFormation AvailabilityZoneId Eigenschaft .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Mindestens zwei aktive AWS-Konten in derselben AWS-Region.
- Prüfen Sie, wie viele Availability Zones zur Unterstützung Ihrer VPC-Anforderungen in der Region benötigt werden.
- Identifizieren und notieren Sie die AZ-ID für jede Availability Zone, die Sie unterstützen müssen. Weitere Informationen dazu finden Sie unter Availability Zone IDs für Ihre AWS-Ressourcen in der AWS Resource Access Manager-Dokumentation.
- Eine geordnete, durch Komma getrennte Liste Ihrer AZ-IDs. Die erste Availability Zone in Ihrer Liste wird beispielsweise als `az1`, die zweite Availability Zone als zugewiesen und diese Zuordnungsstruktur wird fortgesetzt`az2`, bis Ihre durch Komma getrennte Liste vollständig zugeordnet ist. Es gibt keine maximale Anzahl von AZ-IDs, die zugeordnet werden können.
- Die `az-mapping.yaml` Datei aus dem GitHub Zuordnungs-Repository für mehrere Konten und Availability Zones, die auf Ihren lokalen Computer kopiert wurde

Architektur

Das folgende Diagramm zeigt die Architektur, die in einem Konto bereitgestellt wird und AWS Systems Manager Parameter Store-Werte erstellt. Diese Parameter Store-Werte werden verbraucht, wenn Sie eine VPC im Konto erstellen.

Das Diagramm zeigt den folgenden Workflow:

1. Die Lösung dieses Musters wird für alle Konten bereitgestellt, die zonale Konsistenz für eine VPC erfordern.
2. Die Lösung erstellt Parameter Store-Werte für jede AZ-ID und speichert den neuen Availability Zone-Namen.
3. Die AWS- CloudFormation Vorlage verwendet den Namen der Availability Zone, der in jedem Parameter Store-Wert gespeichert ist, und dies gewährleistet die zonale Konsistenz.

Das folgende Diagramm zeigt den Workflow zum Erstellen einer VPC mit der Lösung dieses Musters.

Das Diagramm zeigt den folgenden Workflow:

1. Senden Sie eine Vorlage zum Erstellen einer VPC an AWS CloudFormation.
2. AWS CloudFormation löst die Parameter Store-Werte für jede Availability Zone auf und gibt den Namen der Availability Zone für jede AZ-ID zurück.
3. Eine VPC wird mit den richtigen AZ-IDs erstellt, die für die Zonenkonsistenz erforderlich sind.

Nachdem Sie die Lösung dieses Musters bereitgestellt haben, können Sie Subnetze erstellen, die auf die Parameter Store-Werte verweisen. Wenn Sie AWS verwenden CloudFormation, können Sie auf die Werte der Availability Zone-Zuweisungsparameter aus dem folgenden YAML-formatierten Beispielcode verweisen:

```
Resources:
    PrivateSubnet1AZ1:
        Type: AWS::EC2::Subnet
        Properties:
            VpcId: !Ref VPC
            CidrBlock: !Ref PrivateSubnetAZ1CIDR
            AvailabilityZone:
                !Join
                    - ''
                    - - '{{resolve:ssm:/az-mapping/az1:1}}'
```

Dieser Beispielcode ist in der `-vpc-example.yaml` Datei aus dem GitHub Zuordnungs-Repository für mehrere Konten enthalten. Es zeigt Ihnen, wie Sie eine VPC und Subnetze erstellen, die den Parameter Store-Werten für die Zonenkonsistenz entsprechen.

Technologie-Stack

- AWS CloudFormation
- AWS Lambda
- AWS Systems Manager Parameter Store

Automatisierung und Skalierung

Sie können dieses Muster für alle Ihre AWS-Konten bereitstellen, indem Sie AWS CloudFormation StackSets oder die Lösung Customizations for AWS Control Tower verwenden. Weitere Informationen finden Sie unter Arbeiten mit AWS CloudFormation StackSets in der AWS

Cloudformation-Dokumentation und unter Anpassungen für AWS Control Tower in der AWS Solutions Library.

Nachdem Sie die AWS- CloudFormation Vorlage bereitgestellt haben, können Sie sie aktualisieren, um die Parameter Store-Werte zu verwenden und Ihre VPCs in Pipelines oder entsprechend Ihren Anforderungen bereitzustellen.

Tools

AWS-Services

- AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.
- AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- AWS Systems Manager Parameter Store ist eine Funktion von AWS Systems Manager . Es bietet eine sichere, hierarchische Speicherung für die Verwaltung von Konfigurationsdaten und Secrets.

Code

Der Code für dieses Muster wird im GitHub Zuordnungs-Repository für Availability Zones mit mehreren Konten bereitgestellt.

Sekunden

Bereitstellen der az-mapping.yaml-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie die erforderlichen Availability Zones für die Region.	1. Bestimmen Sie die AZ-IDs, die in Ihrer Region konsistent verwendet werden müssen. 2. Notieren Sie diese AZ-IDs in einer durch Komma getrennten Liste und in der Reihenfolge, in der sie angewendet werden sollen. Beispielsweise wird die erste Availability Zone in Ihrer Liste als `az1` und die zweite als zugeordnet`az2`. Es gibt keine maximale Anzahl von AZ-IDs, die zugeordnet werden können.	Cloud-Architekt
Stellen Sie die Datei az-mapping.yaml bereit.	Verwenden Sie die `az-mapping.yaml` Datei , um einen AWS- CloudFormation Stack in allen erforderlichen AWS-Konten zu erstellen. Verwenden Sie im `AZIds` Parameter die kommagetrennte Liste, die Sie zuvor erstellt haben. Wir empfehlen Ihnen, AWS CloudFormation StackSets oder die Customizations for	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Control Tower-Lösung zu verwenden.	

Bereitstellen der VPCs in Ihren Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die AWS-CloudFormation Vorlagen an.	Wenn Sie die Subnetze mit AWS erstellen CloudForm ation, passen Sie die Vorlagen so an, dass sie die zuvor erstellten Parameter Store-Werte verwenden. Eine Beispielvorlage finden Sie in der `-vpc-examp le.yaml` Datei im GitHub Zuordnungs-Repository für Availability Zones mit mehreren Konten.	Cloud-Architekt
Stellen Sie die VPCs bereit.	Stellen Sie die benutzerd efinierten AWS- CloudForm ation Vorlagen in Ihren Konten bereit. Jede VPC in der Region verfügt dann über zonale Konsistenz in den Availability Zones, die für die Subnetze verwendet werden	Cloud-Architekt

Zugehörige Ressourcen

- Availability Zone-IDs für Ihre AWS-Ressourcen (Dokumentation zu AWS Resource Access Manager)

- AWS::EC2::Subnet (AWS- CloudFormation Dokumentation)

Lokales Validieren des Codes Account Factory für Terraform (AFT)

Erstellt von Alexandru Pop (AWS) und Mi Bol Gorniak (AWS)

Umgebung: Produktion	Technologien: Infrastruktur DevOps; Modernisierung; Softwareentwicklung und -tests	Workload: Open-Source
AWS-Services: AWS Control Tower		

Übersicht

Dieses Muster zeigt, wie HashiCorp Terraform-Code, der von AWS Control Tower Account Factory for Terraform (AFT) verwaltet wird, lokal getestet wird. Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit dem Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können. AFT richtet eine Terraform-Pipeline ein, mit der Sie mehrere AWS-Konten in AWS Control Tower bereitstellen und anpassen können.

Während der Codeentwicklung kann es hilfreich sein, Ihre Terraform-Infrastruktur als Code (IaC) lokal außerhalb der AFT-Pipeline zu testen. Dieses Muster zeigt, wie Sie Folgendes tun:

- Rufen Sie eine lokale Kopie des Terraform-Codes ab, der in den AWS CodeCommit -Repositorys in Ihrem AFT-Verwaltungskonto gespeichert ist.
- Simulieren Sie die AFT-Pipeline lokal mithilfe des abgerufenen Codes.

Dieses Verfahren kann auch verwendet werden, um Terraform-Befehle auszuführen, die nicht Teil der normalen AFT-Pipeline sind. Sie können diese Methode beispielsweise verwenden, um Befehle wie `terraform validate`, `terraform planterraform destroy`, und auszuführen`terraform import`.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive AWS-Umgebung mit mehreren Konten, die AWS Control Tower verwendet

- Eine vollständig bereitgestellte AFT-Umgebung
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- AWS CLI-Anmeldeinformationshilfe für Code Commit , installiert und konfiguriert
- Python 3.x
- Git , auf Ihrem lokalen Computer installiert und konfiguriert
- git-remote-commit Dienstprogramm, installiert und konfiguriert
- Terraform , installiert und konfiguriert (die lokale Terraform-Paketversion muss mit der Version übereinstimmen, die in der AFT-Bereitstellung verwendet wird)

Einschränkungen

- Dieses Muster deckt nicht die Bereitstellungsschritte ab, die für AWS Control Tower, AFT oder bestimmte Terraform-Module erforderlich sind.
- Die Ausgabe, die während dieses Verfahrens lokal generiert wird, wird nicht in den AFT-Pipeline-Laufzeitprotokollen gespeichert.

Architektur

Zieltechnologie-Stack

- AFT-Infrastruktur, die innerhalb einer AWS Control Tower-Bereitstellung bereitgestellt wird
- Terraform
- Git
- AWS CLI Version 2

Automatisierung und Skalierung

Dieses Muster zeigt, wie Terraform-Code für globale AFT-Kontoanpassungen in einem einzigen AFT-verwalteten AWS-Konto lokal aufgerufen wird. Nachdem Ihr Terraform-Code validiert wurde, können Sie ihn auf die verbleibenden Konten in Ihrer Umgebung mit mehreren Konten anwenden. Weitere Informationen finden Sie unter Erneutes Aufrufen von Anpassungen in der AWS Control Tower-Dokumentation.

Sie können auch einen ähnlichen Prozess verwenden, um AFT-Kontoanpassungen in einem lokalen Terminal auszuführen. Um Terraform-Code lokal aus AFT-Kontoanpassungen aufzurufen, klonen Sie

das aft-account-customizations Repository anstelle des aft-global-account-customizationsRepositorys aus CodeCommit in Ihrem AFT-Verwaltungskonto.

Tools

AWS-Services

- AWS Control Tower unterstützt Sie bei der Einrichtung und Verwaltung einer AWS-Umgebung mit mehreren Konten gemäß den bewährten Methoden.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere -Services

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit dem Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.
- Git ist ein verteiltes Open-Source-Versionsverwaltungssystem.

Code

Im Folgenden finden Sie ein Beispiel für ein Bash-Skript, das verwendet werden kann, um Terraform-Code lokal auszuführen, der von AFT verwaltet wird. Um das Skript zu verwenden, folgen Sie den Anweisungen im Abschnitt „Epics“ dieses Musters.

```
#! /bin/bash
# Version: 1.1 2022-06-24 Unsetting AWS_PROFILE since, when set, it interferes with
 script operation
#          1.0 2022-02-02 Initial Version
#
# Purpose: For use with AFT: This script runs the local copy of TF code as if it were
 running within AFT pipeline.
#        * Facilitates testing of what the AFT pipline will do
#           * Provides the ability to run terraform with custom arguments (like 'plan'
 or 'move') which are currently not supported within the pipeline.
#
# © 2021 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.
# This AWS Content is provided subject to the terms of the AWS Customer Agreement
# available at http://aws.amazon.com/agreement or other written agreement between
```

```
# Customer and either Amazon Web Services, Inc. or Amazon Web Services EMEA SARL or
 both.
#
# Note: Arguments to this script are passed directly to 'terraform' without parsing nor
 validation by this script.
#
# Prerequisites:
#    1. local copy of ct GIT repositories
#    2. local backend.tf and aft-providers.tf filled with data for the target account
 on which terraform is to be run
#       Hint: The contents of above files can be obtain from the logs of a previous
 execution of the AFT pipeline for the target account.
#    3. 'terraform' binary is available in local PATH
#    4. Recommended: .gitignore file containing 'backend.tf', 'aft_providers.tf' so the
 local copy of these files are not pushed back to git

readonly credentials=$(aws sts assume-role \
    --role-arn arn:aws:iam::$(aws sts get-caller-identity --query "Account" --output
 text ):role/AWSAFTAdmin \
    --role-session-name AWSAFT-Session \
    --query Credentials )

unset AWS_PROFILE
export AWS_ACCESS_KEY_ID=$(echo $credentials | jq -r '.AccessKeyId')
export AWS_SECRET_ACCESS_KEY=$(echo $credentials | jq -r '.SecretAccessKey')
export AWS_SESSION_TOKEN=$(echo $credentials | jq -r '.SessionToken')
terraform "$@"
```

Polen

Speichern des Beispielcodes als lokale Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie den Beispielcode als lokale Datei.	1. Kopieren Sie das Beispiel-Bash-Skript, das sich im Abschnitt Code dieses Musters befindet, und fügen Sie es in einen Code-Editor ein.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Benennen Sie die Datei `ct_terraform.sh` . Speichern Sie die Datei dann lokal in einem dedizierten Ordner, z. B. `~/scripts` oder `~/bin`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Machen Sie den Beispielcode ausführbar.	Öffnen Sie ein Terminalf enster und authentifizieren Sie sich bei Ihrem AWS AFT-Verwaltungskonto, indem Sie einen der folgenden Schritte ausführen: • Verwenden Sie ein vorhandenes AWS CLI-Profil, das mit den Berechtig ungen konfiguriert ist, die für den Zugriff auf das AFT-Verwaltungskonto erforderl ich sind. Um das Profil zu verwenden, können Sie den folgenden Befehl ausführen: `export AWS_PROFILE=<aft account profile name>` • Wenn Ihre Organisation SSO für den Zugriff auf AWS verwendet, geben Sie die Anmeldeinformationen für Ihr AFT-Verwaltungskon to auf der SSO-Seite Ihrer Organisation ein. Hinweis: Ihre Organisation verfügt möglicherweise auch über ein benutzerdefiniertes Tool, mit dem Sie Authentif izierungsanmeldeinformation	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en für Ihre AWS-Umgebung bereitstellen können.	

Überprüfen Sie den Zugriff auf das AFT-Verwaltungskonto in der richtigen AWS-Region.	Wichtig: Stellen Sie sicher, dass Sie dieselbe Terminals itzung verwenden, mit der Sie sich bei Ihrem AFT-Verwa ltungskonto authentifiziert haben.
	1. Navigieren Sie zur AWS-Region Ihrer AFT-Berei tstellung, indem Sie den folgenden Befehl ausführen:
	`export AWS_REGIO N=<aft_region>`
	2. Stellen Sie sicher, dass Sie sich im richtigen Konto befinden, indem Sie wie folgt vorgehen:
	• Führen Sie den folgenden Befehl aus:
	`aws code-commit list-repositories`
	• Überprüfen Sie dann, ob die in der Ausgabe aufgeführten Repositor ys mit den Namen der Repositorys übereinst immen, die sich in Ihrem AFT-Verwaltungskonto befinden.
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein neues lokales Verzeichnis, um den AFT-Repository-Code zu speichern .	Führen Sie in derselben Terminalsitzung die folgenden Befehle aus:
	`mkdir my_aft`
	`cd my_aft`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie den Remote-AFT-Repository-Code.	1. Führen Sie in Ihrem lokalen Terminal den folgenden Befehl aus:
	`git clone codecommit::$AWS_REGION://aft-global-customizations`
	Hinweis: Der Einfachheit halber verwenden dieses Verfahren und AFT nur einen Hauptcodezweig. Um die Codeverzweigung zu verwenden, können Sie auch hier Befehle zur Codeverzweigung eingeben. Alle angewandten Änderungen aus dem Nicht-Hauptzweig werden jedoch rückgängig gemacht, wenn die AFT-Automatisierung Code aus dem Hauptzweig anwendet.
	2. Navigieren Sie dann in das geklonte Verzeichnis, indem Sie den folgenden Befehl ausführen:
	`cd aft-global-customizations/terraform`
		AWS-Administrator

Erstellen Sie die Terraform-Konfigurationsdateien, die für die lokale Ausführung der AFT-Pipeline erforderlich sind

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie eine zuvor ausgeführte AFT-Pipeline und kopieren Sie die Terraform-Konfigurationsdateien in einen lokalen Ordner.	Hinweis: Die backend.tf- und aft-providers.tf-Konfigurationsdateien, die in diesem Epic erstellt werden, werden benötigt, damit die AFT-Pipeline lokal ausgeführt werden kann. Diese Dateien werden automatisch innerhalb der cloudbasierten AFT-Pipeline erstellt, müssen aber manuell erstellt werden, damit die Pipeline lokal ausgeführt werden kann. Für die lokale Ausführung der AFT-Pipeline ist ein Satz von Dateien erforderlich, der die Ausführung der Pipeline innerhalb eines einzigen AWS-Kontos darstellt. 1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Control Tower-Verwaltungskontos bei der AWS-Managementkonsole an. Öffnen Sie dann die AWS- CodePipeline Konsole . Stellen Sie sicher, dass Sie sich in derselben AWS-Region befinden, in der Sie AFT bereitgestellt haben.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im linken Navigationsbereich die Option Pipelines aus. 3. Wählen Sie ########## -customizations-pipeline aus. (##### ist die AWS-Konto-ID, die Sie verwenden, um Terraform-Code lokal auszuführen). 4. Stellen Sie sicher, dass die letzte markierte Ausführung einen Erfolgreich-Wert anzeigt. Wenn der Wert anders ist, müssen Sie Ihre Anpassungen in der AFT-Pipeline erneut aufrufen. Weitere Informationen finden Sie unter Anpassungen erneut aufrufen in der AWS Control Tower-Dokumentation. 5. Wählen Sie die neueste Laufzeit aus, um ihre Details anzuzeigen. 6. Suchen Sie im Abschnitt Apply-AFT-Global-Customizations die Phase Apply-Terraform. 7. Wählen Sie den Abschnitt Details der Stufe Apply-Terraform aus. 8. Suchen Sie das Laufzeitprotokoll für die Apply-Terraform-Phase.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Suchen Sie im Laufzeitprotokoll nach dem Abschnitt, der mit den folgenden Zeilen beginnt und endet: „\n\n aft-providers.tf ... „\n \n backend.tf“ 10. Kopieren Sie die Ausgabe zwischen diesen beiden Labels und speichern Sie sie als lokale Datei mit dem Namen `aft-providers.tf` im lokalen Terraform-Ordner (dem aktuellen Arbeitsverzeichnis Ihrer Terminalsitzung). Beispiel für eine automatisch generierte providers.tf-Anweisung `## Autogenerated providers.tf ## ## Updated on: 2022-05-31 16:27:45 ## provider "aws" { region = "us-east-2" assume_role { role_arn = "arn:aws:iam::########:role/AWSAFTExecution" } default_tags { tags = { managed_by = "AFT"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> }
	  }
	}</pre>
	11. Suchen Sie im Laufzeitprotokoll nach dem Abschnitt, der mit den folgenden Zeilen beginnt und endet: „\n\n tf ... „\n \n backup.tf“
	12. Kopieren Sie die Ausgabe zwischen diesen beiden Labels und speichern Sie sie als lokale Datei mit dem Namen `tf`im lokalen Terraform-Ordner (dem aktuellen Arbeitsverzeichnis Ihrer Terminalsitzung).
	
	Beispiel für eine automatisch generierte backend.tf-Anweisung
	
	<pre>## Autogenerated
	 backend.tf ##
	## Updated on: 2022-05-3
	1 16:27:45 ##
	terraform {
	  required_version =
	 ">= 0.15.0"
	  backend "s3" {
	    region =
	 "us-east-2"
	    bucket =
	 "aft-backend-#####
	#######-primary-re
	gion"
	    key =
	 "############-aft-</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>global-customizati
	ons/terraform.tfst
	ate"
	    dynamodb_table =
	 "aft-backend-#####
	#######"
	    encrypt =
	 "true"
	    kms_key_id =
	 "cbdc21d6-e04d-4c3
	7-854f-51e199cfcb7c"
	    kms_key_id =
	 "########-####-####-
	####-############"
	    role_arn =
	 "arn:aws:iam::####
	#########:role/AWS
	AFTExecution"
	  }
	}</pre>
	Hinweis: Die `aft-providers.tf` Dateien `backend.tf` und sind an ein bestimmtes AWS-Konto, eine AFT-Bereitstellung und einen bestimmten Ordner gebunden. Diese Dateien unterscheiden sich auch, je nachdem, ob sie sich im aft-global-customizationsRepository und aft-account-customizationsRepository innerhalb derselben AFT-Bereitstellung befinden. Stellen Sie sicher, dass Sie beide Dateien aus derselben Laufzeitliste generieren.	

Lokales Ausführen der AFT-Pipeline mithilfe des Beispiel-Bash-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie die Terraform-Konfigurationsänderungen, die Sie validieren möchten.	1. Navigieren Sie zum geklonten aft-global-customizationsRepository, indem Sie den folgenden Befehl ausführen: `cd aft-global-customizations/terraform` Hinweis: Die Dateien `backend.tf` und `aft-providers.tf` befinden sich in diesem Verzeichnis. Das Verzeichnis enthält auch Terraform-Dateien aus dem aft-global-customizations Repository. 2. Integrieren Sie die Terraform-Codeänderungen, die Sie lokal testen möchten, in die Konfigurationsdateien.	AWS-Administrator
Führen Sie das Skript ct_terraform.sh aus und überprüfen Sie die Ausgabe.	1. Navigieren Sie zu dem lokalen Ordner, der das sh-Skript enthält. 2. Um Ihren geänderten Terraform-Code zu validieren, führen Sie das `ct_terraform.sh` Skript aus, indem Sie den folgenden Befehl ausführen:	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`~/scripts/ct_terraform.sh apply`
	
	Hinweis: Sie können in diesem Schritt jeden Terraform-Befehl ausführen. Führen Sie den folgenden Befehl aus, um eine vollständige Liste der Terraform-Befehle anzuzeigen:
	
	`terraform --help`
	
	3. Überprüfen Sie die Befehlsausgabe. Debuggen Sie dann die Codeänder ungen lokal, bevor Sie die Änderungen festschreiben und zurück in das AFT-Repository verschieben.
	
	Wichtig
	
	• Alle lokal vorgenommenen und nicht in das Remote-Repository übertragenen Änderungen sind temporär und können jederzeit von einer laufenden AFT-Pipeline-Automatisierun g rückgängig gemacht werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die AFT-Automatisierung kann jederzeit ausgeführt werden, da sie von anderen Benutzern und AFT-Autom atisierungsauslösern aufgerufen werden kann. • AFT wendet immer Code aus dem Hauptzweig des Repositorys an und macht alle nicht festgeschriebenen Änderungen rückgängig.	

Übernehmen Sie Ihre lokalen Codeänderungen und übertragen Sie sie zurück in das AFT-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Verweise auf die Dateien backend.tf und aft-providers.tf zu einer Gitignore-Datei hinzu.	Fügen Sie die `aft-providers.tf` Dateien `backend.tf` und , die Sie erstellt haben, zu einer `.gitignore` Datei hinzu, indem Sie die folgenden Befehle ausführen:
	`echo backend.tf >> .gitignore`
	`echo aft-providers.tf >>.gitignore`
	Hinweis: Durch das Verschieb en der Dateien in die `.gitignore` Datei wird sichergestellt, dass sie nicht festgeschrieben und an das
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Remote-AFT-Repository übertragen werden.	

Übernehmen Sie Ihre Codeänderungen und übertragen Sie sie in das Remote-AFT-Repository.	1. Führen Sie den folgenden Befehl aus, um neue Terraform-Konfigurationsdateien zum Repository hinzuzufügen:
	`git add <filename>`
	2. Führen Sie die folgenden Befehle aus CodeCommit, um Ihre Änderungen zu bestätigen und sie in das Remote-AFT-Repository in AWS zu verschieben:
	`git commit -a`
	`git push`
	Wichtig: Die Codeänderungen, die Sie durch Befolgen dieses Verfahrens bis zu diesem Punkt einführen, werden nur auf ein AWS-Konto angewendet.
		AWS-Administrator

Rollout der Änderungen für mehrere Konten, die von AFT verwaltet werden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Änderungen für alle Ihre von AFT verwalteten Konten aus.	Um die Änderungen für mehrere von AFT verwaltete AWS-Konten einzuführen,	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgen Sie den Anweisungen unter Anpassungen erneut aufrufen in der AWS Control Tower-Dokumentation.	

Mehr Muster

- Hinzufügen von HA zu Oracle PeopleSoft auf Amazon RDS Custom mithilfe eines Lesereplikats
- Automatisieren des Hinzufügens oder Aktualisierens von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren der AWS-Ressourcenbewertung
- Automatisieren der Portfolio- und Produktbereitstellung von AWS Service Catalog mithilfe von AWS CDK
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- ???
- Automatisieren der Replikation von Amazon RDS-Instances über AWS-Konten hinweg
- Automatisches Anfügen einer von AWS verwalteten Richtlinie für Systems Manager an EC2-Instance-Profile mithilfe von Cloud Custodian und AWS CDK
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mit AWS CDK
- Automatisches Erkennen von Änderungen und Initiieren verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit
- ???
- Erstellen einer Datenpipeline zur Aufnahme, Transformation und Analyse von Google Analytics-Daten mit dem AWS DataOps Development Kit
- Erstellen Sie einen Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Erstellen und pushen Sie Docker-Images mithilfe von GitHub Aktionen und Terraform auf Amazon ECR
- Zentralisieren der IAM-Zugriffsschlüsselverwaltung in AWS Organizations mithilfe von Terraform
- Zentralisieren der Softwarepaketverteilung in AWS Organizations mithilfe von Terraform
- Verketten von AWS-Services mithilfe eines Serverless-Ansatzes
- Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode
- Konfigurieren von schreibgeschütztem Routing in einer AlwaysOn-Verfügbarkeitsgruppe in SQL Server auf AWS
- ???

- Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte
- Stellen Sie mithilfe von VMware Cloud on AWS ein VMware-SDDC auf AWS bereit
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Bereitstellen und Debuggen von Amazon-EKS-Clustern
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Stellen Sie die Lösung Security Automations für AWS WAF mithilfe von Terraform bereit
- Dokumentieren Ihres AWS-Landing-Zone-Designs
- Sicherstellen, dass ein IAM-Profil einer EC2-Instance zugeordnet ist
- Exportieren von AWS Backup-Berichten aus einer Organisation in AWS Organizations als CSV-Datei
- Generieren Sie personalisierte und neu eingestufte Empfehlungen mit Amazon Personalize
- Identifizieren und warnen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS-Schlüssel verschlüsselt sind
- Implementieren Sie Account Factory for Terraform (AFT) mithilfe einer Bootstrap-Pipeline
- Installieren des SSM-Agenten auf Amazon-EKS-Worker-Knoten mithilfe von Kubernetes DaemonSet
- Installieren Sie den SSM-Agenten und - CloudWatch Agenten auf Amazon-EKS-Worker-Knoten mit preBootstrapCommands
- Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS
- Verwalten von AWS Service Catalog-Produkten in mehreren AWS-Konten und AWS-Regionen
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- Migrieren Sie DNS-Datensätze in großen Mengen in eine privat gehostete Zone von Amazon Route 53
- Migrieren der Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren von Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren Sie RHEL-BYOL-Systeme mithilfe von AWS MGN zu Instances mit AWS-Lizenz
- Migrieren Sie VMware SDDC mit VMware HCX zu VMware Cloud on AWS

- Überwachen Sie ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand
- Überwachen von ElastiCache Clustern für Sicherheitsgruppen
- Überwachen von SAP RHEL-Pacemaker-Clustern mithilfe von AWS-Services
- Privater Zugriff auf einen zentralen AWS-Service-Endpunkt aus mehreren VPCs
- Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern
- Senden einer Benachrichtigung, wenn ein IAM-Benutzer erstellt wird
- Senden Sie mithilfe von VMware Aria Operations for Logs Logs Logs von VMware Cloud on AWS an Splunk
- Einrichten einer CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere mithilfe von AWS CDK und GitLab
- Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein
- ???
- Einrichten einer virtuellen Desktop-Infrastruktur (VDI) mit Auto Scaling mithilfe von NICE EnginFrame und NICE DCV Session Manager
- Einrichten einer HA/DR-Architektur für Oracle E-Business Suite in Amazon RDS Custom mit einer aktiven Standby-Datenbank
- Richten Sie die CloudFormation AWS-Drift-Erkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein
- Einrichten einer Multi-AZ-Infrastruktur für eine SQL Server Always On FCI mithilfe von Amazon FSx
- Einrichten der Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL – kompatibel
- Vereinfachen der Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM
- Automatisches Markieren von Transit Gateway-Anhängen mit AWS Organizations
- Übergangsrollen für eine Oracle- PeopleSoft Anwendung in Amazon RDS Custom für Oracle
- Verwenden von Serverspec für die testgesteuerte Entwicklung von Infrastrukturcode

IoT

Themen

Konfigurieren der Protokollierung und Überwachung für Sicherheitsereignisse in Ihrer AWS IoT-Umgebung

Erstellt von Prateek Prakash (AWS)

Umgebung: Produktion	Technologien: IoT; Sicherheit, Identität, Compliance; Betrieb	Workload: Alle anderen Workloads
AWS-Services: Amazon CloudWatch; Amazon OpenSearch Service; Amazon GuardDuty; AWS IoT Core; AWS IoT Device Defender ; AWS IoT Device Managemen t ; Amazon CloudWatch Logs		

Übersicht

Sicherstellen, dass Ihre Internet of Things (IoT)-Umgebungen sicher sind, hat eine wichtige Priorität, insbesondere weil Organisationen Milliarden von Geräten mit ihren IT-Umgebungen verbinden. Dieses Muster bietet eine Referenzarchitektur, mit der Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer gesamten IoT-Umgebung in der Amazon Web Services (AWS) Cloud implementieren können. In der Regel hat eine IoT-Umgebung in der AWS Cloud die folgenden drei Ebenen:

- IoT-Geräte, die relevante Telemetriedaten generieren.
- AWS IoT-Services (z. B. AWS IoT Core, AWS IoT Device Management oder AWS IoT Device Defender), die Ihre IoT-Geräte mit anderen Geräten und AWS-Services verbinden.
- Backend-AWS-Services, die bei der Verarbeitung von Telemetriedaten helfen und nützliche Einblicke für Ihre verschiedenen Geschäftsanwendungsfälle bieten.

Die bewährten Methoden des Whitepapers AWS IoT Lens – AWS Well-Architected Framework können Ihnen helfen, Ihre cloudbasierte Architektur zu überprüfen und zu verbessern und die Auswirkungen Ihrer Entwurfsentscheidungen auf das Geschäft besser zu verstehen. Eine wichtige

Empfehlung besteht darin, Anwendungsprotokolle und Metriken auf Ihren Geräten und in der AWS Cloud zu analysieren. Sie können dies erreichen, indem Sie verschiedene Ansätze und Techniken (z. B. Bedrohungsmodellierung) verwenden, um Metriken und Ereignisse zu identifizieren, die überwacht werden müssen, um potenzielle Sicherheitsprobleme zu erkennen.

Dieses Muster beschreibt, wie Sie AWS IoT und Sicherheitsservices verwenden, um eine Referenzarchitektur für Sicherheitsprotokollierung und -überwachung für eine IoT-Umgebung in der AWS Cloud zu entwerfen und zu implementieren. Diese Architektur baut auf vorhandenen bewährten AWS-Sicherheitsmethoden auf und wendet sie auf Ihre IoT-Umgebung an.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene Landing Zone-Umgebung. Weitere Informationen dazu finden Sie im Handbuch Einrichten einer sicheren und skalierbaren AWS-Umgebung mit mehreren Konten auf der Website AWS Prescriptive Guidance.
- Die folgenden Konten müssen in Ihrer Landing Zone verfügbar sein:
  - Log-Archive-Konto – Dieses Konto richtet sich an Benutzer, die auf die Protokollierungsinformationen für Konten in den Organisationseinheiten (OUs) Ihrer Landing Zone zugreifen müssen. Weitere Informationen dazu finden Sie im Abschnitt Sicherheits-OU – Protokollarchivkonto des Handbuchs AWS-Sicherheitsreferenzarchitektur auf der Website AWS Prescriptive Guidance.
  - Sicherheitskonto – Ihre Sicherheits- und Compliance-Teams verwenden dieses Konto für die Prüfung oder für die Durchführung von Notfallsicherheitsvorgängen. Dieses Konto wird auch als Administratorkonto für Amazon festgelegt GuardDuty. Benutzer aus dem Administratorkonto können konfigurieren GuardDuty, zusätzlich zum Anzeigen und Verwalten von GuardDuty Ergebnissen für ihr eigenes Konto und alle Mitgliedskonten. Weitere Informationen dazu finden Sie unter Verwalten mehrerer Konten in GuardDuty in der Amazon- GuardDuty Dokumentation.
  - IoT-Konto – Dieses Konto ist für Ihre IoT-Umgebung bestimmt.

Architektur

Dieses Muster erweitert die zentralisierte Protokollierungslösung aus der AWS Solutions Library, um sicherheitsrelevante IoT-Ereignisse zu erfassen und zu verarbeiten. Die zentralisierte Protokollierungslösung wird im Sicherheitskonto bereitgestellt und hilft dabei, Amazon- CloudWatch Protokolle in einem einzigen Dashboard zu sammeln, zu analysieren und anzuzeigen. Diese Lösung

konsolidiert, verwaltet und analysiert Protokolldateien aus mehreren Quellen. Schließlich verwendet die zentralisierte Protokollierungslösung auch Amazon OpenSearch Service und OpenSearch Dashboards, um eine einheitliche Ansicht aller Protokollereignisse anzuzeigen.

Das folgende Architekturdiagramm zeigt die wichtigsten Komponenten einer IoT-Sicherheitsprotokollierungs- und Referenzarchitektur in der AWS Cloud.

Das Diagramm zeigt den folgenden Workflow:

1. IoT-Objekte sind die Geräte, die auf anomale Sicherheitsereignisse überwacht werden müssen. Diese Geräte führen einen Agenten aus, um Sicherheitsereignisse oder Metriken in AWS IoT Core und AWS IoT Device Defender zu veröffentlichen.
2. Wenn die AWS IoT-Protokollierung aktiviert ist, sendet AWS IoT Fortschrittsereignisse zu jeder Nachricht, während sie von Ihren Geräten über den Message Broker und die Regel-Engine an Amazon CloudWatch Logs weitergeleitet wird. Sie können CloudWatch Logs-Abonnements verwenden, um Ereignisse an eine zentralisierte Protokollierungslösung zu übertragen. Weitere Informationen dazu finden Sie unter AWS IoT-Metriken und -Dimensionen in der AWS IoT Core-Dokumentation.
3. AWS IoT Device Defender hilft bei der Überwachung unsicherer Konfigurationen und Sicherheitsmetriken für Ihre IoT-Geräte. Wenn eine Anomalie erkannt wird, benachrichtigen Alarme Amazon Simple Notification Service (Amazon SNS), der über eine AWS Lambda-Funktion als Abonnent verfügt. Die Lambda-Funktion sendet den Alarm als Nachricht an CloudWatch Logs. Sie können - CloudWatch Protokollabonnements verwenden, um Ereignisse an Ihre zentralisierte Protokollierungslösung zu übertragen. Weitere Informationen dazu finden Sie unter Audit-Prüfungen , Geräteseitige Metriken und Cloud-seitige Metriken in der AWS IoT Core-Dokumentation. AWS IoT
4. AWS CloudTrail protokolliert AWS IoT Core-Aktionen auf Steuerebene, die Änderungen vornehmen (z. B. das Erstellen, Aktualisieren oder Anhängen von APIs). Wenn als Teil einer Landing Zone-Implementierung eingerichtet CloudTrail ist, sendet es Ereignisse an - CloudWatch Protokolle und Sie können Abonnements verwenden, um Ereignisse an Ihre zentralisierte Protokollierungslösung zu übertragen
5. Von AWS Config verwaltete Regeln oder benutzerdefinierte Regeln werten Ressourcen aus, die Teil Ihrer IoT-Umgebung sind. Überwachen Sie Ihre Benachrichtigungen über Compliance-Änderungen mit - CloudWatch Ereignissen mit - CloudWatch Protokollen als Ziel. Nachdem Benachrichtigungen über Compliance-Änderungen an - CloudWatch Protokolle gesendet wurden,

können Sie Abonnements verwenden, um Ereignisse an Ihre zentralisierte Protokollierungslösung zu übertragen.

6. Amazon analysiert GuardDuty kontinuierlich CloudTrail Verwaltungsereignisse und hilft dabei, API-Aufrufe an AWS IoT Core-Endpunkte anhand bekannter bösartiger IP-Adressen, ungewöhnlicher Geolocations oder Anonymisierung von Proxys zu identifizieren. Überwachen Sie GuardDuty Benachrichtigungen mit Amazon CloudWatch Events mit Protokollgruppen in CloudWatch Logs als Ziel. Wenn GuardDuty Benachrichtigungen an - CloudWatch Protokolle gesendet werden, können Sie Abonnements verwenden, um Ereignisse an Ihre Lösung für zentralisierte Überwachung zu übertragen, oder die GuardDuty Konsole in Ihrem Sicherheitskonto verwenden, um die Benachrichtigungen anzuzeigen.
7. AWS Security Hub überwacht Ihr IoT-Konto anhand bewährter Sicherheitsmethoden. Überwachen Sie Security Hub-Benachrichtigungen, indem Sie CloudWatch Ereignisse mit Protokollgruppen in - CloudWatch Protokollen als Ziel verwenden. Wenn Security Hub-Benachrichtigungen an CloudWatch Logs gesendet werden, verwenden Sie Abonnements, um Ereignisse an Ihre Lösung für zentralisierte Überwachung zu übertragen, oder verwenden Sie die Security Hub-Konsole in Ihrem Sicherheitskonto, um die Benachrichtigungen anzuzeigen.
8. Amazon Detective wertet Informationen aus und analysiert sie, um die Ursache zu isolieren und Maßnahmen für Sicherheitserkenntnisse für ungewöhnliche Aufrufe an AWS IoT-Endpunkte oder andere Services in Ihrer IoT-Architektur zu ergreifen.
9. Amazon Athena fragt Protokolle ab, die in Ihrem Log-Archive-Konto gespeichert sind, um Ihr Verständnis für Sicherheitserkenntnisse zu verbessern und Trends und böswillige Aktivitäten zu identifizieren.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, der die direkte Analyse von Daten in Amazon Simple Storage Service (Amazon S3) mit Standard-SQL vereinfacht.
- AWS CloudTrail unterstützt Sie bei der Aktivierung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos.
- Amazon CloudWatch überwacht Ihre AWS-Ressourcen und die Anwendungen, die Sie auf AWS ausführen, in Echtzeit. Sie können verwenden, CloudWatch um Metriken zu erfassen und zu verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können.
- Amazon CloudWatch Logs zentralisiert die Protokolle von all Ihren Systemen, Anwendungen und AWS-Services, die Sie verwenden. Sie können die Protokolle anzeigen und überwachen, nach

bestimmten Fehlercodes oder Mustern suchen, sie nach bestimmten Feldern filtern oder sie sicher für zukünftige Analysen archivieren.

- AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto.
- Amazon Detective erleichtert die Analyse, Untersuchung und schnelle Identifizierung der Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten.
- AWS Glue ist ein vollständig verwalteter ETL-Service (Extract, Transform, Load), mit dem Sie Ihre Daten einfach und kostengünstig kategorisieren, bereinigen, anreichern und zuverlässig zwischen verschiedenen Datenspeichern und Datenströmen verschieben können.
- Amazon GuardDuty ist ein kontinuierlicher Service zur Sicherheitsüberwachung.
- AWS IoT Core bietet eine sichere, bidirektionale Kommunikation für mit dem Internet verbundene Geräte (wie Sensoren, Aktuatoren, eingebettete Geräte, WLAN-Geräte und intelligente Appliances), um über MQTT, HTTPS und LoRaWAN eine Verbindung zur AWS Cloud herzustellen.
- AWS IoT Device Defender ist ein Sicherheitsservice, mit dem Sie die Konfiguration Ihrer Geräte überprüfen, verbundene Geräte überwachen können, um anormales Verhalten zu erkennen und Sicherheitsrisiken zu minimieren.
- Amazon OpenSearch Service ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von OpenSearch Clustern in der AWS Cloud vereinfacht.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.
- Amazon Virtual Private Cloud (Amazon VPC) stellt einen logisch isolierten Abschnitt der AWS Cloud bereit, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Polen

Einrichten eines IoT-Kontos in Ihrer Landing-Zone-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Sicherheitsvorkehrungen im IoT-Konto.	Überprüfen Sie, ob die Integritätsschutzrichtlinien für CloudTrail, AWS Config GuardDutyund Security Hub in Ihrem IoT-Konto aktiviert sind.	AWS-Administrator
Überprüfen Sie, ob Ihr IoT-Konto als Mitgliedskonto Ihres Sicherheitskontos konfiguriert ist.	Überprüfen Sie, ob Ihr IoT-Konto konfiguriert und als Mitgliedskonto für GuardDuty und Security Hub in Ihrem Sicherheitskonto verknüpft ist. Weitere Informationen dazu finden Sie unter Verwalten von GuardDuty Konten mit AWS Organizations in der Amazon-GuardDuty Dokumentation und Verwalten von Administrator- und Mitgliedskonten in der AWS Security Hub-Dokumentation.	AWS-Administrator
Validieren Sie die Protokollarchivierung.	Überprüfen Sie, ob CloudTrail-, AWS Config- und VPC-Flow-Protokolle im Log Archive-Konto gespeichert sind.	AWS-Administrator

Einrichten der zentralen Protokollierungslösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die zentralisierte Protokollierungslösung in Ihrem -Sicherheitskonto ein.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Sicherheitskonto an und richten Sie die Lösung für die zentrale Protokollierung aus der AWS Solutions Library ein, um CloudWatch Protokolle in Amazon OpenSearch Service und OpenSearch Dashboard s zu erfassen, zu analysieren und anzuzeigen. Weitere Informationen dazu finden Sie unter Erfassen, Analysieren und Anzeigen von Amazon CloudWatch Logs in einem einzigen Dashboard mit der zentralen Protokoll ierungslösung aus dem Implementierungshandbuch für die zentrale Protokollierung in der AWS-Lösungsbibliothek.	AWS-Administrator

Einrichten und Konfigurieren von AWS-Ressourcen in Ihrem IoT-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die AWS IoT-Protokollierung ein.	Melden Sie sich bei der AWS-Managementkonsole für Ihr IoT-Konto an. Richten Sie AWS IoT Core so ein und konfigurieren Sie es, dass	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protokolle an CloudWatch - Protokolle gesendet werden. Weitere Informationen dazu finden Sie unter Konfigurieren der AWS IoT-Protokollierung und Überwachen von AWS IoT mithilfe von CloudWatch Protokollen in der AWS IoT Core-Dokumentation.	
Richten Sie AWS IoT Device Defender ein.	Richten Sie AWS IoT Device Defender ein, um Ihre IoT-Ressourcen zu überprüfen und Anomalien zu erkennen. Weitere Informationen dazu finden Sie unter Erste Schritte mit AWS IoT Device Defender in der AWS IoT Core-Dokumentation.	AWS-Administrator
Richten Sie ein CloudTrail.	Richten Sie so ein CloudTrail , dass Ereignisse an - CloudWatch Protokolle gesendet werden. Weitere Informationen dazu finden Sie unter Senden von Ereignissen an CloudWatch Protokolle in der AWS-CloudTrail Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS Config- und AWS Config-Regeln ein.	Richten Sie AWS Config und die erforderlichen AWS Config-Regeln ein. Weitere Informationen dazu finden Sie unter Einrichten von AWS Config mit der Konsole und Einrichten von AWS Config-Regeln mit der Konsole in der AWS Config-Dokumentation.	AWS-Administrator
Richten Sie ein GuardDuty.	Richten Sie so ein und konfigurieren Sie GuardDuty so, dass Ergebnisse an Amazon CloudWatch Events mit Protokollgruppen in - CloudWatch Protokollen als Ziel gesendet werden. Weitere Informationen dazu finden Sie unter Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events in der Amazon-GuardDuty Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Security Hub ein.	Richten Sie Security Hub ein und aktivieren Sie die Standards CIS AWS Foundations Benchmark und AWS Foundational Security Best Practices. Weitere Informationen dazu finden Sie unter Automatisierte Reaktion und Behebung in der AWS Security Hub-Dokumentation.	AWS-Administrator
Richten Sie Amazon Detective ein.	Richten Sie Detective ein, um die Analyse von Sicherheitsergebnissen zu erleichtern Weitere Informationen dazu finden Sie unter Einrichten von Amazon Detective in der Amazon-Detective-Dokumentation.	AWS-Administrator
Richten Sie Amazon Athena und AWS Glue ein.	Richten Sie Athena und AWS Glue ein, um die AWS-Serviceprotokolle abzufragen, die Untersuchungen von Sicherheitsvorfällen durchführen. Weitere Informationen dazu finden Sie unter Abfragen von AWS-Serviceprotokollen in der Amazon Athena-Dokumentation.	AWS-Administrator

Zugehörige Ressourcen

- Was ist eine Landing Zone?

Extrahieren und Abfragen von AWS IoT SiteWise -Metadatenattributen in einem Data Lake

Erstellt von Ambarish Dongaonkar (AWS)

Umgebung: Produktion	Technologien: IoT; Analytik; Big Data	AWS-Services: AWS IoT SiteWise ;AWS Lambda ;AWS Glue

Übersicht

AWS IoT SiteWise verwendet Komponentenmodelle und Hierarchien, um Ihre Industrieanlagen, Prozesse und Anlagen darzustellen. Jedes Modell oder jede Komponente kann mehrere Attribute haben, die für Ihre Umgebung spezifisch sind. Beispiele für Metadatenattribute sind der Standort oder physische Standort der Komponente, Anlagendetails und Gerätekennungen. Diese Attributwerte ergänzen die Messungsdaten von Komponenten, um den Geschäftswert zu maximieren. Machine Learning (ML) kann zusätzliche Einblicke in diese Metadaten bieten und Engineering-Aufgaben optimieren.

Metadatenattribute können jedoch nicht direkt vom AWS IoT SiteWise -Service abgefragt werden. Um die Attribute abfragbar zu machen, müssen Sie sie extrahieren und in einen Data Lake aufnehmen. Dieses Muster verwendet ein Python-Skript, um die Attribute für alle AWS IoT SiteWise -Komponenten zu extrahieren und sie in einen Data Lake in einem Amazon Simple Storage Service (Amazon S3)-Bucket aufzunehmen. Wenn Sie diesen Vorgang abgeschlossen haben, können Sie SQL-Abfragen in Amazon Athena verwenden, um auf die AWS IoT SiteWise -Metadatenattribute und andere Datensätze zuzugreifen, z. B. Messungsdatensätze. Die Metadatenattributinformationen sind auch nützlich, wenn Sie mit AWS IoT SiteWise -Monitoren oder Dashboards arbeiten. Sie können ein AWS QuickSight -Dashboard auch mithilfe der extrahierten Attribute im S3-Bucket erstellen.

Das Muster enthält Referenzcode, und Sie können den Code implementieren, indem Sie die besten Datenverarbeitungsservices für Ihren Anwendungsfall verwenden, z. B. AWS Lambda oder AWS Glue .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Einrichten von AWS Lambda-Funktionen oder AWS Glue-Aufträgen.
- Ein Amazon-S3-Bucket
- Die Komponentenmodelle und Hierarchien sind in AWS IoT SiteWise eingerichtet. Weitere Informationen finden Sie unter Erstellen von Komponentenmodellen (AWS IoT SiteWise - Dokumentation).

Architektur

Sie können eine Lambda-Funktion oder einen AWS Glue-Auftrag verwenden, um diesen Vorgang abzuschließen. Wir empfehlen die Verwendung von Lambda, wenn Sie weniger als 100 Modelle haben und jedes Modell durchschnittlich 15 oder weniger Attribute hat. Für alle anderen Anwendungsfälle empfehlen wir die Verwendung von AWS Glue .

Die Lösungsarchitektur und der Workflow sind im folgenden Diagramm dargestellt.

1. Der geplante AWS Glue-Auftrag oder die Lambda-Funktion wird ausgeführt. Es extrahiert die Attribute der Komponentenmetadaten aus AWS IoT SiteWise und nimmt sie in einen S3-Bucket auf.
2. Ein AWS Glue-Crawler crawlt die extrahierten Daten im S3-Bucket und erstellt Tabellen in einem AWS Glue Data Catalog.
3. Mit Standard-SQL fragt Amazon Athena die Tabellen im AWS Glue Data Catalog ab.

Automatisierung und Skalierung

Sie können die Ausführung der Lambda-Funktion oder des AWS Glue-Auftrags täglich oder wöchentlich planen, je nach Aktualisierungshäufigkeit Ihrer AWS IoT SiteWise - Komponentenkonfigurationen.

Es gibt keine Begrenzung für die Anzahl der AWS IoT SiteWise -Komponenten, die der Beispielcode verarbeiten kann, aber eine große Anzahl von Komponenten kann den Zeitaufwand für den Abschluss des Prozesses erhöhen.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- AWS Glue ist ein vollständig verwalteter ETL-Service (Extract, Transform, Load). Es hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS IoT SiteWise hilft Ihnen dabei, Daten von Industrieanlagen in großem Umfang zu sammeln, zu modellieren, zu analysieren und zu visualisieren.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS SDK for Python (Boto3) ist ein Software Development Kit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr -Skript in AWS-Services integrieren können.

Polen

Einrichten des Auftrags oder der Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Berechtigungen in IAM.	Erteilen Sie in der IAM-Konsole Berechtigungen für die IAM-Rolle, die von der Lambda-Funktion oder dem AWS Glue-Auftrag übernommen wird, um Folgendes zu tun: • Aus dem AWS IoT SiteWise -Service lesen • Schreiben in den S3-Bucket	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Erstellen einer Rolle für einen AWS-Service (IAM-Dokumentation).	
Erstellen Sie die Lambda-Funktion oder den AWS Glue-Auftrag.	Wenn Sie Lambda verwenden, erstellen Sie eine neue Lambda-Funktion. Wählen Sie für Laufzeit Python aus. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Python (Lambda-Dokumentation). Wenn Sie AWS Glue verwenden, erstellen Sie einen neuen Python-Shell-Auftrag in der AWS Glue-Konsole. Weitere Informationen finden Sie unter Hinzufügen von Python-Shell-Aufträgen (AWS Glue-Dokumentation).	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Lambda-Funktion oder den AWS Glue-Auftrag.	Ändern Sie die neue Lambda-Funktion oder den AWS Glue-Auftrag und geben Sie das Codebeispiel im Abschnitt Zusätzliche Informationen ein. Ändern Sie den Code nach Bedarf für Ihren Anwendungsfall. Weitere Informationen finden Sie unter Bearbeiten von Code mit dem Konsoleneditor (Lambda-Dokumentation) und Arbeiten mit Skripten (AWS Glue-Dokumentation).	Allgemeines AWS

Ausführen des Auftrags oder der Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Lambda-Funktion oder den AWS Glue-Auftrag aus.	Führen Sie die Lambda-Funktion oder den AWS Glue-Auftrag aus. Weitere Informationen finden Sie unter Aufrufen der Lambda-Funktion (Lambda-Dokumentation) oder Starten von Aufträgen mit Auslösern (AWS Glue-Dokumentation). Dadurch werden die Metadatenattribute für die Komponenten und Modelle in der AWS IoT SiteWise - Hierarchie extrahiert und im angegebenen S3-Bucket gespeichert.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen AWS Glue-Crawler ein.	Richten Sie einen AWS Glue-Crawler mit dem erforderlichen Formatklassifizierer für eine CSV-formatierte Datei ein. Verwenden Sie die S3-Bucket - und Präfixdetails, die in der Lambda-Funktion oder dem AWS Glue-Auftrag verwendet werden. Weitere Informationen finden Sie unter Definieren von Crawlern (AWS Glue-Dokumentation).	Allgemeines AWS
Führen Sie den AWS Glue-Crawler aus.	Führen Sie den Crawler aus, um die Datendatei zu verarbeiten, die von der Lambda-Funktion oder dem AWS Glue-Auftrag erstellt wurde. Der Crawler erstellt eine Tabelle im angegebenen AWS Glue Data Catalog. Weitere Informationen finden Sie unter oder Starten von Crawlern mit Auslösern (AWS Glue-Dokumentation).	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fragen Sie die Metadaten attribute ab.	Verwenden Sie mit Amazon Athena Standard-SQL, um den AWS Glue Data Catalog nach Bedarf für Ihren Anwendungsfall abzufrage n. Sie können die Metadaten attributtabelle mit anderen Datenbanken und Tabellen verknüpfen. Weitere Informati onen finden Sie unter Erste Schritte (Amazon Athena-Do kumentation).	Allgemeines AWS

Zugehörige Ressourcen

- Amazon Athena-Dokumentation
- AWS Glue-Dokumentation
- AWS IoT SiteWise -API-Referenz
- AWS IoT SiteWise -Benutzerhandbuch
  - Erste Schritte
  - Modellieren von Industriekomponenten
  - Definieren von Beziehungen zwischen Komponentenmodellen (Hierarchien)
  - Zuordnen und Aufheben der Zuordnung von Komponenten
  - Erstellen der AWS IoT SiteWise -Demo
- IOTSiteWise (Dokumentation zu SDK für Python)
- Lambda-Dokumentation

Zusätzliche Informationen

Code

Der bereitgestellte Beispielcode dient als Referenz, und Sie können diesen Code nach Bedarf an Ihren Anwendungsfall anpassen.

```
# Following code can be used in an AWS Lambda function or in an AWS Glue Python shell
 job.
# IAM roles used for this job need read access to the AWS IoT SiteWise service and
 write access to the S3 bucket.
sw_client = boto3.client('iotsitewise')
s3_client = boto3.client('s3')
output = io.StringIO()

attribute_list=[]
bucket = '{3_bucket name}'
prefix = '{s3_bucket prefix}'
output.write("model_id,model_name,asset_id,asset_name,attribuet_id,attribute_name,attribute_val
\n")

m_resp = sw_client.list_asset_models()
for m_rec in m_resp['assetModelSummaries']:
     model_id = m_rec['id']
     model_name = m_rec['name']

     attribute_list.clear()
     dam_response = sw_client.describe_asset_model(assetModelId=model_id)
     for rec in dam_response['assetModelProperties']:
         if 'attribute' in rec['type']:
            attribute_list.append(rec['name'])

     response = sw_client.list_assets(assetModelId=model_id, filter='ALL')
     for asset in response['assetSummaries']:
         asset_id = asset['id']
         asset_name = asset['name']
         resp = sw_client.describe_asset(assetId=asset_id)
         for rec in resp['assetProperties']:
            if rec['name'] in attribute_list:
                p_resp = sw_client.get_asset_property_value(assetId=asset_id,
 propertyId=rec['id'])
                if 'propertyValue' in p_resp:
                    if p_resp['propertyValue']['value']:
                        if 'stringValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
```

```
 str(p_resp['propertyValue']['value']['stringValue']) + "\n")

                        if 'doubleValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['doubleValue']) + "\n")
                        if 'integerValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['integerValue']) + "\n")
                         if 'booleanValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['booleanValue']) + "\n")

output.seek(0)
s3_client.put_object(Bucket=bucket, Key= prefix + '/data.csv', Body=output.getvalue())
output.close()
```

Einrichten und Beheben von Problemen mit AWS IoT Greengrass mit Clientgeräten

Erstellt von Marouane Sefiani und Akalanka De Silva (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: IoT	AWS-Services: AWS IoT Greengrass; AWS IoT Core

Übersicht

AWS IoT Greengrass ist ein Open-Source-Edge-Laufzeit- und Cloud-Service zum Erstellen, Bereitstellen und Verwalten von Internet of Things (IoT)-Software auf Edge-Geräten. Zu den Anwendungsfällen für AWS IoT Greengrass gehören:

- Smart Homes, in denen ein AWS IoT Greengrass-Gateway als Hub für die Hausautomatisierung verwendet wird
- Smart Factorys, in denen AWS IoT Greengrass die Aufnahme und lokale Verarbeitung von Daten aus der Shop-Etage ermöglichen kann

AWS IoT Greengrass kann als sicherer, authentifizierter MQTT-Verbindungsendpunkt für andere Edge-Geräte (auch bekannt als Client-Geräte) fungieren, die andernfalls normalerweise direkt eine Verbindung zu AWS IoT Core herstellen würden. Diese Funktion ist nützlich, wenn Client-Geräte keinen direkten Netzwerkzugriff auf den AWS IoT Core-Endpunkt haben.

Sie können AWS IoT Greengrass für die Verwendung mit Client-Geräten für die folgenden Anwendungsfälle einrichten:

- Damit Client-Geräte Daten an AWS IoT Greengrass senden können
- Damit AWS IoT Greengrass Daten an AWS IoT Core weiterleiten kann
- So nutzen Sie die erweiterten AWS IoT Core-Regel-Engine-Funktionen

Diese Funktionen erfordern die Installation und Konfiguration der folgenden Komponenten auf dem AWS IoT Greengrass-Gerät:

- MQTT-Broker

- MQTT-Brücke
- Client-Geräteauthentifizierung
- IP-Detektor

Darüber hinaus müssen veröffentlichte Nachrichten von Client-Geräten im JSON-Format oder im Protocol Buffers (protobuf)-Format vorliegen.

Dieses Muster beschreibt, wie Sie diese erforderlichen Komponenten installieren und konfigurieren, und enthält Tipps zur Fehlerbehebung und bewährte Methoden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2
- Zwei Client-Geräte mit Python 3.7 oder höher
- Ein Core-Gerät mit Java Runtime Environment (JRE) Version 8 oder höher und Amazon Corretto 11 oder OpenJDK 11

Einschränkungen

- Sie müssen eine AWS-Region auswählen, in der AWS IoT Core verfügbar ist. Die aktuelle Liste der Regionen für AWS IoT Core finden Sie unter AWS-Services nach Region .
- Das Core-Gerät muss über mindestens 172 MB RAM und 512 MB Festplattenspeicher verfügen.

Architektur

Das folgende Diagramm zeigt die Lösungsarchitektur für dieses Muster.

Die Architektur umfasst:

- Zwei Client-Geräte. Jedes Gerät enthält einen privaten Schlüssel, ein Gerätezertifikat und ein CA-Zertifikat (Root Certificate Authority). Das AWS IoT Device SDK, das einen MQTT-Client enthält, ist ebenfalls auf jedem Client-Gerät installiert.

- Ein Core-Gerät, auf dem AWS IoT Greengrass mit den folgenden Komponenten bereitgestellt wird:
  - MQTT-Broker
  - MQTT-Brücke
  - Client-Geräteauthentifizierung
  - IP-Detektor

Diese Architektur unterstützt die folgenden Szenarien:

- Client-Geräte können ihren MQTT-Client verwenden, um über den MQTT-Broker des Core-Geräts miteinander zu kommunizieren.
- Client-Geräte können auch über den MQTT-Broker des Core-Geräts und die MQTT-Bridge mit AWS IoT Core in der Cloud kommunizieren.
- AWS IoT Core in der Cloud kann Nachrichten über den MQTT-Testclient und die MQTT-Bridge und den MQTT-Broker des Core-Geräts an Client-Geräte senden.

Weitere Informationen zur Kommunikation zwischen Client-Geräten und dem Core-Gerät finden Sie im Abschnitt Zusätzliche Informationen.

Tools

AWS-Services

- AWS IoT Greengrass ist ein Open-Source-Edge-Laufzeit- und Cloud-Service für das Internet der Dinge (IoT), mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können.
- AWS IoT Core bietet eine sichere, bidirektionale Kommunikation für mit dem Internet verbundene Geräte, um eine Verbindung zur AWS Cloud herzustellen.
- AWS IoT Device SDK ist ein Software Development Kit, das Open-Source-Bibliotheken, Entwicklerhandbücher mit Beispielen und Portierungshandbüchern enthält, sodass Sie innovative IoT-Produkte oder -Lösungen auf Hardwareplattformen Ihrer Wahl entwickeln können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.

Bewährte Methoden

- Die Nutzlast der Nachrichten von Client-Geräten sollte entweder im JSON- oder Protobuf-Format vorliegen, um die erweiterten Funktionen der AWS IoT Core-Regel-Engine zu nutzen, z. B. Transformations- und bedingte Aktionen.
- Konfigurieren Sie die MQTT-Brücke, um bidirektionale Kommunikation zu ermöglichen.
- Konfigurieren und stellen Sie die IP-Detektorkomponente in AWS IoT Greengrass bereit, um sicherzustellen, dass die IP-Adressen des Core-Geräts im Feld Subject Alternative Name (SAN) des MQTT-Brokerzertifikats enthalten sind.

Polen

Einrichten des Core-Geräts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS IoT Greengrass auf Ihrem Core-Gerät ein.	Installieren Sie die AWS IoT Greengrass Core-Software, indem Sie den Anweisungen im Entwicklerhandbuch folgen.	AWS IoT Greengrass

Überprüfen Sie den Status Ihrer Installation.	Verwenden Sie den folgenden Befehl, um den Status des AWS IoT Greengrass-Services auf Ihrem Core-Gerät zu überprüfen:
	`sudo systemctl status greengrass.service`
	Die erwartete Ausgabe des Befehls ist:
	`Launched Nucleus successfully`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine IAM-Richtlinie ein und fügen Sie sie der Greengrass-Servicerolle an.	1. Erstellen Sie eine IAM-Richtlinie, um die Kommunikation zur und von der MQTT-Brücke zu ermöglichen. Hier ist ein Beispiel für eine Richtlinie: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iot:*" ], "Resource": "*" }, { "Sid": "GreengrassActions", "Effect": "Allow", "Action": [ "greengrass:*" ], "Resource": "*" } ] }`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Fügen Sie die Richtlinie an die Greengrass-Servicerolle an. Verwenden Sie den Befehl , um die Servicerolle abzurufen: `aws greengrassv2 get-service-role-for-account --region <region>` wobei sich auf Ihre AWS-Region `<region>` bezieht.	
Konfigurieren und stellen Sie die erforderlichen Komponenten im AWS IoT Greengrass-Kerngerät bereit.	Konfigurieren Sie die folgenden Komponenten und stellen Sie sie bereit: • `greengrass.clientdevices.mqtt.Moquette` (siehe Konfigurationsdetails) • `greengrass.clientdevices.mqtt.Bridge` (siehe Konfigurationsdetails und nächste Aufgabe) • `greengrass.clientdevices.Auth` (siehe Konfigurationsdetails und die Aufgabe nach der nächsten) • `aws.greengrass.clientdevices.IPDetector` (siehe Konfigurationsdetails)	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die MQTT-Brücke bidirekti onale Kommunikation zulässt.	Um MQTT-Nachrichten zwischen Client-Geräten und AWS IoT Core weiterzuleiten, konfigurieren und stellen Sie die MQTT-Bridge-Kompon ente bereit und geben Sie die Themen an, die weitergeleitet werden sollen. Ein Beispiel: `{ "mqttTopicMapping": { "ClientDevicesToCloud": { "topic": "dt/#", "source": "LocalMqtt", "target": "IotCore" }, "CloudToClientDevices": { "topic": "cmd/#", "source": "IotCore", "target": "LocalMqtt" } } }`	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die Authentifizierungskomponente es Client-Geräten ermöglicht, Themen zu verbinden und zu veröffentlichen oder zu abonnieren.	Die folgende `aws.greengrass.clientdevices.Auth` Konfiguration ermöglicht es allen Client-Geräten, eine Verbindung herzustellen, Nachrichten zu veröffentlichen und alle Themen zu abonnieren. `{ "deviceGroups": { "formatVersion": "2021-03-05", "definitions": { "MyPermissiveDeviceGroup": { "selectionRule": "thingName: *", "policyName": "MyPermissivePolicy" } }, "policies": { "MyPermissivePolicy": { "AllowAll": { "statementDescription": "Allow client devices to perform all actions.", "operations": ["*"], "resources": ["*"] }`	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>}
	}
	}
	}</pre>	

Einrichten von Client-Geräten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS IoT Device SDK.	Installieren Sie das AWS IoT Device SDK auf Client-Ge räten. Eine vollständige Liste der unterstützten Sprachen und der zugehörigen SDKs finden Sie in der AWS IoT Core-Dokumentation. Beispielsweise befindet sich das AWS IoT Device SDK for Python SDK auf . GitHub So installieren Sie dieses SDK: 1. Vergewissern Sie sich, dass Python 3.7 oder höher installiert ist, wie auf der Seite Voraussetzungen des GitHub Repositorys beschrieben. 2. Verwenden Sie den Befehl pip, um das SDK zu installie ren. Für MacOS und Linux:	Allgemeines AWS IoT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`python3 -m pip install awsiotsdk`
	
	Für Windows:
	
	`python -m pip install awsiotsdk`
	
	Alternativ können Sie das SDK aus dem Quell-Repository installieren:
	
	`# Create a workspace directory to hold all the SDK files`
	`mkdir sdk-workspace`
	`cd sdk-workspace`
	`# Clone the repository`
	`git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git`
	`# Install using Pip (use 'python' instead of 'python3' on Windows)`
	`python3 -m pip install ./aws-iot-device-sdk-python-v2`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Objekt.	1. Wenn in der AWS IoT-Konsole eine Schaltfläche Erste Schritte angezeigt wird, wählen Sie sie aus. Andernfalls wählen Sie im Navigationsbereich Sicherheit, Richtlinien aus. 2. Wenn das Dialogfeld Sie haben noch keine Richtlinien angezeigt wird, wählen Sie Richtlinie erstellen aus. Wählen Sie andernfalls Erstellen. 3. Geben Sie einen Namen für die AWS IoT-Richtlinie ein (z. B. `ClientDevicePolicy`). 4. Ersetzen Sie im Abschnitt Anweisungen hinzufügen die vorhandene Richtlinie durch den folgenden JSON-Code. Ersetzen Sie `<region>` und `<account>` durch Ihre AWS-Region und AWS-Kontonummer. `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "iot:Connect",`	AWS IoT Core

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Resource": "arn:aws:iot:region:account:client/*" }, { "Effect": "Allow", "Action": "iot:Publish", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Receive", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Subscribe", "Resource": "*" }, { "Effect": "Allow", "Action": ["iot:GetThingShadow", "iot:UpdateThingShadow", "iot:DeleteThingShadow"], "Resource": "arn:aws:iot:region:account:thing/*"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre> }] }</pre> 5. Wählen Sie Erstellen. 6. Wählen Sie in der AWS IoT-Konsole im Navigatio nsbereich Verwalten, Objekte aus. 7. Wenn das Dialogfeld Sie haben noch keine Objekte angezeigt wird, wählen Sie Objekt registrieren aus. Wählen Sie andernfalls Erstellen. 8. Wählen sie auf der Seite Creating AWS IoT things (AWS IoT-Objekte erstellen) den Eintrag Create a single thing (Einzelnes Objekt erstellen). 9. Geben Sie auf der Seite Add your device to the device registry (Ihr Gerät zur Geräteregistrierung hinzufügen) einen Namen für Ihr IoT-Objekt ein (z. B. `ClientDevice1`) und wählen Sie dann Next (Weiter). Hinweis: Sie können den Namen eines Objekts nicht mehr ändern, nachdem Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	es erstellt haben. Um den Namen zu ändern, müssen Sie ein neues Objekt erstellen, ihm den neuen Namen geben und dann das alte Objekt löschen. 10. Wählen Sie auf der Seite Add a certificate for your thing (Fügen Sie ein Zertifikat für Ihr Objekt hinzu.) die Option Create certificate (Zertifikat erstellen). 11. Klicken Sie auf die Download-Links, um das Zertifikat, den privaten Schlüssel und das CA-Stammzertifikat herunterzuladen. Wichtig: Dies ist Ihre einzige Möglichkeit, Ihr Zertifikat und Ihren privaten Schlüssel herunterzuladen. 12. Wählen Sie Aktivieren aus, um Ihr Zertifikat zu aktivieren. Das Zertifikat muss aktiv sein, damit ein Gerät eine Verbindung mit AWS IoT herstellen kann. 13. Wählen Sie Attach a policy (Richtlinie anfügen) aus. 14. Wählen Sie für Richtlinie für Ihr Objekt hinzufügen die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Option ClientDevicePolicy, Objekt registrieren aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das CA-Zertifikat vom Greengrass-Core-Gerät herunter.	Wenn Sie erwarten, dass das Greengrass-Core-Gerät in Offline-Umgebungen funktioniert, müssen Sie das Greengrass-Core-CA-Zertifikat für das Client-Gerät verfügbar machen, damit es das Zertifikat des MQTT-Brokers überprüfen kann (das von der Greengrass-Core-CA ausgestellt wurde). Daher ist es wichtig, eine Kopie dieses Zertifikats zu erhalten. Verwenden Sie einen der folgenden Ansätze, um das CA-Zertifikat herunterzuladen: • Wenn Sie von Ihrem PC aus Netzwerkzugriff auf das AWS IoT Greengrass-Gerät haben, geben Sie `https://<device IP>:8883` in Ihren Webbrowser ein und zeigen Sie das MQTT-Brokerzertifikat und das CA-Zertifikat an. Sie können das CA-Zertifikat auch auf dem Client-Gerät speichern. • Alternativ können Sie die OpenSSL-Befehlszeile verwenden:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`openssl s_client -showcerts -connect <device IP>:8883`	
Kopieren Sie die Anmeldeinformationen auf den Client-Geräten.	Kopieren Sie das Greengrass-Core-CA-Zertifikat, das Gerätezertifikat und den privaten Schlüssel auf den Clientgeräten.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie dem Core-Gerät Client-Geräte zu.	Ordnen Sie Client-Geräte einem Core-Gerät zu, damit sie das Core-Gerät erkennen können. Die Client-Geräte können dann die Greengrass-Discovery-API verwenden, um Konnektivitätsinformationen und Zertifikate für ihre zugehörigen Core-Geräte abzurufen. Weitere Informationen finden Sie unter Zuordnen von Clientgeräten in der AWS IoT Greengrass-Dokumentation. 1. Wählen Sie in der AWS IoT Greengrass-Konsole die Option Core-Geräte aus. 2. Wählen Sie das zu verwaltende Core-Gerät aus. 3. Wählen Sie auf der Detailseite des Core-Geräts die Registerkarte Client-Geräte aus. 4. Wählen Sie im Abschnitt Zugeordnete Client-Geräte die Option Client-Geräte zuordnen aus. 5. Gehen Sie im Modal Client-Geräte dem Core-Gerät zuordnen für jedes Client-Gerät wie folgt vor:	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	a. Geben Sie den Namen des AWS IoT-Objekts ein, das als Client-Gerät zugeordnet werden soll. b. Wählen Sie Hinzufügen aus. 6. Wählen Sie Associate aus. Die Client-Geräte, die Sie zugeordnet haben, können jetzt die Greengrass-Erkennungs-API verwenden , um dieses Core-Gerät zu erkennen.	

Senden und Empfangen von Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Daten von einem Client-Gerät an ein anderes Client-Gerät.	Verwenden Sie den MQTT-Client auf Ihrem Gerät, um eine Nachricht zum `dt/client1/sensor` Thema zu veröffentlichen.	Allgemeines AWS
Senden Sie Daten vom Client-Gerät an AWS IoT Core.	Verwenden Sie den MQTT-Client auf Ihrem Gerät, um eine Nachricht zum `dt/client1/sensor` Thema zu veröffentlichen. Abonnieren Sie im MQTT-Test client das Thema, zu dem das Gerät Nachrichten sendet,	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder abonnieren Sie # für alle Themen (siehe Details).	
Senden Sie Nachrichten von AWS IoT Core an Client-Geräte.	Geben Sie auf der Seite MQTT-Testclient auf der Registerkarte In einem Thema veröffentlichen im Feld Themenname den Themennamen Ihrer Nachricht ein. In diesem Beispiel verwenden Sie `cmd/client1` für das Thema.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Fehler beim Serverzertifikat konnte nicht überprüft werden	Dieser Fehler tritt auf, wenn der MQTT-Client das vom MQTT-Broker während des TLS-Handshakes vorgelegte Zertifikat nicht verifizieren kann. Der häufigste Grund ist, dass der MQTT-Client nicht über das CA-Zertifikat verfügt. Gehen Sie wie folgt vor, um sicherzustellen, dass das CA-Zertifikat dem MQTT-Client zur Verfügung gestellt wird. 1. Wenn Sie von Ihrem PC aus Netzwerkzugriff auf das AWS IoT Greengrass-Gerät haben, geben Sie `https://<device IP>:8883` in ein Browserfenster ein, um das MQTT-Brokerzertifikat und das CA-Zertifikat anzuzeigen. Sie können das CA-Zertifikat auch auf dem Client-Gerät speichern.

Problem	Lösung

	Alternativ können Sie die OpenSSL-B efehlszeile verwenden:
	
	`openssl s_client -showcerts -connect <device IP>:8883`
	
	2. Speichern Sie den Inhalt der Zertifikate der Moquette CA und der Greengrass Core CA in Dateien und zeigen Sie dann den dekodierten Inhalt mit dem Befehl an:
	
	`openssl x509 -in <Name of CA>.pem -text`
	
	Das Moquette-CA-Zertifikat sollte das SAN-Feld wie in diesem Beispiel anzeigen:
	
	`X509v3 Subject Alternative Name: IP Address:XXX.XXX.XXX.XXX, IP Address:127.0.0.1, DNS:localhost`

Problem	Lösung
Fehler beim Servernamen konnte nicht überprüft werden	Dieser Fehler tritt auf, wenn der MQTT-Client nicht überprüfen kann, ob er eine Verbindun g zum richtigen Server herstellt. Der häufigste Grund ist, dass die IP-Adresse des Greengras s-Geräts nicht im SAN-Feld des Zertifikats aufgeführt ist. Befolgen Sie die Anweisungen in der vorherige n Lösung, um das MQTT-Brokerzertifikat zu erhalten und zu überprüfen, ob das SAN-Feld die IP-Adresse des AWS IoT Greengrass-Geräts enthält, wie im Abschnitt Zusätzliche Informationen erläutert. Wenn nicht, überprüfe n Sie, ob die IP-Detektorkomponente korrekt installiert ist, und starten Sie das Core-Gerät neu.
Der Servername kann nur überprüft werden, wenn eine Verbindung von einem eingebetteten Client-Gerät hergestellt wird	Mbed TLS, eine beliebte TLS-Bibliothek, die in eingebetteten Geräten verwendet wird, unterstützt derzeit die DNS-Namenüberprüfung nur im SAN-Feld des Zertifikats, wie im Code der Mbed-TLS-Bibliothek gezeigt. Da das Core-Gerät keinen eigenen Domänennamen hat und von der IP-Adresse abhängt, schlagen TLS-Clients, die Mbed TLS verwenden, die Verifizierung des Servernamens während des TLS-Handshakes fehl und verursachen einen Verbindungsfehler. Wir empfehlen Ihnen, die Überprüfung der SAN-IP-Adresse zu Ihrer Mbed-TLS-Bibliothek in der Funktion x509_crt_ check_san hinzuzufügen.

Zugehörige Ressourcen

- AWS IoT Greengrass-Dokumentation
- AWS IoT Core-Dokumentation
- MQTT-Brokerkomponente
- MQTT-Bridge-Komponente
- Komponente für die Client-Geräteauthentifizierung
- IP-Detektorkomponente
- AWS IoT Device SDKs
- Implementieren lokaler Client-Geräte mit AWS IoT Greengrass (AWS-Blogbeitrag)
- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)-Profil

Zusätzliche Informationen

Dieser Abschnitt enthält zusätzliche Informationen zur Kommunikation zwischen den Client-Geräten und dem Core-Gerät.

Der MQTT-Broker überwacht Port 8883 auf dem Core-Gerät auf einen TLS-Client-Verbindungsversuch. Die folgende Abbildung zeigt ein Beispiel für das Serverzertifikat des MQTT-Brokers.

Das Beispielzertifikat zeigt die folgenden Details an:

- Das Zertifikat wird von der AWS IoT Greengrass Core CA ausgestellt, die lokal und spezifisch für das Core-Gerät ist, d. h. es fungiert als lokale CA.
- Dieses Zertifikat wird automatisch jede Woche von der Client-Authentifizierungskomponente gedreht, wie in der folgenden Abbildung gezeigt. Sie können dieses Intervall in der Konfiguration der Client-Authentifizierungskomponente festlegen.

- Der Subject Alternative Name (SAN) spielt eine kritische Rolle bei der Überprüfung des Servernamens auf dem TLS-Client-Ende. Es hilft dem TLS-Client sicherzustellen, dass er eine

Verbindung zum richtigen Server herstellt, und trägt dazu bei, man-in-the-middle Angriffe während der Einrichtung der TLS-Sitzung zu vermeiden. Im Beispielzertifikat gibt das SAN-Feld an, dass dieser Server localhost (den lokalen Unix-Domain-Socket) überwacht und die Netzwerkschnittstelle die IP-Adresse 192.168.1.12 hat.

Der TLS-Client verwendet das SAN-Feld im Zertifikat, um zu überprüfen, ob er während der Serververifizierung eine Verbindung zu einem legitimen Server herstellt. Im Gegensatz dazu wird bei einem typischen TLS-Handshake zwischen einem HTTP-Server und einem Browser der Domänenname im Common Name (CN)-Feld oder SAN-Feld verwendet, um die Domäne, mit der der Browser während des Serververifizierungsprozesses tatsächlich eine Verbindung herstellt, gegenzuprüfen. Wenn das Core-Gerät keinen Domänennamen hat, dient die im SAN-Feld enthaltene IP-Adresse demselben Zweck. Weitere Informationen finden Sie im Abschnitt Alternative Antragstellername von RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile .

Die IP-Detektorkomponente in AWS IoT Greengrass stellt sicher, dass die richtigen IP-Adressen im SAN-Feld des Zertifikats enthalten sind.

Das Zertifikat im Beispiel wird von dem AWS IoT Greengrass-Gerät signiert, das als lokale Zertifizierungsstelle fungiert. Der TLS-Client (MQTT-Client) kennt diese CA nicht, daher müssen wir ein CA-Zertifikat bereitstellen, das wie folgt aussieht.

Mehr Muster

- Kostengünstige Aufnahme von IoT-Daten direkt in Amazon S3 mit AWS IoT Greengrass

Maschinelles Lernen und KI

Themen

Aggregieren von Daten in Amazon DynamoDB für ML-Prognosen in Athena

Erstellt von Putin Doshi (AWS) und Bolnar (AWS)

Code-Repository: Verwenden Sie ML-Vorhersagen für Amazon-DynamoDB-Daten mit Amazon Athena ML	Umgebung: Produktion	Technologien: Machine Learning und KI; Datenbanken; Serverless
Workload: Open-Source	AWS-Services: Amazon Athena ; Amazon DynamoDB ; AWS Lambda ; Amazon SageMaker; Amazon QuickSight	

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe von Amazon Athena komplexe Aggregationen von Internet of Things (IoT)-Daten in einer Amazon-DynamoDB-Tabelle erstellen. Sie erfahren auch, wie Sie die Daten mit Machine Learning (ML)-Inferenz mithilfe von Amazon SageMaker und wie Sie Geodaten mithilfe von Athena abfragen. Sie können dieses Muster als Grundlage für die Erstellung einer ML-Prognoselösung verwenden, die den Anforderungen Ihrer Organisation entspricht.

Zu Demonstrationszwecken verwendet dieses Muster ein Beispielszenario eines Unternehmens, das ein Scooter-Snapshare betreibt und die optimale Anzahl von Scootern vorhersagen möchte, die für Kunden in verschiedenen Bol bereitgestellt werden müssen. Das Unternehmen verwendet ein vortrainiertes ML-Modell, das den Kundenbedarf für die nächste Stunde auf der Grundlage der letzten vier Stunden vorhersagt. Im Szenario wird ein öffentlicher Datensatz des Office of Civic Innovation & Technology für die verwendet. Die Ressourcen für dieses Szenario sind in einem GitHub Repository verfügbar.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto

- Berechtigungen zum Erstellen eines AWS- CloudFormation Stacks mit AWS Identity and Access Management (IAM)-Rollen für Folgendes:
  - Amazon Simple Storage Service (Amazon S3)-Bucket
  - Athena
  - DynamoDB
  - SageMaker
  - AWS Lambda

Architektur

Technologie-Stack

- Amazon QuickSight
- Amazon S3
- Athena
- DynamoDB
- Lambda
- SageMaker

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur zum Erstellen komplexer Datenaggregationen in DynamoDB mithilfe der Abfragefunktionen von Athena, einer Lambda-Funktion, Amazon S3-Speicher, eines SageMaker Endpunkts und eines QuickSight Dashboards.

Das Diagramm zeigt den folgenden Workflow:

1. Eine DynamoDB-Tabelle nimmt IoT-Daten auf, die aus einer Flotte von Scootern übertragen werden.
2. Eine Lambda-Funktion lädt die DynamoDB-Tabelle mit den aufgenommenen Daten.
3. Eine Athena-Abfrage erstellt eine neue DynamoDB-Tabelle für die Geodaten, die die Bol-Nachbarschaften darstellt.
4. Der Abfragespeicherort wird in einem S3-Bucket gespeichert.

5. Eine Athena-Funktion fragt die ML-Inferenz von dem SageMaker Endpunkt ab, der das vortrainierte ML-Modell hostet.
6. Athena fragt Daten direkt aus den DynamoDB-Tabellen ab und aggregiert die Daten für die Analyse.
7. Ein Benutzer zeigt die Ausgabe der analysierten Daten in einem QuickSight Dashboard an.

Tools

AWS-Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon SageMaker ist ein verwalteter ML-Service, mit dem Sie ML-Modelle erstellen und trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitstellen können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon QuickSight ist ein Cloud-Scale Business Intelligence (BI)-Service, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

Code

Der Code für dieses Muster ist im GitHub ML-Vorhersagen für Amazon-DynamoDB-Daten mit Amazon Athena-ML-Repository verwenden verfügbar. Sie können die CloudFormation Vorlage aus dem Repository verwenden, um die folgenden Ressourcen zu erstellen, die im Beispielszenario verwendet werden:

- Eine DynamoDB-Tabelle
- Eine Lambda-Funktion zum Laden der Tabelle mit relevanten Daten
- Ein SageMaker Endpunkt für Inferenzanforderungen mit dem vortrainierten XGBoost-Modell, das in Amazon S3 gespeichert ist

- Eine Athena-Arbeitsgruppe mit dem Namen`V2EngineWorkGroup`
- Benannte Athena-Abfragen, um die Geodaten-Shapefiles nachzuschlagen und den Bedarf an Scootern vorherzusagen
- Ein vorgefertigter Amazon Athena DynamoDB-Konnektor, der es Athena ermöglicht, mit DynamoDB zu kommunizieren, und AWS Serverless Application Model (AWS SAM) verwendet, um die Anwendung in Bezug auf den DynamoDB-Konnektor zu erstellen

Polen

Abrufen des Beispieldatensatzes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Datensatz und die Ressourcen herunter.	1. Laden Sie einen öffentlichen Datensatz mit Dockless-Autoverleih herunter. Zu Demozwecken werden diese Daten im Rahmen des Anwendungsfalls bereits in DynamoDB ausgefüllt, aber in einer Produktionsumgebung senden Sie diese Daten über verschiedene Mechanismen wie IoT-Geräte oder Amazon KinesisKonsumenten an DynamoDB. Diese Mechanismen verwenden Lambda, um Daten in DynamoDB einzufügen. 2. Laden Sie die GIS-Shapefiles herunter, die die Grenzen historischer und kultureller Bereiche innerhalb der Stadt Bol	App-Entwickler, Datenwissenschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bol, , darstellen. Der öffentliche Datensatz wird vom Louis Bol und Bolerson Bol, Informati on Consortium, bereitges tellt. Die ursprünglichen Shapefiles sind bereits in eine Textdatei konvertie rt, die Sie mit Athena abfragen können. Sie finden jedoch den Python-Co de für die Transformation von Shapefiles im Jupyter-Notebook unter Geo-Spatial Processing of GIS Shapefile s with Amazon Athena in GitHub. 3. Laden Sie den vortraini erten Python-Code herunter, der das ML-Modell mithilfe von SageMaker und Athena für stündliche Prognosen trainiert. 4. Rufen Sie die SQL-Abfra ge in Athena ab, die alles zusammenfasst, um Live-Vorhersagen aus den in DynamoDB gespeicherten Daten zu erhalten. 5. (Optional) Verwenden Sie , QuickSight um Geodaten über eine Karte von Bol, Kentucky, zu visualisi	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eren.https://data.lojic.org/datasets/LOJIC::louisville-ky-hud-grant-neighborhoods-from-1979-urban-neighborhoods/explore	

Verwenden einer CloudFormation Vorlage zum Bereitstellen der erforderlichen Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CloudFormation Stack.	1. Laden Sie die CloudFormation Vorlage aus dem GitHub Repository herunter. 2. Melden Sie sich bei der AWS-Managementkonsole an und wählen Sie dann aus`us-east-1` . Hinweis: Das ML-Modell wird in der Amazon Elastic Container Registry (Amazon ECR) für die `us-east-1` AWS-Region gespeichert, aber das Muster ist regionsunabhängig. Sie können das Muster in jeder Region replizieren, in der die in diesem Muster verwendeten AWS-Services unterstützt werden. 3. Öffnen Sie die CloudFormation -Konsole und wählen Sie dann im Navigationsbereich Stacks aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Stack erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren) aus. 5. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 6. Wählen Sie im Abschnitt Vorlage angeben für Vorlagenquelle die Option Vorlagendatei hochladen aus. 7. Wählen Sie Datei und dann die CloudFormation Vorlage aus, die Sie zuvor heruntergeladen haben. 8. Wählen Sie Weiter, akzeptieren Sie die Standardparameterwerte und wählen Sie Weiter, um den Rest des Einrichtungsassistenten zu durchlaufen. 9. Aktivieren Sie das Kontrollkästchen Ich bestätige, dass AWS möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen CloudFormation erstellt. 10. Wählen Sie Stack erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Es kann 15–20 Minuten dauern, bis der CloudFormation Stack diese Ressourcen erstellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CloudFormation Bereitstellung.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Beispieldaten aus der CloudFormation Vorlage in DynamoDB geladen wurden: 1. Öffnen Sie die DynamoDB-Konsole und wählen Sie dann im Navigationsbereich Tabellen aus. 2. Suchen Sie im Abschnitt Tabellen nach der `DynamoDBTableDocklessVehicles` Tabelle. 3. Nachdem die Ressourcenerstellung abgeschlossen ist, öffnen Sie die Athena-Konsole und wählen Sie dann im Navigationsbereich Arbeitsgruppen aus. 4. Wählen Sie die `V2EngineWorkGroup` Arbeitsgruppe und dann Arbeitsgruppe wechseln aus. 5. Wenn Sie eine Aufforderung zum Speichern des Speicherorts des Abfrageergebnisses erhalten, wählen Sie einen Amazon S3-Speicherort aus, an dem Sie über Schreibberechtigungen verfügen. 6. Wählen Sie Speichern.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie im Navigationsbereich Abfrage-Editor und dann die `athena-ml-db-<your-AWS-account-number>` Datenbank aus.	

Laden von Geolocation-Dateien in Athena

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Athena-Tabelle mit Geodaten.	Gehen Sie wie folgt vor, um die Geolocation-Dateien in Athena zu laden: 1. Öffnen Sie die Athena-Konsole und wählen Sie dann im Navigationsbereich Abfrage-Editor aus. 2. Wählen Sie die Registerkarte Gespeicherte Abfragen aus. 3. Suchen Sie nach Q1: Neighbor Bols und wählen Sie es aus. 4. Um zum Abfrage-Editor zurückzukehren, wählen Sie die Registerkarte Editor. 5. Wählen Sie Ausführen aus. Dadurch wird eine Tabelle mit dem Namen `louisville_ky_neighborhoods` in Ihrer Datenbank erstellt. Stellen Sie sicher,	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dass die Tabelle in der `athena-ml-db-<your-AWS-account-number>` Datenbank erstellt wurde. Die Abfrage erstellt eine neue Tabelle für die Geodaten, die die Bol-Nachbarschaften darstellt. Die Datentabelle wird aus GIS-Shapefiles erstellt. Die `CREATE EXTERNAL TABLE` Anweisung definiert das Schema der Tabelle sowie den Speicherort und das Format der zugrunde liegenden Datendatei. Den Python-Code zum Verarbeiten von Shapefiles und zum Erstellen dieser Tabelle finden Sie unterGeo-Spatial Processing of GIS Shapefiles with Amazon Athena in AWS Samples. Detaillierter SQL-Code finden Sie unter create_neighborhood_table.sql auf GitHub.	

Prognostizieren der Nachfrage nach Scootern nach Nachbarschaft aus den aggregierten DynamoDB-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deklarieren Sie eine Funktion in Athena, um abzufragen SageMaker.	1. Öffnen Sie die Athena-Konsole, wählen Sie im Navigationsbereich Abfrage-Editor und dann die Registerkarte Editor aus. 2. Kopieren Sie die folgende SQL-Anweisung und fügen Sie sie in den Abfrage-Editor ein: `USING EXTERNAL FUNCTION predict_demand ( location_id BIGINT, hr BIGINT , dow BIGINT, n_pickup_1 BIGINT, n_pickup_2 BIGINT, n_pickup_3 BIGINT, n_pickup_4 BIGINT, n_dropoff_1 BIGINT, n_dropoff_2 BIGINT, n_dropoff_3 BIGINT, n_dropoff_4 BIGINT ) RETURNS DOUBLE SAGEMAKER '<Your SageMaker endpoint>'` Der erste Teil der SQL-Anweisung deklariert die externe Funktion zum Abfragen von ML-Inferenzen von dem SageMaker Endpunkt, der das vortrainierte Modell hostet.	Datenwissenschaftler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie dann die folgenden Schritte aus: 1. Definieren Sie die Reihenfolge und den Typ der Eingabeparameter und den Typ der Rückgabewerte. 2. Wählen Sie Ausführen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Prognostizieren Sie die Nachfrage nach Scootern nach den aggregierten DynamoDB-Daten.	Jetzt können Sie Athena verwenden, um Transakti onsdaten direkt von DynamoDB abzufragen und die Daten dann für Analysen und Prognosen zu aggregier en. Dies lässt sich nicht leicht erreichen, indem eine DynamoDB-NoSQL-Dat enbank direkt abgefragt wird. 1. Öffnen Sie die Athena-Ko nsole und wählen Sie dann im Navigationsbereich den Abfrage-Editor aus. 2. Wählen Sie die Registerk arte Gespeicherte Abfragen aus. 3. Suchen Sie nach Q2: DynamoDBAthenaMLSc ooterPredict und wählen Sie es aus. 4. Um zum Abfrage-Editor zurückzukehren, wählen Sie die Registerkarte Editor. 5. Wählen Sie Ausführen aus. Die SQL-Anweisung führt Folgendes aus: • Verwendet eine Athena-Verbundabfrage, um die DynamoDB-Tabelle mit den Rohdaten abzufragen	App-Entwickler, Datenwiss enschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Platziert geografische Koordinaten mithilfe der Geodatenfunktionen von Athena in Nachbarschaften • Anreicherung von Daten mit ML-Inferenz mithilfe von SageMaker Informationen zur Verwendung von SQL zum Aggregieren von DynamoDB-Daten und SageMaker Inferenzdaten in Athena finden Sie unter athena_long.sql in GitHub.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ausgabe.	Die Ausgabetabelle enthält die Nachbarschaft, den Längengrad und den Breitengrad des Schwerpunkts der Nachbarschaft. Sie enthält auch die Anzahl der Fahrzeuge, die für die nächste Stunde vorhergesagt werden. Die Abfrage erstellt die Vorhersagen für einen ausgewählten Zeitpunkt . Sie können jederzeit Vorhersagen treffen, indem Sie den Ausdruck `TIMESTAMP '2019-09-07 15:00'` überall in der Anweisung ändern. Wenn Sie einen Echtzeit-Daten-Feed in Ihrer DynamoDB-Tabelle haben, ändern Sie den Zeitstempel in `NOW()`.	App-Entwickler, Datenwissenschaftler

Bereinigen der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie Ressourcen.	1. Öffnen Sie die Athena-Konsole und leeren Sie den Bucket, den Sie als Teil des CloudFormation Stacks erstellt haben.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen Sie die CloudFormation -Konsole und löschen Sie dann den Stack mit dem Namen `bdb-1462-athena-dynamodb-ml-stack` . 3. Öffnen Sie die Amazon-CloudWatch Konsole und löschen Sie dann die Protokollgruppe mit dem Namen `/aws/sagemaker/Endpoints/Sg-athena-ml-dynamodb-model-endpoint` .	

Zugehörige Ressourcen

- Amazon Athena Query Federation SDK (GitHub)
- Abfragen von Geodaten (Amazon Athena-Benutzerhandbuch)
- Verwenden von ML-Vorhersagen über Amazon-DynamoDB-Daten mit Amazon Athena ML (AWS Big Data Blog)
- Amazon ElastiCache for Redis (AWS-Dokumentation)
- Amazon Neptune (AWS-Dokumentation)

Zuordnen eines AWS- CodeCommit Repositorys in einem AWS-Konto zu SageMaker Studio in einem anderen Konto

Erstellt von Bols Van der Maas (AWS) und Aubrey Oosthuizen (AWS)

Umgebung: Produktion	Technologien: Machine Learning und KI DevOps; Sicherheit, Identität, Compliance; Cloudnativ	AWS-Services: AWS CodeCommit; Amazon SageMaker; AWS Identity and Access Management

Übersicht

Dieses Muster enthält Anweisungen und Code zum Zuordnen eines AWS- CodeCommit Repositorys in einem AWS-Konto (Konto A) zu Amazon SageMaker Studio in einem anderen AWS-Konto (Konto B). Um die Zuordnung einzurichten, müssen Sie eine AWS Identity and Access Management (IAM)-Richtlinie und -Rolle in Konto A und eine IAM-Inline-Richtlinie in Konto B erstellen. Anschließend verwenden Sie ein Shell-Skript, um das CodeCommit Repository von Konto A zu SageMaker Studio in Konto B zu klonen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei AWS-Konten, eines mit dem CodeCommit Repository und das andere mit einer SageMaker Domain mit einem Benutzer
- Bereitgestellte SageMaker Domain und Benutzer mit Internetzugriff oder Zugriff auf CodeCommit und AWS Security Token Service (AWS STS) über Virtual Private Network (VPC)-Endpunkte
- Ein grundlegendes Verständnis von IAM
- Ein grundlegendes Verständnis von SageMaker Studio
- Ein grundlegendes Verständnis von Git und CodeCommit

Einschränkungen

Dieses Muster gilt nur für SageMaker Studio, nicht für RStudio auf Amazon SageMaker.

Architektur

Technologie-Stack

- Amazon SageMaker
- Amazon SageMaker Studio
- AWS CodeCommit
- AWS Identity and Access Management (IAM)
- Git

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur, die ein CodeCommit Repository von Konto A mit SageMaker Studio in Konto B verknüpft.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer übernimmt die `MyCrossAccountRepositoryContributorRole` Rolle in Konto A über die `sts:AssumeRole` Rolle, während er die SageMaker Ausführungsrolle in SageMaker Studio in Konto B verwendet. Die angenommene Rolle enthält die CodeCommit Berechtigungen zum Klonen und Interagieren mit dem angegebenen Repository.
2. Der Benutzer führt Git-Befehle vom System-Terminal in SageMaker Studio aus.

Automatisierung und Skalierung

Dieses Muster besteht aus manuellen Schritten, die mithilfe des AWS Cloud Development Kit (AWS CDK) ,AWS CloudFormation oder Terraform automatisiert werden können.

Tools

AWS-Tools

- Amazon SageMaker ist ein verwalteter Machine Learning (ML)-Service, mit dem Sie ML-Modelle erstellen und trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitstellen können.

- Amazon SageMaker Studio ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für Machine Learning, mit der Sie Ihre Machine-Learning-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.

Andere Tools

- Git ist ein verteiltes Versionskontrollsystem zur Verfolgung von Änderungen am Quellcode während der Softwareentwicklung.

Polen

Erstellen einer IAM-Richtlinie und einer IAM-Rolle in Konto A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie für den Repository-Zugriff in Konto A.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Policies (Richtlinien) und dann Create policy (Richtlinie erstellen). 3. Wählen Sie den Tab JSON. 4. Kopieren Sie die Richtlinienanweisung aus Beispiel-IAM-Richtlinie im Abschnitt Zusätzliche Informationen dieses Musters und fügen Sie die Anweisung dann	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in den JSON-Editor ein. Stellen Sie sicher, dass Sie alle Platzhalterwerte in der Richtlinie ersetzen. 5. Wählen Sie Next:Tags und dann Next:Review aus. 6. Geben Sie unter Name einen Namen für die Richtlinie ein. Hinweis: In diesem Muster wird die IAM-Richtlinie als bezeichnet`CrossAccountAccessForMySharedDemoRepo` , aber Sie können den von Ihnen bevorzugten Richtlinennamen auswählen. 7. Wählen Sie Richtlinie erstellen aus. Tipp: Es hat sich bewährt, den Umfang Ihrer IAM-Richtlinien auf die für Ihren Anwendungsfall mindestens erforderlichen Berechtigungen zu beschränken.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den Repository-Zugriff in Konto A.	1. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen und dann Rolle erstellen aus. 2. Wählen Sie für Vertrauenswürdiger Entitätstyp die Option AWS-Konto aus. 3. Wählen Sie im Abschnitt AWS-Konto die Option Ein anderes AWS-Konto aus. 4. Geben Sie für Konto-ID die Konto-ID für Konto B ein. 5. Suchen Sie auf der Seite Berechtigungen hinzufügen nach der `CrossAccountAccessForMySharedDemoRepo` Richtlinie, die Sie zuvor erstellt haben, und wählen Sie sie aus. 6. Wählen Sie Weiter aus. 7. Geben Sie in Role name (Name der Rolle) einen Namen ein. Hinweis: In diesem Muster wird der IAM-Rollenname als bezeichnet`MyCrossAccountRepositoryContributorRole` , aber Sie können den gewünschten Rollennamen auswählen. 8. Wählen Sie Rolle erstellen und kopieren Sie dann den	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-Ressourcennamen (ARN) der neuen Rolle.	

Erstellen einer IAM-Inline-Richtlinie in Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Ausführungsrolle, die Ihrem SageMaker Domain-Benutzer in Konto B zugeordnet ist, eine Inline-Richtlinie an.	1. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen aus. 2. Suchen Sie in Konto B nach der Ausführungsrolle, die Ihrem SageMaker Domain-Benutzer zugeordnet ist, und wählen Sie sie aus. 3. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus. 4. Wählen Sie den Tab JSON. 5. Kopieren Sie die folgende Richtlinienanweisung und fügen Sie sie dann in den JSON-Editor ein. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole",`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Resource": "arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>"
	}
	]
	}</pre>
	6. Ersetzen Sie<Account_A_ID> durch die Konto-ID für Konto A. Ersetzen Sie <Account_A_Role_Name> durch den Namen der IAM-Rolle, die Sie zuvor erstellt haben.
	7. Wählen Sie Richtlinie prüfen.
	8. Geben Sie unter Name einen Namen für Ihre Inline-Richtlinie ein.
	9. Wählen Sie Richtlinie erstellen aus.	

Klonen des Repositorys in SageMaker Studio für Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Shell-Skript in SageMaker Studio in Konto B.	1. Wählen Sie im Navigationsbereich der SageMaker Konsole Studio aus. 2. Wählen Sie Ihr Benutzerprofil und dann Open Studio aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie im Abschnitt Home die Option Open Launcher aus. 4. Wählen Sie im Abschnitt Dienstprogramme und Dateien die Option Textdatei aus. 5. Kopieren Sie das Skript aus Beispiel- SageMaker Shell-Skript im Abschnitt Zusätzliche Informationen dieses Musters und fügen Sie dann die Anweisung in die neue Datei ein. Stellen Sie sicher, dass Sie alle Platzhalterwerte im Skript ersetzen. 6. Klicken Sie mit der rechten Maustaste auf die Registerkarte untitled.txt Ihrer neuen Datei und wählen Sie dann Text umbenennen aus. Geben Sie für Neuer Name cross_account_git_clone.sh ein und wählen Sie dann Umbenennen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das Shell-Skript vom System-Terminal aus auf.	1. Wählen Sie im Abschnitt Home der SageMaker Konsole Open Launcher aus. 2. Wählen Sie im Abschnitt Dienstprogramme und Dateien die Option Systemterminal aus. 3. Führen Sie im Terminal den folgenden Befehl aus: `chmod u+x ./cross_account_git_clone.sh && ./cross_account_git_clone.sh` Sie haben Ihr CodeCommit Repository in einem kontoüber greifenden SageMaker Studio geklont. Sie können jetzt alle Git-Befehle vom System-Terminal aus ausführen.	AWS DevOps

Zusätzliche Informationen

Beispiel für eine IAM-Richtlinie

Wenn Sie diese Beispielrichtlinie verwenden, gehen Sie wie folgt vor:

- Ersetzen Sie durch `<CodeCommit_Repository_Region>` die AWS-Region für das Repository.
- Ersetzen Sie durch `<Account_A_ID>` die Konto-ID für Konto A.
- Ersetzen Sie `<CodeCommit_Repository_Name>` durch den Namen Ihres CodeCommit Repositorys in Konto A.

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "codecommit:BatchGet*",
            "codecommit:Create*",
            "codecommit:DeleteBranch",
            "codecommit:Get*",
            "codecommit:List*",
            "codecommit:Describe*",
            "codecommit:Put*",
            "codecommit:Post*",
            "codecommit:Merge*",
            "codecommit:Test*",
            "codecommit:Update*",
            "codecommit:GitPull",
            "codecommit:GitPush"
        ],
        "Resource": [

 "arn:aws:codecommit:<CodeCommit_Repository_Region>:<Account_A_ID>:<CodeCommit_Repository_Name>
        ]
    }
]
}
```

Beispiel für ein SageMaker Shell-Skript

Wenn Sie dieses Beispielskript verwenden, gehen Sie wie folgt vor:

- Ersetzen Sie <Account_A_ID>durch die Konto-ID für Konto A.
- Ersetzen Sie durch <Account_A_Role_Name>den Namen der IAM-Rolle, die Sie zuvor erstellt haben.
- Ersetzen Sie durch <CodeCommit_Repository_Region>die AWS-Region für das Repository.
- Ersetzen Sie <CodeCommit_Repository_Name>durch den Namen Ihres CodeCommit Repositorys in Konto A.

```
#!/usr/bin/env bash
```

```
#Launch from system terminal
pip install --quiet git-remote-codecommit

mkdir -p ~/.aws
touch ~/.aws/config

echo "[profile CrossAccountAccessProfile]
region = <CodeCommit_Repository_Region>
credential_source=EcsContainer
role_arn = arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>
output = json" > ~/.aws/config

echo '[credential "https://git-
codecommit.<CodeCommit_Repository_Region>.amazonaws.com"]
        helper = !aws codecommit credential-helper $@ --profile
 CrossAccountAccessProfile
        UseHttpPath = true' > ~/.gitconfig

git clone codecommit::<CodeCommit_Repository_Region>://
CrossAccountAccessProfile@<CodeCommit_Repository_Name>
```

Automatisieren Sie das Training und die Bereitstellung von Amazon Lookout for Vision zur Erkennung von Anomalien

Erstellt von Bolwallner (AWS), GaBriel Bolriguez GarSpeed (AWS), Kangkang Wang (AWS), Shukhrat Khodjaev (AWS), Sanjay Ashok (AWS), Yassineafouri (AWS) und GaBriel Zylka (AWS)

Code-Repository: automated-silicon-wafer-anomaly-detection-using-amazon-lookout--for-vision	Umgebung: Produktion	Technologien: Machine Learning und KI; Cloudnativ; DevOps
AWS-Services: AWS CloudFormation; AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; AWS Lambda ; Amazon Lookout for Vision		

Übersicht

Dieses Muster hilft Ihnen, das Training und die Bereitstellung von Machine-Learning-Modellen von Amazon Lookout for Vision für die visuelle Überprüfung zu automatisieren. Obwohl sich dieses Muster auf die Anomalieerkennung für Silicon-Wafers konzentriert, können Sie die Lösung für die Verwendung in einer Vielzahl von Produkten und Branchen anpassen.

Im Jahr 2020 hat die Jahreskapazität eines der größten Telefoniehersteller der Welt 12 Millionen gleichwertige Wafer im 12-Pol-Bereich überschritten. Um die Qualität und Zuverlässigkeit dieser Wafer zu gewährleisten, ist die visuelle Überprüfung ein wesentlicher Schritt im Produktionsprozess. Die herkömmlichen Methoden der visuellen Prüfung, wie manuelles Sampling oder die Verwendung veralteter, älterer Tools, die auf statistischen Maßnahmen basieren, können zeitaufwändig und ineffizient sein. Angesichts des Umfangs dieses Prozesses und seiner Bedeutung für die breitere Rechtsbranche besteht eine erhebliche Gelegenheit, die visuelle Prüfung mithilfe fortschrittlicher Technologien für künstliche Intelligenz (KI) zu optimieren und zu automatisieren.

Lookout for Vision optimiert den Image- und Objektprüfungsprozess und reduziert so den Bedarf an kostspieliger und inkonsistenter manueller Prüfung. Diese Lösung verbessert die Qualitätskontrolle,

erleichtert eine genaue Bewertung von Fehlern und Beschädigungen und stellt die Einhaltung der Industriestandards sicher. Darüber hinaus können Sie den Überprüfungsprozess von Lookout for Vision automatisieren, ohne spezialisiertes Machine-Learning-Fachwissen.

Mit dieser Lösung können Sie Ihr Computer Vision-Modell in jedes System integrieren. Sie können beispielsweise ein Modell in eine Website integrieren, auf der Benutzer Bilder hochladen und auf Fehler analysieren. Die folgende Abbildung zeigt ein Beispiel für einen Silicon-Wafer mit Scratch-Fehlern aus einem CMP-Prozess (CLI-Snapshoting). Sie können Lookout for Vision verwenden, um diese Anomalien zu erkennen. Lookout for Vision hat beispielsweise Anomalien in diesem Bild mit 99,04 % Zuverlässigkeit erkannt.

Diese Lösung basiert auf dem Code und dem Anwendungsfall, der im Blogbeitrag Erstellen einer ereignisbasierten Tracking-Lösung mit Amazon Lookout for Vision beschrieben wird. Diese Lösung ändert den ursprünglichen Code, um die CI/CD-Pipeline-Automatisierung zu aktivieren und das Open-Source-Python-SDK von Amazon Lookout for Vision () zu integrierenGitHub. Weitere Informationen zum Python SDK finden Sie im Blogbeitrag Erstellen, Trainieren und Bereitstellen von Amazon Lookout for Vision-Modellen mit dem Python SDK.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Administrative Berechtigungen im AWS-Konto
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- AWS-CDK, installiert und konfiguriert
- Python Version 3.10, installiert

Architektur

Zielarchitektur

Diese Architektur veranschaulicht die Automatisierung von Build, Training und Bereitstellung von Amazon Lookout for Vision-Modellen über eine CI/CD-Pipeline. Das Diagramm zeigt den folgenden Workflow:

1. Der Code wird in einem Amazon- CodeCommit Repository gespeichert. Entwickler können den Code ändern, Eingabebilder ändern oder der Automatisierungspipeline andere Schritte hinzufügen.
2. Nach der Bereitstellung der Lösung oder der Aktualisierung des Hauptzweigs des CodeCommit Repositorys überträgt Amazon den Code CodePipeline automatisch an Amazon CodeBuild.
3. CodeBuild verwendet das Lookout for Vision Python SDK, um das Bildklassifizierungsmodell zu trainieren und bereitzustellen. Die für das Training verwendeten Bilder werden in einem Amazon Simple Storage Service (Amazon S3)-Bucket gespeichert. lädt diese Bilder CodeBuild automatisch herunter und speichert sie. Um die Lösung an Ihre Bedürfnisse anzupassen, können Sie Ihre eigenen Bilder importieren.
4. Das Lookout for Vision-Modell wird Endbenutzern über AWS Lambda zur Verfügung gestellt. Sie sind jedoch nicht auf diesen Ansatz beschränkt. Sie können Lookout for Vision auch am Edge auf IoT-Geräten bereitstellen oder als Batch-Prozess auf geplanter Basis ausführen, um Vorhersagen zu generieren.

Tools

AWS-Services

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Lookout for Vision verwendet Computer Vision, um visuelle Erkennungen in Industrieprodukten genau und skalierbar zu finden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Automatisieren von Amazon Lookout for Vision Training und Bereitstellung für die Erkennung von Silicon Wafer Anomalien verfügbar.

Bewährte Methoden

Wenn Sie den Code als Experiment ausführen, stellen Sie sicher, dass Sie Ihren Endpunkt von Amazon Lookout for Vision stoppen.

Epics

Bereitstellen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Repository GitHub Automatisieren der Schulung und Bereitstellung von Amazon Lookout for Vision für die Erkennung von Anomalien in Silicon Wafer auf Ihre lokale Workstation. `git clone https://github.com/aws-samples/automated-silicon-wafer-anomaly-detection-using-amazon-lookout-for-vision.git`	Bash
Erstellen Sie eine virtuelle Umgebung.	Geben Sie den folgenden Befehl ein, um eine virtuelle Umgebung auf Ihrer lokalen Workstation zu erstellen. `python3 -m venv .venv`	Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Abhängigkeiten.	Nachdem die virtuelle Umgebung erstellt wurde, geben Sie den folgenden Befehl ein, um die erforderlichen Abhängigkeiten zu installieren. `pip install -r requirements.txt`	Python
(Nur Linux-Benutzer) Aktivieren Sie die virtuelle Umgebung.	Nachdem die Initialisierung abgeschlossen und die virtuelle Umgebung erstellt wurde, verwenden Sie den folgenden Befehl, um die virtuelle Umgebung zu aktivieren. `source .venv/bin/activate`	Bash
(Nur Windows-Benutzer) Aktivieren Sie die virtuelle Umgebung.	Nachdem die Initialisierung abgeschlossen und die virtuelle Umgebung erstellt wurde, verwenden Sie den folgenden Befehl, um die virtuelle Umgebung zu aktivieren. `.venv\Scripts\activate.bat`	PowerShell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Stack bereit.	1. Geben Sie in der AWS-CDK-CLI den folgenden Befehl ein, um die AWS-CloudFormation Vorlage zu synthetisieren.
	`cdk synth`
	2. Geben Sie den folgenden Befehl ein, um den CloudFormation Stack bereitzustellen.
	`cdk deploy --all --require-approval never`
	Die `--all flag` stellt sicher, dass alle Komponenten gleichzeitig installiert werden. macht es `--require-approval` nie überflüssig, jede Komponentenbereitstellung zu genehmigen.
		AWS-Administrator

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie ein Beispiel für ein Testereignis ein.	1. Öffnen Sie die Seite Funktionen der Lambda-Konsole. 2. Wählen Sie die `amazon-lookout-for-vision-`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`project-lambda` Funktion aus. 3. Wählen Sie die Registerkarte Test. 4. Wählen Sie unter Testereignis die Option Neues Ereignis erstellen aus. 5. Geben Sie Folgendes ein. 6. Wählen Sie Test aus. `{ "tbd": "tbd" }` 7. Erweitern Sie unter Execution result (Ausführungsergebnis) die Option Details, um die Testergebnisse anzuzeigen.	

Zugehörige Ressourcen

AWS-Dokumentation

- Erste Schritte mit Amazon Lookout for Vision
- Erste Schritte mit AWS CDK

AWS-Blogbeiträge

- Erstellen, Trainieren und Bereitstellen von Amazon Lookout for Vision-Modellen mit dem Python SDK
- Erstellen Sie eine ereignisbasierte Tracking-Lösung mit Amazon Lookout for Vision
- Amazon Lookout for Vision Python SDK: Kreuzvalidierung und Integration mit anderen AWS-Services

Automatisches Extrahieren von Inhalten aus PDF-Dateien mit Amazon Textract

Erstellt von Tianxia Jia (AWS)

Umgebung: Produktion	Technologien: Machine Learning und KI; Analytik; Big Data	AWS-Services: Amazon S3; Amazon Textract; Amazon SageMaker

Übersicht

Viele Organisationen müssen Informationen aus PDF-Dateien extrahieren, die in ihre Geschäftsanwendungen hochgeladen werden. Beispielsweise könnte eine Organisation Informationen aus Steuer- oder medizinischen PDF-Dateien zur Steueranalyse oder zur Bearbeitung von medizinischen Ansprüchen präzise extrahieren müssen.

In der Amazon Web Services (AWS) Cloud extrahiert Amazon Textract automatisch Informationen (z. B. gedruckten Text, Formularen und Tabellen) aus PDF-Dateien und erstellt eine JSON-formatierte Datei, die Informationen aus der ursprünglichen PDF-Datei enthält. Sie können Amazon Textract in der AWS-Managementkonsole oder durch die Implementierung von API-Aufrufen verwenden. Wir empfehlen, programmgesteuerte API-Aufrufe zu verwenden, um eine große Anzahl von PDF-Dateien zu skalieren und automatisch zu verarbeiten.

Wenn Amazon Textract eine Datei verarbeitet, erstellt es die folgende Liste von `Block` Objekten: Seiten, Zeilen und Textwörter, Formen (Schlüssel-Wert-Paare), Tabellen und Zellen sowie Auswahlelemente. Andere Objektinformationen sind ebenfalls enthalten, z. B. Begrenzungsrahmen , Konfidenzintervalle, IDs und Beziehungen. Amazon Textract extrahiert die Inhaltsinformationen als Zeichenfolgen. Korrekt identifizierte und transformierte Datenwerte sind erforderlich, da sie einfacher von Ihren Downstream-Anwendungen verwendet werden können.

Dieses Muster beschreibt einen step-by-step Workflow für die Verwendung von Amazon Textract, um Inhalte automatisch aus PDF-Dateien zu extrahieren und in einer sauberen Ausgabe zu verarbeiten. Das Muster verwendet eine Vorlagenabgleichstechnik, um das erforderliche Feld, den Schlüsselnamen und die Tabellen korrekt zu identifizieren, und wendet dann Korrekturen nach der Verarbeitung auf jeden Datentyp an. Sie können dieses Muster verwenden, um verschiedene

Arten von PDF-Dateien zu verarbeiten, und Sie können diesen Workflow dann skalieren und automatisieren, um PDF-Dateien mit einem identischen Format zu verarbeiten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3)-Bucket zum Speichern der PDF-Dateien, nachdem sie zur Verarbeitung durch Amazon Textract in das JPEG-Format konvertiert wurden. Weitere Informationen zu S3-Buckets finden Sie unter Bucket-Übersicht in der Amazon S3-Dokumentation.
- Das `Textract_PostProcessing.ipynb` Jupyter Notebook (angefügt), installiert und konfiguriert. Weitere Informationen zu Jupyter-Notebooks finden Sie unter Erstellen eines Jupyter-Notebooks in der Amazon- SageMaker Dokumentation.
- Vorhandene PDF-Dateien mit einem identischen Format.
- Ein Verständnis von Python.

Einschränkungen

- Ihre PDF-Dateien müssen von guter Qualität und klar lesbar sein. Native PDF-Dateien werden empfohlen, aber Sie können gescannte Dokumente verwenden, die in ein PDF-Format konvertiert werden, wenn alle einzelnen Wörter klar sind. Weitere Informationen dazu finden Sie unter Vorverarbeitung von PDF-Dokumenten mit Amazon Textract: Erkennung und Entfernung von Visualisierungen im AWS Machine Learning Blog.
- Für mehrseitige Dateien können Sie eine asynchrone Operation verwenden oder die PDF-Dateien auf eine einzelne Seite aufteilen und eine synchrone Operation verwenden. Weitere Informationen zu diesen beiden Optionen finden Sie unter Erkennen und Analysieren von Text in mehrseitigen Dokumenten und Erkennen und Analysieren von Text in einseitigen Dokumenten in der Amazon-Textract-Dokumentation.

Architektur

Der Workflow dieses Musters führt zunächst Amazon Textract auf einer Beispiel-PDF-Datei aus (erstmalige Ausführung) und führt es dann auf PDF-Dateien aus, die ein identisches Format wie das erste PDF haben (wiederholte Ausführung). Das folgende Diagramm zeigt den kombinierten

Workflow für Erst- und Wiederholungsausführung, der Inhalte automatisch und wiederholt aus PDF-Dateien mit identischen Formaten extrahiert.

Das Diagramm zeigt den folgenden Workflow für dieses Muster:

1. Konvertieren Sie eine PDF-Datei in das JPEG-Format und speichern Sie sie in einem S3-Bucket.
2. Rufen Sie die Amazon-Textract-API auf und analysieren Sie die Amazon-Textract-Antwort-JSON-Datei.
3. Bearbeiten Sie die JSON-Datei, indem Sie das richtige `KeyName:DataType` Paar für jedes erforderliche Feld hinzufügen. Erstellen Sie eine `TemplateJSON` Datei für die Phase Wiederholen der Ausführung.
4. Definieren Sie die Korrekturfunktionen nach der Verarbeitung für jeden Datentyp (z. B. Float, Ganzzahl und Datum).
5. Bereiten Sie die PDF-Dateien vor, die ein identisches Format wie Ihre erste PDF-Datei haben.
6. Rufen Sie die Amazon-Textract-API auf und analysieren Sie das Amazon-Textract-Antwort-JSON.
7. Ordnen Sie die analysierte JSON-Datei der `TemplateJSON` Datei zu.
8. Implementieren Sie Korrekturen nach der Verarbeitung.

Die endgültige JSON-Ausgabedatei enthält das richtige `KeyName` und `Value` für jedes erforderliche Feld.

Zieltechnologie-Stack

- Amazon SageMaker
- Amazon S3
- Amazon Textract

Automatisierung und Skalierung

Sie können den Workflow „Wiederholungsausführung“ automatisieren, indem Sie eine AWS Lambda-Funktion verwenden, die Amazon Textract initiiert, wenn eine neue PDF-Datei zu Amazon S3 hinzugefügt wird. Amazon Textract führt dann die Verarbeitungsskripts aus und die endgültige Ausgabe kann an einem Speicherort gespeichert werden. Weitere Informationen dazu finden Sie

unter Verwenden eines Amazon S3-Auslösers zum Aufrufen einer Lambda-Funktion in der Lambda-Dokumentation.

Tools

- Amazon SageMaker ist ein vollständig verwalteter ML-Service, mit dem Sie ML-Modelle schnell und einfach erstellen und trainieren und sie dann direkt in einer produktionsbereiten gehosteten Umgebung bereitstellen können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Textract erleichtert das Hinzufügen von Texterkennung und -analyse zu Ihren Anwendungen.

Polen

Erstmalige Ausführung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie die PDF-Datei.	Bereiten Sie die PDF-Datei für Ihre erste Ausführung vor, indem Sie sie in eine einzelne Seite aufteilen und in das JPEG-Format für die synchrone Amazon-Textract-Operation (`Syn API`) konvertieren. Hinweis: Sie können auch die asynchrone Amazon Textract-Operation (`Asyn API`) für mehrseitige PDF-Dateien verwenden.	Datenwissenschaftler, Entwickler
Parsen Sie das Amazon Textract-Antwort-JSON.	Öffnen Sie das `Textract_PostProcessing.ipynb` Jupyter Notebook	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(angefügt) und rufen Sie die Amazon Textract API mit dem folgenden Code auf:
	
	`response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`
	
	Parsen Sie den Antwort-JSON in ein Formular und eine Tabelle, indem Sie den folgenden Code verwenden:
	
	`parseformKV=form_kv_from_JSON(response) parseformTables=get_tables_fromJSON(response)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die TemplateJSON-Datei.	Bearbeiten Sie den analysierten JSON-Code für jede `KeyName` und die entsprechenden Tabellenüberschriften `DataType` (z. B. Zeichenfolge, Gleitkommazahl, Ganzzahl oder Datum) und Tabellenüberschriften (z. B. `ColumnNames` und `RowNames`). Diese Vorlage wird für jeden einzelnen PDF-Dateityp verwendet, was bedeutet, dass die Vorlage für PDF-Dateien mit einem identischen Format wiederverwendet werden kann.	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Korrektur funktionen nach der Verarbeit ung.	Die Werte in der Antwort von Amazon Textract für die `TemplateJSON` Datei sind Zeichenfolgen. Für Datum, Gleitkommazahl, Ganzzahl oder Währung gibt es keine Abhilfe. Diese Werte müssen in den richtigen Datentyp für Ihren nachgelagerten Anwendungsfall konvertiert werden. Korrigieren Sie jeden Datentyp entsprechend der `TemplateJSON` Datei mithilfe des folgenden Codes: `finalJSON=postprocessingCorrection(parsedJSON,templateJSON)`	Datenwissenschaftler, Entwickler

Wiederholen der Ausführung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die PDF-Dateien vor.	Bereiten Sie die PDF-Dateien vor, indem Sie sie in eine einzelne Seite aufteilen und sie für die synchrone Amazon-Textract-Operation in das JPEG-Format konvertieren (`Syn API`).	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Sie können auch die asynchrone Amazon Textract-Operation (`Asyn API`) für mehrseitige PDF-Dateien verwenden.	
Rufen Sie die Amazon Textract API auf.	Rufen Sie die Amazon Textract API mit dem folgenden Code auf: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`	Datenwissenschaftler, Entwickler
Parsen Sie das Amazon Textract-Antwort-JSON.	Parsen Sie den Antwort-JSON in ein Formular und eine Tabelle, indem Sie den folgenden Code verwenden: `parseformKV=form_kv_from_JSON(response) parseformTables=get_tables_fromJSON(response)`	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die TemplateJSON-Datei und ordnen Sie sie dem analysierten JSON-Code zu.	Verwenden Sie die `-TemplateJSON` Datei, um die richtigen Schlüssel-Wert-Paare und die richtige Tabelle mit den folgenden Befehlen zu extrahieren: `form_kv_corrected= form_kv_correction (parseformKV,templ ateJSON) form_table_correct ed=form_Table_corr ection(parseformTa bles, templateJSON) form_kv_table_correcte d_final={**form_kv _corrected , **form_ta ble_corrected}`	Datenwissenschaftler, Entwickler
Korrekturen nach der Verarbeitung.	Verwenden Sie `DataType` in der `TemplateJSON` Datei und den Nachverarbeitungsf unktionen, um Daten mithilfe des folgenden Codes zu korrigieren: `finalJSON=postproc essingCorrection(f orm_kv_table_corre cted_final,templat eJSON)`	Datenwissenschaftler, Entwickler

Zugehörige Ressourcen

- Automatisches Extrahieren von Text und strukturierten Daten aus Dokumenten mit Amazon Textract
- Extrahieren von Text und strukturierten Daten mit Amazon Textract
- Amazon-Textract-Ressourcen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie einen MLOps-Workflow mithilfe von Amazon SageMaker und Azure DevOps

Erstellt von Deepika Kumar (AWS) und Sara van de Moosdijk (AWS)

Umwelt: Produktion	Technologien: Maschinelles Lernen und KI DevOps; Betrieb	Arbeitslast: Microsoft
AWS-Dienste: Amazon API Gateway; Amazon ECR; Amazon EventBridge; AWS Lambda; Amazon SageMaker		

Übersicht

Machine Learning Operations (MLOps) besteht aus einer Reihe von Verfahren zur Automatisierung und Vereinfachung von Workflows und Bereitstellungen für maschinelles Lernen (ML). MLOps konzentriert sich auf die Automatisierung des ML-Lebenszyklus. Es trägt dazu bei, dass Modelle nicht nur entwickelt, sondern auch systematisch und wiederholt eingesetzt, überwacht und neu trainiert werden. Es bringt DevOps Prinzipien in das maschinelle Lernen. MLOps führt zu einer schnelleren Bereitstellung von ML-Modellen, einer höheren Genauigkeit im Laufe der Zeit und einer stärkeren Gewissheit, dass sie einen echten Geschäftswert bieten.

Organizations verfügen häufig bereits über DevOps Tools und Datenspeicherlösungen, bevor sie mit MLOps beginnen. Dieses Muster zeigt, wie die Stärken von Microsoft Azure und AWS genutzt werden können. Es hilft Ihnen bei der Integration von Azure DevOps in Amazon SageMaker , um einen MLOps-Workflow zu erstellen.

Die Lösung vereinfacht die Arbeit zwischen Azure und AWS. Sie können Azure für die Entwicklung und AWS für maschinelles Lernen verwenden. Es fördert einen effektiven Prozess zur Erstellung von Modellen für maschinelles Lernen von Anfang bis Ende, einschließlich Datenverarbeitung, Schulung und Bereitstellung auf AWS. Aus Effizienzgründen verwalten Sie diese Prozesse über DevOps Azure-Pipelines.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Azure-Abonnement — Zugriff auf Azure-Dienste wie Azure DevOps für die Einrichtung der Pipelines für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD).
- Aktives AWS-Konto — Berechtigungen zur Nutzung der in diesem Muster verwendeten AWS-Services.
- Daten — Zugriff auf historische Daten zum Trainieren des Modells für maschinelles Lernen.
- Vertrautheit mit ML-Konzepten — Verständnis von Python, Jupyter Notebooks und Modellentwicklung für maschinelles Lernen.
- Sicherheitskonfiguration — Richtige Konfiguration von Rollen, Richtlinien und Berechtigungen in Azure und AWS, um eine sichere Datenübertragung und einen sicheren Datenzugriff zu gewährleisten.

Einschränkungen

- Diese Anleitung enthält keine Hinweise zu sicheren cloudübergreifenden Datenübertragungen. Weitere Informationen zu cloudübergreifenden Datenübertragungen finden Sie unter AWS-Lösungen für Hybrid- und Multicloud.
- Multicloud-Lösungen können die Latenz für Datenverarbeitung und Modellinferenz in Echtzeit erhöhen.
- Diese Anleitung bietet ein Beispiel für eine MLOps-Architektur mit mehreren Konten. Anpassungen sind auf der Grundlage Ihrer Strategie für maschinelles Lernen und AWS erforderlich.

Architektur

Zielarchitektur

Die Zielarchitektur integriert Azure DevOps in Amazon SageMaker und schafft so einen cloudübergreifenden ML-Workflow. Sie verwendet Azure für CI/CD-Prozesse sowie SageMaker für das Training und die Bereitstellung von ML-Modellen. Es beschreibt den Prozess des Abrufs von Daten (aus Quellen wie Amazon S3, Snowflake und Azure Data Lake) durch Modellerstellung und -bereitstellung. Zu den wichtigsten Komponenten gehören CI/CD-Pipelines für die Modellerstellung und -bereitstellung, Datenvorbereitung, Infrastrukturmanagement und Amazon SageMaker für die

Schulung, Evaluierung und Bereitstellung von ML-Modellen. Diese Architektur wurde entwickelt, um effiziente, automatisierte und skalierbare ML-Workflows auf allen Cloud-Plattformen bereitzustellen.

Die Architektur besteht aus den folgenden Komponenten:

1. Datenwissenschaftler führen im Entwicklungskonto ML-Experimente durch, um mithilfe verschiedener Datenquellen verschiedene Ansätze für ML-Anwendungsfälle zu untersuchen. Datenwissenschaftler führen Unit-Tests und Studien durch. Nach der Modellevaluierung übertragen Datenwissenschaftler den Code und führen ihn in das Model Build-Repository ein, das auf Azure gehostet wird DevOps. Dieses Repository enthält Code für eine mehrstufige Modellerstellungspipeline.
2. In Azure DevOps kann die Model Build Pipeline, die Continuous Integration (CI) bietet, bei der Codezusammenführung mit dem Hauptzweig automatisch oder manuell aktiviert werden. Im Automation-Konto wird dadurch die SageMaker Pipeline für die Datenvorverarbeitung, das Modelltraining und die Evaluierung sowie die bedingte Modellregistrierung auf der Grundlage der Genauigkeit aktiviert.
3. Das Automation-Konto ist ein zentrales Konto für alle ML-Plattformen, das ML-Umgebungen (Amazon ECR), Modelle (Amazon S3), Modellmetadaten (SageMaker Model Registry), Funktionen (SageMaker Feature Store), automatisierte Pipelines (SageMaker Pipelines) und ML-Log-Insights (CloudWatch und OpenSearch Service) hostet. Dieses Konto ermöglicht die Wiederverwendbarkeit von ML-Assets und setzt bewährte Verfahren durch, um die Bereitstellung von ML-Anwendungsfällen zu beschleunigen.
4. Die neueste Modellversion wird zur Überprüfung zur SageMaker Modellregistrierung hinzugefügt. Es verfolgt Modellversionen und die jeweiligen Artefakte (Herkunft und Metadaten). Es verwaltet auch den Status des Modells (genehmigt, abgelehnt oder ausstehend) und verwaltet die Version für die nachgelagerte Bereitstellung.
5. Nachdem ein in Model Registry trainiertes Modell über die Studio-Oberfläche oder einen API-Aufruf genehmigt wurde, kann eine Veranstaltung an Amazon gesendet werden EventBridge. EventBridge startet die Model Deploy-Pipeline auf Azure DevOps.
6. Die Model Deploy-Pipeline, die eine kontinuierliche Bereitstellung (CD) ermöglicht, checkt die Quelle aus dem Model Deploy-Repository aus. Der Quellcode enthält Code, die Konfiguration für die Modellbereitstellung und Testskripte für Qualitätsbenchmarks. Die Model Deploy-Pipeline kann auf Ihren Inferenztyp zugeschnitten werden.
7. Nach den Qualitätskontrollen stellt die Model Deploy-Pipeline das Modell für das Staging-Konto bereit. Das Staging-Konto ist eine Kopie des Produktionskontos und wird für Integrationstests und

Evaluierungen verwendet. Bei einer Batch-Transformation kann die Model Deploy-Pipeline den Batch-Inferenzprozess automatisch aktualisieren, sodass die neueste genehmigte Modellversion verwendet wird. Für eine serverlose oder asynchrone Inferenz in Echtzeit richtet sie den jeweiligen Modellendpunkt ein oder aktualisiert ihn.

8. Nach erfolgreichen Tests im Staging-Konto kann ein Modell durch manuelle Genehmigung über die Model Deploy-Pipeline für das Produktionskonto bereitgestellt werden. Diese Pipeline stellt einen Produktionsendpunkt im Schritt „Bereitstellen bis zur Produktion“ bereit, einschließlich der Modellüberwachung und eines Mechanismus zur Datenrückkopplung.
9. Sobald das Modell in Produktion ist, können Sie Tools wie SageMaker Model Monitor und SageMaker Clarify verwenden, um Abweichungen zu erkennen, Abweichungen zu erkennen und die Leistung des Modells kontinuierlich zu überwachen.

Automatisierung und Skalierung

Verwenden Sie Infrastructure as Code (IaC) für die automatische Bereitstellung auf mehreren Konten und Umgebungen. Durch die Automatisierung des Prozesses der Einrichtung eines MLOps-Workflows ist es möglich, die Umgebungen zu trennen, die von ML-Teams verwendet werden, die an verschiedenen Projekten arbeiten. AWS CloudFormation unterstützt Sie bei der Modellierung, Bereitstellung und Verwaltung von AWS-Ressourcen, indem Infrastruktur als Code behandelt wird.

Tools

AWS-Services

- Amazon SageMaker ist ein verwalteter ML-Service, der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. In diesem Muster wird Amazon S3 für die Datenspeicherung verwendet und SageMaker für Modelltraining und Modellobjekte integriert.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster wird Lamdba für Aufgaben zur Vor- und Nachverarbeitung von Daten verwendet.

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. In diesem Muster werden Docker-Container gespeichert, die als Schulungs- und Bereitstellungsumgebungen SageMaker verwendet werden.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. In diesem Muster EventBridge orchestriert er ereignisgesteuerte oder zeitbasierte Workflows, die eine automatische Neuschulung oder Bereitstellung des Modells einleiten.
- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung. In diesem Muster wird es verwendet, um einen nach außen gerichteten, zentralen Einstiegspunkt für SageMaker Amazon-Endgeräte zu erstellen.

Andere Tools

- Azure DevOps unterstützt Sie bei der Verwaltung von CI/CD-Pipelines und erleichtert das Erstellen, Testen und Bereitstellen von Code.
- Azure Data Lake Storage oder Snowflake sind mögliche Quellen von Drittanbietern für Trainingsdaten für ML-Modelle.

Bewährte Methoden

Bevor Sie eine Komponente dieses Multicloud-MLOps-Workflows implementieren, führen Sie die folgenden Aktivitäten durch:

- Definieren und verstehen Sie den Workflow für maschinelles Lernen und die Tools, die zu seiner Unterstützung erforderlich sind. Verschiedene Anwendungsfälle erfordern unterschiedliche Workflows und Komponenten. Beispielsweise kann ein feature store für die Wiederverwendung von Funktionen und die Inferenz mit niedriger Latenz in einem Personalisierungs-Anwendungsfall erforderlich sein, für andere Anwendungsfälle jedoch möglicherweise nicht. Um die Architektur erfolgreich anpassen zu können, ist es erforderlich, den Ziel-Workflow, die Anforderungen an den Anwendungsfall und die bevorzugten Methoden der Zusammenarbeit des Data-Science-Teams zu verstehen.
- Sorgen Sie für eine klare Trennung der Zuständigkeiten für die einzelnen Komponenten der Architektur. Die Verteilung des Datenspeichers auf Azure Data Lake Storage, Snowflake und Amazon S3 kann die Komplexität und die Kosten erhöhen. Wählen Sie nach Möglichkeit einen

konsistenten Speichermechanismus. Vermeiden Sie auch die Verwendung einer Kombination aus Azure- und DevOps AWS-Services oder einer Kombination aus Azure- und AWS-ML-Services.

- Wählen Sie ein oder mehrere vorhandene Modelle und Datensätze aus, um den MLOps-Workflow zu end-to-end testen. Die Testartefakte sollten reale Anwendungsfälle widerspiegeln, die die Data-Science-Teams entwickeln, wenn die Plattform in Produktion geht.

Epen

Entwerfen Sie Ihre MLOps-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Datenquellen.	Dokumentieren Sie auf der Grundlage aktueller und future Anwendungsfälle, verfügbarer Datenquellen und Datentypen (z. B. vertraulicher Daten) die Datenquellen, die in die MLOps-Plattform integriert werden müssen. Daten können in Amazon S3, Azure Data Lake Storage, Snowflake oder anderen Quellen gespeichert werden. Erstellen Sie einen Plan zur Integration dieser Quellen in Ihre Plattform und zur Sicherung des Zugriffs auf die richtigen Ressourcen.	Dateningenieur, Datenwissenschaftler, Cloud-Architekt
Wählen Sie die entsprechenden Dienste aus.	Passen Sie die Architektur an, indem Sie Dienste auf der Grundlage des gewünschten Workflows des Data-Science-Teams, der entsprechenden Datenquellen und der vorhandenen Cloud-	AWS-Administrator, Dateningenieur, Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Architektur hinzufügen oder entfernen. Beispielsweise können Dateningenieure und Datenwissenschaftl er Datenvorverarbeitung und Feature-Engineering in SageMaker AWS Glue oder Amazon EMR durchführen. Es ist unwahrscheinlich, dass alle drei Dienste erforderlich wären.	
Analysieren Sie die Sicherhei tsanforderungen.	Sammeln und dokumentieren Sie die Sicherheitsanforde rungen. Dies beinhaltet die Festlegung von: • Welche Teams oder Ingenieure können auf bestimmte Datenquellen zugreifen • Ob Teams auf den Code und die Modelle anderer Teams zugreifen dürfen • Welche Berechtigungen (falls vorhanden) sollten Teammitglieder für Konten haben, die keine Entwickler sind • Welche Sicherhei tsmaßnahmen müssen für die cloudübergreifende Datenübertragung implementiert werden	AWS-Administrator, Cloud-Arc hitekt

AWS Organizations einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS Organizations ein.	Richten Sie AWS Organizations auf dem AWS-Stammkonto ein. Dies hilft Ihnen bei der Verwaltung der nachfolgenden Konten, die Sie im Rahmen einer MLOps-Strategie für mehrere Konten erstellen. Weitere Informationen finden Sie in der Dokumentation zu AWS Organizations.	AWS-Administrator

Richten Sie die Entwicklungsumgebung und die Versionierung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AWS-Entwicklungskonto.	Erstellen Sie ein AWS-Konto, in dem Dateningenieure und Datenwissenschaftler die Erlaubnis haben, mit ML-Modellen zu experimentieren und sie zu erstellen. Anweisungen finden Sie unter Erstellen eines Mitgliedskontos in Ihrer Organisation in der Dokumentation zu AWS Organizations.	AWS-Administrator
Erstellen Sie ein `Model Build`-Repository.	Erstellen Sie ein Git-Repository in Azure, in dem Datenwissenschaftler ihren Modellerstellungs- und	DevOps Ingenieur, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellungscode nach Abschluss der Experimentierphase pushen können. Anweisungen finden Sie in der DevOps Azure-Dokumentation unter Ein Git-Repository einrichten.	
Erstellen Sie ein `Model Deploy`-Repository.	Erstellen Sie ein Git-Repository in Azure, in dem Standardbereitstellungscode und Vorlagen gespeichert werden. Es sollte Code für jede Bereitstellungsoption enthalten, die die Organisation verwendet, wie in der Entwurfsphase festgelegt. Es sollte beispielsweise Echtzeit-Endpunkte, asynchrone Endpunkte, serverlose Inferenz oder Batch-Transformationen enthalten. Anweisungen finden Sie in der DevOps Azure-Dokumentation unter Ein Git-Repository einrichten.	DevOps Ingenieur, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Richten Sie ein Amazon ECR-Repository ein, das die genehmigten ML-Umgebungen als Docker-Images speichert. Ermöglichen Sie Datenwissenschaftlern und ML-Ingenieuren, neue Umgebungen zu definieren. Anweisungen finden Sie in der Amazon ECR-Dokumentation unter Erstellen eines privaten Repositorys.	ML-Ingenieur
Richten Sie SageMaker Studio ein.	Richten Sie SageMaker Studio auf dem Entwicklungskonto gemäß den zuvor definierten Sicherheitsanforderungen und den bevorzugten Data-Science-Tools ein, z. B. Ihrer Wahl der integrierten Entwicklungsumgebung (IDE). Verwenden Sie Lebenszykluskonfigurationen, um die Installation wichtiger Funktionen zu automatisieren und eine einheitliche Entwicklungsumgebung für Datenwissenschaftler zu schaffen. Weitere Informationen finden Sie in der SageMaker Dokumentation zu Amazon SageMaker Studio.	ML-Ingenieur, Datenwissenschaftler

Integrieren Sie CI/CD-Pipelines

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Automation-Konto.	Erstellen Sie ein AWS-Konto , in dem automatisierte Pipelines und Jobs ausgeführt werden. Sie können Data-Science-Teams Lesezugriff auf dieses Konto gewähren. Anweisungen finden Sie unter Erstellen eines Mitgliedskontos in Ihrer Organisation in der Dokumentation zu AWS Organizations.	AWS-Administrator
Richten Sie eine Modellregistrierung ein.	Richten Sie SageMaker Model Registry im Automation-Konto ein. Dieses Register speichert die Metadaten für ML-Modelle und hilft bestimmten Datenwissenschaftlern oder Teamleitern, Modelle zu genehmigen oder abzulehnen. Weitere Informationen finden Sie in der SageMaker Dokumentation unter Registrieren und Bereitstellen von Modellen mit Model Registry.	ML-Ingenieur
Erstellen Sie eine `ModelBuild` Pipeline.	Erstellen Sie eine CI/CD-Pipeline in Azure, die manuell oder automatisch gestartet wird, wenn Code in das `ModelBuild` Repository übertragen wird. Die Pipeline sollte den Quellcode auschecken und	DevOps Ingenieur, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine SageMaker Pipeline im Automation-Konto erstellen oder aktualisieren. Die Pipeline sollte der Modellreg istrierung ein neues Modell hinzufügen. Weitere Informati onen zum Erstellen einer Pipeline finden Sie in der Azure Pipelines-Dokument ation.	

Erstellen Sie den Deployment-Stack

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie AWS-Staging- und Bereitstellungskonten.	Erstellen Sie AWS-Konte n für die Bereitstellung und Bereitstellung von ML-Modellen. Diese Konten sollten identisch sein, um ein genaues Testen der Modelle im Staging zu ermöglichen, bevor sie zur Produktion übergehen. Sie können Data-Science-Teams Lesezugri ff auf das Staging-Konto gewähren. Anweisungen finden Sie unter Erstellen eines Mitgliedskontos in Ihrer Organisation in der Dokumentation zu AWS Organizations.	AWS-Administrator
Richten Sie S3-Buckets für die Modellüberwachung ein.	Führen Sie diesen Schritt aus, wenn Sie die Modellübe	ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rwachung für die bereitges tellten Modelle aktiviere n möchten, die von der `Model Deploy` Pipeline erstellt wurden. Erstellen Sie Amazon S3 S3-Buckets zum Speichern der Eingabe- und Ausgabedaten. Weitere Informationen zum Erstellen von S3-Buckets finden Sie unter Bucket erstellen in der Amazon S3 S3-Dokume ntation. Richten Sie kontoüber greifende Berechtigungen ein, sodass die automatis ierten Modellüberwachungs aufträge im Automation-Konto ausgeführt werden. Weitere Informationen finden Sie in der SageMaker Dokumentation unter Überwachen der Daten- und Modellqualität.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine `Model Deploy` Pipeline.	Erstellen Sie eine CI/CD-Pipeline in Azure, die startet, wenn ein Modell in der Modellregistrierung genehmigt wird. Die Pipeline sollte den Quellcode und das Modellartefakt auschecken, die Infrastrukturvorlagen für die Bereitstellung des Modells in den Staging- und Produktionskonten erstellen, das Modell im Staging-Konto bereitstellen, automatisierte Tests ausführen, auf die manuelle Genehmigung warten und das genehmigte Modell im Produktionskonto bereitstellen. Weitere Informationen zum Erstellen einer Pipeline finden Sie in der Dokumentation zu Azure Pipelines.	DevOps Ingenieur, ML-Ingenieur

(Optional) Automatisieren Sie die Infrastruktur der ML-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie AWS-CDKs oder CloudFormation Vorlagen.	Definieren Sie das AWS Cloud Development Kit (AWS CDK) oder CloudFormation AWS-Vorlagen für alle Umgebungen, die automatisch bereitgestellt werden müssen. Dies kann die Entwicklungsumgebung, die Automatisierungsum	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gebung sowie die Staging- und Bereitstellungsumgebungen umfassen. Weitere Informationen finden Sie im AWS-CDK und in der CloudFormationDokumentation.	
Erstellen Sie eine `Infrastructure` Pipeline.	Erstellen Sie eine CI/CD-Pipeline in Azure für die Bereitstellung der Infrastruktur. Ein Administrator kann diese Pipeline initiieren, um neue AWS-Konten zu erstellen und die Umgebungen einzurichten, die das ML-Team benötigt.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Unzureichende Überwachung und Drifterkennung — Eine unzureichende Überwachung kann dazu führen, dass Probleme mit der Modellleistung oder Datenabweichungen nicht erkannt werden.	Stärken Sie die Monitoring-Frameworks mit Tools wie Amazon CloudWatch, SageMaker Model Monitor und SageMaker Clarify. Konfigurieren Sie Warnmeldungen, um bei erkannten Problemen sofort Maßnahmen ergreifen zu können.
Fehler beim Auslösen der CI-Pipeline — Die CI-Pipeline in Azure wird bei der Codezusammenführung aufgrund einer Fehlkonfiguration DevOps möglicherweise nicht ausgelöst.	Überprüfen Sie die DevOps Azure-Projekteinstellungen, um sicherzustellen, dass die Webhooks ordnungsgemäß eingerichtet sind und auf die richtigen SageMaker Endpunkte verweisen.

Problem	Lösung
Verwaltung — Das zentrale Automation-Konto setzt möglicherweise keine Best Practices auf allen ML-Plattformen durch, was zu inkonsist enten Workflows führt.	Prüfen Sie die Automation-Kontoeinstellungen und stellen Sie sicher, dass alle ML-Umgebu ngen und -Modelle den vordefinierten Best Practices und Richtlinien entsprechen.
Verzögerungen bei der Genehmigung durch die Modellregistrierung — Dies passiert, wenn es zu Verzögerungen bei der Prüfung und Genehmigung des Modells kommt, entweder weil sich die Mitarbeiter Zeit nehmen, es zu überprüfen, oder weil technische Probleme auftreten.	Implementieren Sie ein Benachrichtigungss ystem, um die Beteiligten über Modelle zu informieren, deren Genehmigung noch aussteht, und um den Überprüfungsprozess zu rationalisieren.
Fehler bei der Modellbereitstellung — Ereigniss e, die an den Start von Pipelines zur Modellber eitstellung gesendet werden, können fehlschla gen und zu Verzögerungen bei der Bereitste llung führen.	Vergewissern Sie sich, dass Amazon EventBrid ge über die richtigen Berechtigungen und Ereignismuster verfügt, um DevOps Azure-Pip elines erfolgreich aufzurufen.
Engpässe bei der Produktionsbereitstellung — Manuelle Genehmigungsprozesse können zu Engpässen führen und die Produktionsbereits tellung von Modellen verzögern.	Optimieren Sie den Genehmigungsablauf innerhalb der Pipeline für die Modellbereitstellu ng und fördern Sie so zeitnahe Überprüfungen und klare Kommunikationskanäle.

Zugehörige Ressourcen

AWS-Dokumentation

- SageMaker Amazon-Dokumentation
- Linse für Machine Learning (AWS Well Architected Framework)
- Planung erfolgreicher MLOps (AWS Prescriptive Guidance)

Andere AWS-Ressourcen

- Roadmap zur Gründung von MLOp für Unternehmen mit Amazon SageMaker (AWS-Blogbeitrag)

- AWS Summit ANZ 2022 — E nd-to-end MLOps für Architekten (Video) YouTube

Azure-Dokumentation

- DevOps Azure-Dokumentation
- Dokumentation zu Azure Pipelines

Erstellen Sie ein benutzerdefiniertes Docker-Container-Image für SageMaker und verwenden Sie es für Modelltrainings in AWS Step Functions

Erstellt von Julia Bluszcz (AWS), Neha Sharma (AWS), Aubrey Oosthuizen (AWS), Mohan Gowda Purushothama (AWS) und Mateusz Zaremba (AWS)

Umgebung: Produktion	Technologien: Maschinelles Lernen und KI; DevOps	AWS-Services: Amazon ECR; Amazon SageMaker; AWS Step Functions

Übersicht

Dieses Muster zeigt, wie Sie ein Docker-Container-Image für Amazon erstellen SageMaker und es für ein Trainingsmodell in AWS Step Functions verwenden. Indem Sie benutzerdefinierte Algorithmen in einem Container verpacken, können Sie fast jeden Code in der SageMaker Umgebung ausführen, unabhängig von Programmiersprache, Framework oder Abhängigkeiten.

In dem bereitgestellten SageMaker Beispiel-Notizbuch wird das benutzerdefinierte Docker-Container-Image in Amazon Elastic Container Registry (Amazon ECR) gespeichert. Step Functions verwendet dann den Container, der in Amazon ECR gespeichert ist, um ein Python-Verarbeitungsskript für SageMaker auszuführen. Anschließend exportiert der Container das Modell nach Amazon Simple Storage Service (Amazon S3).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM) -Rolle für SageMaker mit Amazon S3 S3-Berechtigungen
- Eine IAM-Rolle für Step Functions
- Vertrautheit mit Python
- Vertrautheit mit dem Amazon SageMaker Python SDK

- Vertrautheit mit der AWS-Befehlszeilenschnittstelle (AWS CLI)
- Vertrautheit mit dem AWS-SDK SDK for Python (Boto3)
- Vertrautheit mit Amazon ECR
- Vertrautheit mit Docker

Produktversionen

- AWS Step Functions SDK für Datenwissenschaft, Version 2.3.0
- Amazon SageMaker Python SDK versie 2.78.0

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Erstellung eines Docker-Container-Images für und SageMaker dessen anschließende Verwendung für ein Trainingsmodell in Step Functions:

Das Diagramm zeigt den folgenden Workflow:

1. Ein Datenwissenschaftler oder DevOps Ingenieur verwendet ein SageMaker Amazon-Notizbuch, um ein benutzerdefiniertes Docker-Container-Image zu erstellen.
2. Ein Datenwissenschaftler oder DevOps Ingenieur speichert das Docker-Container-Image in einem privaten Amazon ECR-Repository, das sich in einer privaten Registrierung befindet.
3. Ein Datenwissenschaftler oder DevOps Ingenieur verwendet den Docker-Container, um einen SageMaker Python-Verarbeitungsjob in einem Step Functions Functions-Workflow auszuführen.

Automatisierung und Skalierung

Das SageMaker Beispiel-Notizbuch in diesem Muster verwendet einen `ml.m5.xlarge` Notebook-Instanztyp. Sie können den Instanztyp an Ihren Anwendungsfall anpassen. Weitere Informationen zu SageMaker Notebook-Instance-Typen finden Sie unter SageMaker Amazon-Preise.

Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Amazon SageMaker ist ein verwalteter Service für maschinelles Lernen (ML), der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen.
- Das Amazon SageMaker Python SDK ist eine Open-Source-Bibliothek für das Training und die Bereitstellung von Modellen für maschinelles Lernen. SageMaker
- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- Das AWS Step Functions Data Science Python SDK ist eine Open-Source-Bibliothek, mit der Sie Step Functions Functions-Workflows erstellen können, die Modelle für maschinelles Lernen verarbeiten und veröffentlichen.

Epen

Erstellen Sie ein benutzerdefiniertes Docker-Container-Image und speichern Sie es in Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon ECR ein und erstellen Sie eine neue private Registrierung.	Falls Sie dies noch nicht getan haben, richten Sie Amazon ECR ein, indem Sie den Anweisungen unter Einrichtung mit Amazon ECR im Amazon ECR-Benut zerhandbuch folgen. Jedes AWS-Konto ist mit einer standardmäßigen privaten Amazon ECR-Registrierung ausgestattet.	DevOps Ingenieur
Erstellen Sie ein privates Amazon ECR-Repository.	Folgen Sie den Anweisungen unter Erstellen eines privaten Repositorys im Amazon ECR-Benutzerhandbuch.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: In dem Repository, das Sie erstellen, speichern Sie Ihre benutzerdefinierten Docker-Container-Images.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Dockerfile, das die Spezifikationen enthält, die für die Ausführung Ihres SageMaker Verarbeitungsjobs erforderlich sind.	Erstellen Sie ein Dockerfile, das die für die Ausführung Ihres SageMaker Verarbeitungsjobs erforderlichen Spezifikationen enthält, indem Sie ein Dockerfile konfigurieren. Eine Anleitung finden Sie im Amazon SageMaker Developer Guide unter Anpassung Ihres eigenen Trainingscontainers.
	
	Weitere Informationen zu Dockerfiles finden Sie in der Dockerfile-Referenz in der Docker-Dokumentation.
	
	Beispiel: Jupyter-Notebook-Codezellen zum Erstellen eines Dockerfiles
	
	Zelle 1
	
	`# Make docker folder`
	`!mkdir -p docker`
	
	Zelle 2
	
	`%%writefile docker/Dockerfile`
	
	`FROM python:3.7-slim-buster`
	
	`RUN pip3 install pandas==0.25.3 scikit-learn==0.21.3`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`ENV PYTHONUNBUFFERED=TRUE`
	
	`ENTRYPOINT ["python3"]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihr Docker-Container-Image und übertragen Sie es auf Amazon ECR.	1. Erstellen Sie das Container-Image mit der Dockerfile, die Sie erstellt haben, indem Sie den `docker build` Befehl in der AWS-CLI ausgeführt haben. 2. Senden Sie das Container-Image an Amazon ECR, indem Sie den `docker push` Befehl ausführen. Weitere Informationen finden Sie unter Container erstellen und registrieren unter Erstellen eines eigenen Algorithmus-Containers auf GitHub. Beispiel für Jupyter-Notebook-Codezellen zum Erstellen und Registrieren eines Docker-Images Wichtig: Bevor Sie die folgenden Zellen ausführen, stellen Sie sicher, dass Sie ein Dockerfile erstellt und im Verzeichnis namens gespeichert haben. `docker` Stellen Sie außerdem sicher, dass Sie ein Amazon ECR-Repository erstellt haben und dass Sie den `ecr_repository` Wert in der ersten Zelle durch den Namen Ihres Repositorys ersetzen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Zelle 1
	
	`import boto3 tag = ':latest' account_id = boto3.client('sts').get_caller_identity().get('Account') region = boto3.Session().region_name ecr_repository = 'byoc'`
	
	`image_uri = '{}.dkr.ecr.{}.amazonaws.com/{}'.format(account_id, region, ecr_repository + tag)`
	
	Zelle 2
	
	`# Build docker image !docker build -t $image_uri docker`
	
	Zelle 3
	
	`# Authenticate to ECR !aws ecr get-login-password --region {region} | docker login --username AWS --password-stdin {account_id}.dkr.ecr.{region}.amazonaws.com`
	
	Zelle 4
	
	`# Push docker image`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`!docker push $image_ur i` Hinweis: Sie müssen Ihren Docker-Client bei Ihrer privaten Registrierung authentifizieren, damit Sie die Befehle `docker push` und `docker pull` verwenden können. Mit diesen Befehlen werden Bilder in und aus den Repositorys in Ihrer Registrierung übertragen und abgerufen.	

Erstellen Sie einen Step Functions Functions-Workflow, der Ihr benutzerdefiniertes Docker-Container-Image verwendet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Python-Skript, das Ihre benutzerd efinierte Verarbeitungs- und Modelltrainingslogik enthält.	Schreiben Sie eine benutzerd efinierte Verarbeitungslogik , die in Ihrem Datenvera rbeitungsskript ausgeführt werden soll. Speichern Sie es dann als Python-Skript mit dem Name`training.py` . Weitere Informationen finden Sie unter Bringen Sie Ihr eigenes Modell mit aktiviertem SageMaker Skriptmodus mit GitHub.	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Beispiel für ein Python-Skript, das benutzerdefinierte Verarbeitungs- und Modelltraiiningslogik enthält
	
	`%%writefile training.py`
	`from numpy import empty`
	`import pandas as pd`
	`import os`
	`from sklearn import datasets, svm`
	`from joblib import dump, load`
	
	`if __name__ == '__main__':`
	`digits = datasets.load_digits()`
	`#create classifier object`
	`clf = svm.SVC(gamma=0.001, C=100.)`
	
	`#fit the model`
	`clf.fit(digits.data[:-1], digits.target[:-1])`
	
	`#model output in binary format`
	`output_path = os.path.join('/opt/ml/processing/model', "model.joblib")`
	`dump(clf, output_path)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Step Functions Functions-Workflow , der Ihren SageMaker Verarbeitungsjob als einen der Schritte enthält.	Installieren und importieren Sie das AWS Step Functions Data Science SDK und laden Sie die Datei training. py auf Amazon S3 hoch. Verwenden Sie dann das Amazon SageMaker Python SDK, um einen Verarbeit ungsschritt in Step Functions zu definieren.
	
	Wichtig: Stellen Sie sicher, dass Sie in Ihrem AWS-Konto eine IAM-Ausführungsrolle für Step Functions erstellt haben.
	
	Beispiel für die Einrichtung einer Umgebung und ein benutzerdefiniertes Trainings skript zum Hochladen auf Amazon S3
	
	`!pip install stepfunct ions`
	
	`import boto3 import stepfunctions import sagemaker import datetime`
	
	`from stepfunctions import steps from stepfunct ions.inputs import ExecutionInput from stepfunct ions.steps import ( Chain`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	)
	from stepfunct
	ions.workflow import
	 Workflow
	from sagemaker
	.processing import
	 ScriptProcessor,
	 ProcessingInput,
	 ProcessingOutput
	
	sagemaker_session =
	 sagemaker.Session()
	bucket = sagemaker
	_session.default_b
	ucket()
	role = sagemaker
	.get_execution_role()
	prefix = 'byoc-tra
	ining-model'
	
	# See prerequisites
	 section to create this
	 role
	workflow_execution_rol
	e = f"arn:aws:iam::
	{account_id}:role/Ama
	zonSageMaker-StepF
	unctionsWorkflowEx
	ecutionRole"
	
	execution_input =
	 ExecutionInput(
	    schema={
	        "Preproce
	ssingJobName": str})
	
	input_code = sagemaker
	_session.upload_data(
	    "training.py",
	    bucket=bucket,
	``	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`key_prefix="preprocessing.py",` `)`	

	Beispiel für eine Definition eines SageMaker Verarbeitungsschritts, die ein benutzerdefiniertes Amazon ECR-Image und ein Python-Skript verwendet
	
	Hinweis: Stellen Sie sicher, dass Sie den `execution_input` Parameter verwenden, um den Jobnamen anzugeben. Der Wert des Parameters muss bei jeder Ausführung des Jobs eindeutig sein. Außerdem wird der Code der Datei training.py als `input` Parameter an die übergeben`ProcessingStep` , was bedeutet, dass er in den Container kopiert wird. Das Ziel für den `ProcessingInput` Code ist dasselbe wie das zweite Argument in der`container_entrypoint` .
	
	`script_processor = ScriptProcessor(command=['python3'],`
	
	`image_uri=image_uri,`
	
	`role=role,`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>instance_count=1,
	
	instance_type='ml.
	m5.xlarge')
	
	processing_step =
	steps.ProcessingStep(
	"training-step",
	processor=script_p
	rocessor,
	job_name=execution
	_input["Preprocess
	ingJobName"],
	inputs=[
	Processin
	gInput(
	source=in
	put_code,
	destinati
	on="/opt/ml/proces
	sing/input/code",
	input_nam
	e="code",
	),
	],
	outputs=[
	Processin
	gOutput(
	source='/
	opt/ml/processing/
	model',
	destinati
	on="s3://{}/{}".fo
	rmat(bucket, prefix),
	output_na
	me='byoc-example')
	],
	container_entrypoi
	nt=["python3", "/opt/</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ml/processing/input/code/training.py"],` `)`	

	Beispiel Step Functions Functions-Workflow, der einen SageMaker Verarbeitungsjob ausführt
	
	Hinweis: Dieser Beispiel-Workflow umfasst nur den SageMaker Verarbeitungs-Job-Schritt, keinen vollständigen Step Functions Functions-Workflow. Ein vollständiges Beispiel für einen Workflow finden Sie unter Beispiel-Notebooks SageMaker in der AWS Step Functions Data Science SDK-Dokumentation.
	
	`workflow_graph = Chain([processing_step])`
	
	`workflow = Workflow(`
	`name="ProcessingWorkflow",`
	`definition=workflow_graph,`
	`role=workflow_execution_role`
	`)`
	
	`workflow.create()`
	`# Execute workflow`
	`execution = workflow.execute(`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> inputs={
	        "Preproce
	ssingJobName":
	 str(datetime.datet
	ime.now().strftime
	("%Y%m%d%H%M-%SS")),
	  # Each pre processin
	g job (SageMaker
	 processing job)
	 requires a unique name,
	    }
	)
	execution_output =
	 execution.get_outp
	ut(wait=True)</pre>	

Zugehörige Ressourcen

- Daten verarbeiten (Amazon SageMaker Developer Guide)
- Anpassung Ihres eigenen Trainingscontainers (Amazon SageMaker Developer Guide)

Bereitstellen von Vorverarbeitungslogik in einem ML-Modell in einem einzigen Endpunkt mithilfe einer Inferenz-Pipeline in Amazon SageMaker

Erstellt von Mohan Gowda Purushothama (AWS), Gabriel Bolriguez Gar microSD (AWS) und Mateuszremba (AWS)

Umgebung: Produktion	Technologien: Machine Learning und KI; Container und Microservices	AWS-Services: Amazon SageMaker; Amazon ECR

Übersicht

Dieses Muster erklärt, wie Sie mehrere Pipeline-Modellobjekte in einem einzigen Endpunkt mithilfe einer Inferenz-Pipeline in Amazon bereitstellen SageMaker. Das Pipeline-Modellobjekt stellt verschiedene Workflow-Phasen für Machine Learning (ML) dar, z. B. Vorverarbeitung, Modellinferenz und Nachbearbeitung. Um die Bereitstellung von seriell verbundenen Pipeline-Modellobjekten zu veranschaulichen, zeigt dieses Muster, wie Sie einen Scikit-learn-Container und ein Regressionsmodell basierend auf dem in integrierten linearen Lernalgorithmus bereitstellen SageMaker. Die Bereitstellung wird hinter einem einzelnen Endpunkt in gehostet SageMaker.

Hinweis: Die Bereitstellung in diesem Muster verwendet den Instance-Typ ml.m4.2xlarge. Wir empfehlen, einen Instance-Typ zu verwenden, der Ihren Anforderungen an die Datengröße und der Komplexität Ihres Workflows entspricht. Weitere Informationen finden Sie unter Amazon- SageMaker Preise. Dieses Muster verwendet vorgefertigte Docker-Images für Scikit-learn, aber Sie können Ihre eigenen Docker-Container verwenden und sie in Ihren Workflow integrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Python 3.9
- Amazon SageMaker Python SDK und Boto3-Bibliothek

- AWS Identity and Access Management (AWS IAM)-Rolle mit grundlegenden SageMaker Berechtigungen und Amazon Simple Storage Service (Amazon S3)-Berechtigungen

Produktversionen

- Amazon SageMaker Python SDK 2.49.2

Architektur

Zieltechnologie-Stack

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon SageMaker
- Amazon SageMaker Studio
- Amazon Simple Storage Service (Amazon S3)
- Echtzeit-Inferenzendpunkt für Amazon SageMaker

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für die Bereitstellung eines Amazon- SageMaker Pipeline-Modellobjekts.

Das Diagramm zeigt den folgenden Workflow:

1. Ein SageMaker Notebook stellt ein Pipeline-Modell bereit.
2. Ein S3-Bucket speichert die Modellartefakte.
3. Amazon ECR ruft die Quell-Container-Images aus dem S3-Bucket ab.

Tools

AWS-Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Amazon SageMaker ist ein verwalteter ML-Service, mit dem Sie ML-Modelle erstellen und trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitstellen können.
- Amazon SageMaker Studio ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für ML, mit der Sie Ihre ML-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Code für dieses Muster ist in der GitHub Inferenz-Pipeline mit Scikit-learn und Linear Learner-Repository verfügbar.

Polen

Vorbereiten des Datensatzes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereiten Sie den Datensatz für Ihre Regressionsaufgabe vor.	Öffnen Sie ein Notebook in Amazon SageMaker Studio.
	
	Verwenden Sie den folgenden Beispielcode in Ihrem Notebook, um alle erforderl ichen Bibliotheken zu importier en und Ihre Arbeitsumgebung zu initialisieren:
	
	`import sagemaker`
	`from sagemaker import get_execution_role`
	
	`sagemaker_session = sagemaker.Session()`
	
	`# Get a SageMaker-compatible role used by this Notebook Instance.`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`role = get_execu tion_role()`
	
	`# S3 prefix`
	`bucket = sagemaker _session.default_b ucket()`
	`prefix = "Scikit-L inearLearner-pipel ine-abalone-example"`
	
	Um einen Beispieldatensatz herunterzuladen, fügen Sie Ihrem Notebook den folgenden Code hinzu:
	
	`! mkdir abalone_data`
	`! aws s3 cp s3://sage maker-sample-files /datasets/tabular/ uci_abalone/abalon e.csv ./abalone_data`
	
	Hinweis: Das Beispiel in diesem Muster verwendet den Abalone-Datensatz aus dem UCI Machine Learning Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie den Datensatz in einen S3-Bucket hoch.	Fügen Sie in dem Notebook, in dem Sie Ihren Datensatz zuvor vorbereitet haben, den folgenden Code hinzu, um Ihre Beispieldaten in einen S3-Bucket hochzuladen:
	`WORK_DIRECTORY = "abalone_data"`
	`train_input = sagemaker_session.upload_data( path="{}/{}".format(WORK_DIRECTORY, "abalone.csv"), bucket=bucket, key_prefix="{}/{}".format(prefix, "train"), )`
		Data Scientist

Erstellen des Datenpräprozessors mit SKLearn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das preprocessor.py-Skript vor.	1. Kopieren Sie die Vorverarbeitungslogik aus der Python-Datei im Repository GitHub sklearn_abalone_featurizer.py und fügen Sie dann den Code in eine separate Python-Datei mit dem Namen ein `sklearn_abalone_featurizer.py` . Sie können den Code an Ihren benutzerd	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	efinierten Datensatz und Ihren benutzerdefinierten Workflow anpassen. 2. Speichern Sie die `sklearn_abalone_featurizer.py` Datei im Stammverzeichnis Ihres Projekts (d. h. an demselben Speicherort, an dem Sie Ihr SageMaker Notebook ausführen).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das SKLearn-Präprozessorobjekt.	Um ein SKLearn-Präprozessorobjekt (SKLearn Estimator) zu erstellen, das Sie in Ihre endgültige Inferenzpipeline integrieren können, führen Sie den folgenden Code in Ihrem SageMaker Notebook aus:
	`from sagemaker.sklearn.estimator import SKLearn`
	
	`FRAMEWORK_VERSION = "0.23-1"`
	`script_path = "sklearn_abalone_featurizer.py"`
	
	`sklearn_preprocessor = SKLearn(`
	`entry_point=script_path,`
	`role=role,`
	`framework_version=FRAMEWORK_VERSION,`
	`instance_type="ml.c4.xlarge",`
	`sagemaker_session=sagemaker_session,`
	`)`
	`sklearn_preprocessor.fit({"train": train_input})`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Inferenz des Präprozessors.	Um zu bestätigen, dass Ihr Präprozessor korrekt definiert ist, starten Sie einen Batch-Transformationsauftrag, indem Sie den folgenden Code in Ihr SageMaker Notebook eingeben:
	`# Define a SKLearn Transformer from the trained SKLearn Estimator`
	`transformer = sklearn_preprocessor.transformer(`
	`instance_count=1, instance_type="ml.m5.xlarge", assemble_with="Line", accept="text/csv"`
	`)`
	
	`# Preprocess training input`
	`transformer.transform(train_input, content_type="text/csv")`
	`print("Waiting for transform job: " + transformer.latest_transform_job.job_name)`
	`transformer.wait()`
	`preprocessed_train = transformer.output_path`	

Erstellen eines Machine-Learning-Modells

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Modellobjekt.	Um ein Modellobjekt basierend auf dem Algorithmus für lineares Lernen zu erstellen, geben Sie den folgenden Code in Ihr SageMaker Notebook ein:
	`import boto3`
	`from sagemaker`
	`.image_uris import`
	` retrieve`
	
	`ll_image = retrieve(`
	`"linear-learner",`
	` boto3.Session().re`
	`gion_name)`
	`s3_ll_output_key`
	`_prefix = "ll_train`
	`ing_output"`
	`s3_ll_output_location`
	` = "s3://{}/{}/{}/{}"`
	`.format(`
	`  bucket, prefix,`
	` s3_ll_output_key_p`
	`refix, "ll_model"`
	`)`
	
	`ll_estimator =`
	` sagemaker.estimato`
	`r.Estimator(`
	`  ll_image,`
	`  role,`
	`  instance_count=1,`
	`  instance_type="ml.`
	`m4.2xlarge",`
	`  volume_size=20,`
	`  max_run=3600,`
	`  input_mode="File",`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> output_path=s3_ll_
	output_location,
	    sagemaker_session=
	sagemaker_session,
	)
	
	ll_estimator.s
	et_hyperparameters
	(feature_dim=10,
	 predictor_type="re
	gressor", mini_batc
	h_size=32)
	
	ll_train_data =
	 sagemaker.inputs.T
	rainingInput(
	    preprocessed_train
	,
	    distribution="Full
	yReplicated",
	    content_type="text
	/csv",
	    s3_data_type="S3Pr
	efix",
	)
	
	data_channels =
	 {"train": ll_train_
	data}
	ll_estimator.fit(inpu
	ts=data_channels,
	 logs=True)</pre>	

	Der vorherige Code ruft das relevante Amazon-ECR-Docker-Image aus der öffentlichen Amazon-ECR-Registry für das Modell ab, erstellt ein Schätzerobjekt und verwendet dieses Objekt dann, um	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Regressionsmodell zu trainieren.	

Bereitstellen der endgültigen Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie das Pipeline-Modell bereit.	Um ein Pipeline-Modellobjekt (d. h. ein Präprozessorobjekt) zu erstellen und das Objekt bereitzustellen, geben Sie den folgenden Code in Ihr SageMaker Notebook ein:
	`from sagemaker.model import Model`
	`from sagemaker.pipeline import PipelineModel`
	`import boto3`
	`from time import gmtime, strftime`
	
	`timestamp_prefix = strftime("%Y-%m-%d-%H-%M-%S", gmtime())`
	
	`scikit_learn_inferencee_model = sklearn_preprocessor.create_model()`
	`linear_learner_model = ll_estimator.create_model()`
	
	`model_name = "inferenc e-pipeline-" + timestamp_prefix`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>endpoint_name =
	"inference-pipeline-
	ep-" + timestamp_prefix
	sm_model = PipelineM
	odel(
	name=model_name,
	role=role, models=
	[scikit_learn_infe
	rencee_model,
	linear_learner_model]
	)
	
	sm_model.deploy(init
	ial_instance_count
	=1, instance_type="ml.
	c4.xlarge", endpoint_
	name=endpoint_name)</pre>
	Hinweis: Sie können den im Modellobjekt verwendeten Instance-Typ an Ihre Anforderungen anpassen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Inferenz.	Um zu bestätigen, dass der Endpunkt ordnungsgemäß funktioniert, führen Sie den folgenden Beispiel-Inferenzcode in Ihrem SageMaker Notebook aus:
	`from sagemaker.predictor import Predictor`
	`from sagemaker.serializers import CSVSerializer`
	
	`payload = "M, 0.44, 0.365, 0.125, 0.516, 0.2155, 0.114, 0.155"`
	`actual_rings = 10`
	`predictor = Predictor(`
	`endpoint_name=endpoint_name, sagemaker_session=sagemaker_session, serializer=CSVSerializer()`
	`)`
	
	`print(predictor.predict(payload))`
		Data Scientist

Zugehörige Ressourcen

- Verarbeiten Sie Eingabedaten vor der Erstellung von Vorhersagen mithilfe von Amazon SageMaker -Inferenzpipelines und Scikit-learn (AWS Machine Learning Blog)
- End-to-End Machine Learning mit Amazon SageMaker (GitHub)

Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct

Erstellt von Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS) und Shuai Cao (AWS)

Code-Repository: genai-bedrock-chatbot	Umgebung: PoC oder Pilotprojekt	Technologien: Maschinelles Lernen und KI; Datenbanken DevOps; Serverlos
AWS-Dienste: Amazon Bedrock; Amazon ECS; Amazon Kendra; AWS Lambda		

Übersicht

In einem typischen Unternehmen sind 70 Prozent seiner Daten in isolierten Systemen gespeichert. Mithilfe generativer, KI-gestützter Chat-Assistenten können Sie mithilfe von Interaktionen in natürlicher Sprache Einblicke und Beziehungen zwischen diesen Datensilos gewinnen. Um das Beste aus generativer KI herauszuholen, müssen die Ergebnisse vertrauenswürdig und genau sein und die verfügbaren Unternehmensdaten beinhalten. Erfolgreiche Chat-Assistenten hängen von folgenden Faktoren ab:

- Generative KI-Modelle (wie Anthropic Claude 2)
- Vektorisierung von Datenquellen
- Fortgeschrittene Argumentationstechniken, wie z. B. das ReAct Framework, als Grundlage für das Modell

Dieses Muster bietet Datenabrufansätze aus Datenquellen wie Amazon Simple Storage Service (Amazon S3) -Buckets, AWS Glue und Amazon Relational Database Service (Amazon RDS). Aus diesen Daten wird Wert gewonnen, indem Retrieval Augmented Generation (RAG) mit Methoden verknüpft wird. chain-of-thought Die Ergebnisse unterstützen komplexe Chat-basierte Assistentengespräche, die sich auf die Gesamtheit der in Ihrem Unternehmen gespeicherten Daten stützen.

Dieses Muster verwendet SageMaker Amazon-Handbücher und Preisdatentabellen als Beispiel, um die Funktionen eines generativen KI-Assistenten auf Chatbasis zu untersuchen. Sie werden einen Chat-basierten Assistenten entwickeln, der Kunden hilft, den SageMaker Service zu bewerten, indem er Fragen zur Preisgestaltung und zu den Funktionen des Dienstes beantwortet. Die Lösung verwendet eine Streamlit-Bibliothek für die Erstellung der Frontend-Anwendung und das LangChain Framework für die Entwicklung des Anwendungs-Backends, das auf einem Large Language Model (LLM) basiert.

Anfragen an den Chat-Assistenten werden zunächst mit einer Absichtsklassifizierung beantwortet, sodass sie an einen von drei möglichen Workflows weitergeleitet werden. Der ausgefeilteste Arbeitsablauf kombiniert allgemeine Beratung mit komplexen Preisanalysen. Sie können das Muster an Anwendungsfälle in Unternehmen, Unternehmen und der Industrie anpassen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS-Befehlszeilenschnittstelle (AWS CLI) installiert und konfiguriert
- AWS Cloud Development Kit (AWS CDK) Toolkit 2.114.1 oder höher installiert und konfiguriert
- Grundkenntnisse in Python und AWS CDK
- Git installiert
- Docker installiert
- Python 3.11 oder höher installiert und konfiguriert (weitere Informationen finden Sie im Abschnitt Tools)
- Ein aktives AWS-Konto, das mithilfe von AWS CDK gestartet wurde
- Der Zugriff auf die Modelle Amazon Titan und Anthropic Claude ist im Amazon Bedrock-Service aktiviert
- AWS-Sicherheitsanmeldedaten`AWS_ACCESS_KEY_ID`, einschließlich korrekt konfigurierter Anmeldeinformationen in Ihrer Terminalumgebung

Einschränkungen

- LangChain unterstützt nicht jedes LLM für Streaming. Die Modelle von Anthropic Claude werden unterstützt, Modelle von AI21 Labs jedoch nicht.
- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.

- Diese Lösung kann nur in AWS-Regionen eingesetzt werden, in denen Amazon Bedrock und Amazon Kendra verfügbar sind. Informationen zur Verfügbarkeit finden Sie in der Dokumentation für Amazon Bedrock und Amazon Kendra.

Produktversionen

- Python-Version 3.11 oder höher
- Streamlit Version 1.30.0 oder höher
- Streamlit-Chat Version 0.1.1 oder höher
- LangChain Version 0.1.12 oder höher
- AWS CDK Version 2.132.1 oder höher

Architektur

Zieltechnologie-Stack

- Amazon Athena
- Amazon Bedrock
- Amazon Elastic Container Service (Amazon ECS)
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon Kendra
- Elastic Load Balancing

Zielarchitektur

Der AWS-CDK-Code stellt alle Ressourcen bereit, die für die Einrichtung der Chat-basierten Assistentenanwendung in einem AWS-Konto erforderlich sind. Die in der folgenden Abbildung gezeigte Chat-basierte Assistentenanwendung wurde entwickelt, um verwandte Anfragen von Benutzern zu beantworten SageMaker . Benutzer stellen über einen Application Load Balancer eine Verbindung zu einer VPC her, die einen Amazon ECS-Cluster enthält, der die Streamlit-Anwendung hostet. Eine Orchestrierungs-Lambda-Funktion stellt eine Verbindung zur Anwendung her. S3-Bucket-Datenquellen stellen Daten für die Lambda-Funktion über Amazon Kendra und AWS Glue

bereit. Die Lambda-Funktion stellt eine Verbindung zu Amazon Bedrock her, um Anfragen (Fragen) von Chat-basierten Assistentenbenutzern zu beantworten.

1. Die Orchestrierungs-Lambda-Funktion sendet die LLM-Prompt-Anfrage an das Amazon Bedrock-Modell (Claude 2).
2. Amazon Bedrock sendet die LLM-Antwort zurück an die Orchestrierungs-Lambda-Funktion.

Logikfluss innerhalb der Orchestrierungs-Lambda-Funktion

Wenn Benutzer über die Streamlit-Anwendung eine Frage stellen, wird die Orchestrierungs-Lambda-Funktion direkt aufgerufen. Das folgende Diagramm zeigt den Logikfluss, wenn die Lambda-Funktion aufgerufen wird.

- Schritt 1 — Die Eingabe `query` (Frage) wird in eine der drei Absichten eingeteilt:
  - Allgemeine SageMaker Orientierungsfragen
  - Allgemeine Fragen zur SageMaker Preisgestaltung (Schulung/Inferenz)
  - Komplexe Fragen im Zusammenhang mit und zur Preisgestaltung SageMaker
- Schritt 2 — Die Eingabe `query` initiiert einen der drei Dienste:
  - `RAG Retrieval service`, das den relevanten Kontext aus der Amazon Kendra Kendra-Vektordatenbank abruft und das LLM über Amazon Bedrock aufruft, um den abgerufenen Kontext als Antwort zusammenzufassen.
  - `Database Query service`, das das LLM, Datenbank-Metadaten und Beispielzeilen aus relevanten Tabellen verwendet, um die Eingabe in eine SQL-Abfrage umzuwandeln. `query` Der Datenbankabfragedienst führt die SQL-Abfrage für die SageMaker Preisdatenbank über Amazon Athena aus und fasst die Abfrageergebnisse als Antwort zusammen.
  - `In-context ReACT Agent service`, der die Eingabe `query` in mehrere Schritte unterteilt, bevor eine Antwort bereitgestellt wird. Der Agent verwendet `RAG Retrieval service` und `Database Query service` als Hilfsmittel, um während des Argumentationsprozesses relevante Informationen abzurufen. Nachdem der Argumentations- und Handlungsprozess abgeschlossen ist, generiert der Agent die endgültige Antwort als Antwort.
- Schritt 3 — Die Antwort der Orchestrierungs-Lambda-Funktion wird als Ausgabe an die Streamlit-Anwendung gesendet.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Foundation-Modelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue Glue-Crawler und eine AWS Glue Glue-Datenkatalogtabelle.
- Amazon Kendra ist ein intelligenter Suchdienst, der natürliche Sprachverarbeitung und fortschrittliche Algorithmen für maschinelles Lernen verwendet, um spezifische Antworten auf Suchfragen aus Ihren Daten zurückzugeben.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Code-Repository

Der Code für dieses Muster ist im GitHub genai-bedrock-chatbotRepository verfügbar.

Das Code-Repository enthält die folgenden Dateien und Ordner:

- `assets`Ordner — Die statischen Objekte, das Architekturdiagramm und der öffentliche Datensatz.
- `code/lambda-container`folder — Der Python-Code, der in der Lambda-Funktion ausgeführt wird
- `code/streamlit-app`folder — Der Python-Code, der als Container-Image in Amazon ECS ausgeführt wird
- `tests`folder — Die Python-Dateien, die zum Komponententest der AWS-CDK-Konstrukte ausgeführt werden
- `code/code_stack.py`— Das AWS-CDK-Konstrukt Python-Dateien, die zur Erstellung von AWS-Ressourcen verwendet werden
- `app.py`— Die AWS-CDK-Stack-Python-Dateien, die zur Bereitstellung von AWS-Ressourcen im AWS-Zielkonto verwendet werden
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die für AWS CDK installiert werden müssen
- `requirements-dev.txt`— Die Liste aller Python-Abhängigkeiten, die installiert werden müssen, damit AWS CDK die Unit-Test-Suite ausführen kann
- `cdk.json`— Die Eingabedatei zur Bereitstellung von Werten, die zum Hochfahren von Ressourcen erforderlich sind

Hinweis: Der AWS-CDK-Code verwendet L3-Konstrukte (Layer 3) und AWS Identity and Access Management (IAM) -Richtlinien, die von AWS für die Bereitstellung der Lösung verwaltet werden.

Bewährte Methoden

- Das hier bereitgestellte Codebeispiel ist nur für eine proof-of-concept (PoC) oder Pilotdemo vorgesehen. Wenn Sie den Code in die Produktionsumgebung übernehmen möchten, sollten Sie die folgenden bewährten Methoden anwenden:
  - Die Amazon S3 S3-Zugriffsprotokollierung ist aktiviert.
  - VPC Flow Logs ist aktiviert.
  - Der Amazon Kendra Enterprise Edition-Index ist aktiviert.

- Richten Sie die Überwachung und Warnung für die Lambda-Funktion ein. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen. Allgemeine bewährte Methoden für die Arbeit mit Lambda-Funktionen finden Sie in der AWS-Dokumentation.

Epen

AWS-Anmeldeinformationen auf Ihrem lokalen Computer einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die AWS-Region, in der der Stack bereitgestellt wird.	Führen Sie die folgenden Befehle aus, um AWS-Anmeldeinformationen für AWS CDK mithilfe von Umgebungsvariablen bereitzustellen.
	`export CDK_DEFAULT_ACCOUNT=<12 Digit AWS Account Number>`
	`export CDK_DEFAULT_REGION=<region>`
		DevOps Ingenieur, AWS DevOps

Richten Sie das AWS-CLI-Profil ein.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um das AWS-CLI-Profil für das Konto einzurichten.	DevOps Ingenieur, AWS DevOps

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihrem lokalen Computer.	Um das Repository zu klonen, führen Sie den folgenden Befehl in Ihrem Terminal aus. `git clone https://github.com/awslabs/`	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`genai-bedrock-chat bot.git`	

Richten Sie die virtuelle Python-Umgebung ein und installieren Sie die erforderl ichen Abhängigkeiten.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurich ten.
	`cd genai-bedrock-chat bot`
	`python3 -m venv .venv`
	`source .venv/bin/ activate`
	Führen Sie den folgenden Befehl aus, um die erforderl ichen Abhängigkeiten einzurichten.
	`pip3 install -r requirements.txt`
		DevOps Ingenieur, AWS DevOps

Richten Sie die AWS-CDK-Umgebung ein und synthetis ieren Sie den AWS-CDK-C ode.	1. Führen Sie den folgenden Befehl aus, um die AWS-CDK-Umgebung in Ihrem AWS-Konto einzurichten. `cdk bootstrap aws:// ACCOUNT-NUMBER/ REGION` 2. Führen Sie den Befehl aus, um den Code in eine CloudFormation AWS-Stack -Konfiguration zu konvertie rencdk synth.	DevOps Ingenieur, AWS DevOps

Konfigurieren und implementieren Sie die Chat-basierte Assistentenanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff auf das Claude-Modell.	Folgen Sie den Anweisungen in der Amazon Bedrock-Dokumentation, um den Zugriff auf das Anthropic-Claude-Modell für Ihr AWS-Konto zu aktivieren.	AWS DevOps
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe des AWS-CDK bereitzustellen: 1. Geben Sie im Stammverzeichnis des geklonten Repositorys in der `cdk.json` Datei Eingaben für die `logging` Parameter ein. Beispielwerte sind`INFO`, `DEBUGWARN`, und`ERROR`. Diese Werte definieren Nachrichten auf Protokollebene für die Lambda-Funktion und die Streamlit-Anwendung. 2. Die `app.py` Datei im Stammverzeichnis des geklonten Repositorys enthält den CloudFormation AWS-Stack-Namen, der für die Bereitstellung verwendet wird. Der	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standard-Stack-Name ist`chatbot-stack` . 3. Führen Sie den Befehl aus, um Ressourcen bereitzustellen`cdk deploy`. Der `cdk deploy` Befehl verwendet L3-Konstrukte, um mehrere Lambda-Funktionen zum Kopieren von Dokumenten und CSV-Datensatzdateien in S3-Buckets zu erstellen. 4. Melden Sie sich nach Abschluss des Befehls bei der AWS-Managementkonsole an, öffnen Sie die CloudFormation Konsole und überprüfen Sie, ob der Stack erfolgreich bereitgestellt wurde. Nach erfolgreicher Bereitstellung können Sie über die im Abschnitt CloudFormation Ausgaben angegebene URL auf die Chat-basierte Assistentenanwendung zugreifen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue Glue-Crawler aus und erstellen Sie die Datenkata logtabelle.	Ein AWS Glue Glue-Crawler wird verwendet, um das Datenschema dynamisch zu halten. Die Lösung erstellt und aktualisiert Partitionen in der AWS Glue Data Catalog-Tabelle, indem sie den Crawler bei Bedarf ausführt. Nachdem die CSV-Datensatzdateien in den S3-Bucket kopiert wurden, führen Sie den AWS Glue Glue-Crawler aus und erstellen Sie das Datenkata log-Tabellenschema zum Testen: 1. Navigieren Sie zur AWS Glue Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkata log die Option Crawlers aus. 3. Wählen Sie den Crawler mit Suffix aus. `sagemaker-pricing-crawler` 4. Führen Sie den Crawler aus. 5. Nachdem der Crawler erfolgreich ausgeführt wurde, erstellt er eine AWS Glue Data Catalog-Tabelle. Hinweis: Der AWS-CDK-Code konfiguriert den AWS Glue-	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Crawler so, dass er bei Bedarf ausgeführt wird. Sie können ihn aber auch so planen, dass er regelmäßig ausgeführt wird.	
Initiieren Sie die Indizierung von Dokumenten.	Nachdem die Dateien in den S3-Bucket kopiert wurden, verwenden Sie Amazon Kendra, um sie zu crawlen und zu indizieren: 1. Navigieren Sie zur Amazon Kendra Kendra-Konsole. 2. Wählen Sie den Index mit dem Suffix aus `chatbot-index` . 3. Wählen Sie im Navigationsbereich Datenquellen und dann den Datenquellenconnector mit dem Suffix aus `chatbot-index` . 4. Wählen Sie Jetzt synchronisieren, um den Indizierungsvorgang zu starten. Hinweis: Der AWS-CDK-Code konfiguriert die Amazon Kendra Kendra-Indexsynchronisierung so, dass sie bei Bedarf ausgeführt wird. Sie können sie jedoch auch regelmäßig ausführen, indem Sie den Parameter Schedule verwenden.	AWS DevOps, DevOps Ingenieur

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	Nachdem Sie die Lösung getestet haben, bereinigen Sie die Ressourcen: 1. Führen Sie den Befehl aus, um die von der Lösung bereitgestellten AWS-Ressourcen zu entfernen `cdk destroy`. 2. Löschen Sie alle Objekte aus den beiden S3-Buckets und entfernen Sie dann die Buckets. Weitere Informationen finden Sie unter Löschen eines Buckets.	DevOps Ingenieur, AWS DevOps

Fehlerbehebung

Problem	Lösung
AWS CDK gibt Fehler zurück.	Hilfe bei Problemen mit AWS CDK finden Sie unter Behebung häufiger Probleme mit AWS CDK.

Zugehörige Ressourcen

- Amazonas-Grundgestein:
  - Modellzugriff
  - Inferenzparameter für Fundamentmodelle

- Lambda-Funktionen mit Python erstellen
- Erste Schritte mit dem AWS CDK
- Arbeiten mit dem AWS CDK in Python
- Generativer KI-Anwendungsgenerator auf AWS
- LangChain Dokumentation
- Rationalisierte Dokumentation

Zusätzliche Informationen

AWS CDK-Befehle

Beachten Sie bei der Arbeit mit AWS CDK die folgenden nützlichen Befehle:

- Listet alle Stacks in der App auf

```
cdk ls
```

- Gibt die synthetisierte AWS-Vorlage aus CloudFormation

```
cdk synth
```

- Stellt den Stack für Ihr AWS-Standardkonto und Ihre Region bereit

```
cdk deploy
```

- Vergleicht den bereitgestellten Stack mit dem aktuellen Status

```
cdk diff
```

- Öffnet die AWS CDK-Dokumentation

```
cdk docs
```

- Löscht den CloudFormation Stack und entfernt von AWS bereitgestellte Ressourcen

```
cdk destroy
```

Entwickeln Sie mithilfe von Amazon Bedrock-Agenten und Wissensdatenbanken einen vollautomatischen Chat-basierten Assistenten

Erstellt von Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS), Praveen Kumar Jeyarajan (AWS) und Shuai Cao (AWS)

Code-Repository: genai-bedrock-agent-chatbot	Umgebung: PoC oder Pilotprojekt	Technologien: Maschinelles Lernen und KI; Serverlos
AWS-Dienste: Amazon Bedrock; AWS CDK; AWS Lambda		

Übersicht

Viele Unternehmen stehen vor Herausforderungen, wenn es darum geht, einen Chat-basierten Assistenten zu entwickeln, der in der Lage ist, verschiedene Datenquellen zu orchestrieren, um umfassende Antworten zu bieten. Dieses Muster bietet eine Lösung für die Entwicklung eines Chat-basierten Assistenten, der Anfragen sowohl aus der Dokumentation als auch aus Datenbanken beantworten kann, und das bei einer einfachen Bereitstellung.

Beginnend mit Amazon Bedrock bietet dieser vollständig verwaltete Service für generative künstliche Intelligenz (KI) eine breite Palette von Advanced Foundation Models (FMs). Dies ermöglicht die effiziente Erstellung generativer KI-Anwendungen mit einem starken Fokus auf Datenschutz und Sicherheit. Im Zusammenhang mit dem Abruf von Dokumenten ist die Retrieval Augmented Generation (RAG) ein zentrales Merkmal. Es verwendet Wissensdatenbanken, um FM-Eingabeaufforderungen um kontextrelevante Informationen aus externen Quellen zu erweitern. Ein Amazon OpenSearch Serverless-Index dient als Vektordatenbank hinter den Wissensdatenbanken für Amazon Bedrock. Diese Integration wird durch sorgfältiges, zeitnahes Engineering verbessert, um Ungenauigkeiten zu minimieren und sicherzustellen, dass die Antworten in einer sachlichen Dokumentation verankert sind. Für Datenbankabfragen wandeln die FMs von Amazon Bedrock Textanfragen in strukturierte SQL-Abfragen um, die spezifische Parameter enthalten. Dies ermöglicht den präzisen Abruf von Daten aus Datenbanken, die von AWS Glue Glue-Datenbanken verwaltet werden. Amazon Athena wird für diese Abfragen verwendet.

Um kompliziertere Anfragen zu bearbeiten und umfassende Antworten zu erhalten, sind Informationen erforderlich, die sowohl aus der Dokumentation als auch aus Datenbanken stammen. Agents for Amazon Bedrock ist eine generative KI-Funktion, mit der Sie autonome Agenten erstellen können, die komplexe Aufgaben verstehen und sie für die Orchestrierung in einfachere Aufgaben aufteilen können. Die Kombination der Erkenntnisse aus den vereinfachten Aufgaben, die durch die autonomen Agenten von Amazon Bedrock unterstützt werden, verbessert die Informationssynthese und führt zu gründlicheren und umfassenderen Antworten. Dieses Muster zeigt, wie Sie mithilfe von Amazon Bedrock und den zugehörigen generativen KI-Diensten und -Funktionen innerhalb einer automatisierten Lösung einen chatbasierten Assistenten erstellen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Docker, installiert
- AWS Cloud Development Kit (AWS CDK), installiert und in die `us-east-1`AWS-Regionen gestartet `us-west-2`
- AWS CDK Toolkit Version 2.114.1 oder höher, installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert
- Python Version 3.11 oder höher, installiert
- Aktivieren Sie in Amazon Bedrock den Zugriff auf Claude 2, Claude 2.1, Claude Instant und Titan Embeddings G1 — Text

Einschränkungen

- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.
- Diese Lösung kann nur in AWS-Regionen eingesetzt werden, in denen Amazon Bedrock und Amazon OpenSearch Serverless unterstützt werden. Weitere Informationen finden Sie in der Dokumentation für Amazon Bedrock und Amazon OpenSearch Serverless.

Produktversionen

- LLAMA-Index Version 0.10.6 oder höher
- Sqlalchemy Version 2.0.23 oder höher
- OpenSearch-PY Version 2.4.2 oder höher

- Requests_AWS4Auth Version 1.2.3 oder höher
- AWS-SDK SDK for Python (Boto3) Version 1.34.57 oder höher

Architektur

Zieltechnologie-Stack

Das AWS Cloud Development Kit (AWS CDK) ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Cloud-Infrastruktur im Code definiert und über AWS bereitgestellt werden kann. CloudFormation Der in diesem Muster verwendete AWS-CDK-Stack stellt die folgenden AWS-Ressourcen bereit:

- AWS Key Management Service (AWS KMS)
- Amazon-Simple-Storage-Service (Amazon-S3)
- AWS Glue Glue-Datenkatalog für die AWS Glue Glue-Datenbankkomponente
- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon OpenSearch Serverlos
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer

Zielarchitektur

Das Diagramm zeigt ein umfassendes Cloud-natives AWS-Setup innerhalb einer einzigen AWS-Region unter Verwendung mehrerer AWS-Services. Die primäre Schnittstelle für den Chat-basierten Assistenten ist eine Streamlit-Anwendung, die auf einem Amazon ECS-Cluster gehostet wird. Ein Application Load Balancer verwaltet die Barrierefreiheit. Abfragen, die über diese Schnittstelle gestellt werden, aktivieren die `Invocation` Lambda-Funktion, die dann eine Schnittstelle zu Agenten für Amazon Bedrock herstellt. Dieser Agent beantwortet Benutzeranfragen, indem er entweder die Wissensdatenbanken für Amazon Bedrock konsultiert oder eine `Agent executor` Lambda-Funktion

aufruft. Diese Funktion löst nach einem vordefinierten API-Schema eine Reihe von Aktionen aus, die dem Agenten zugeordnet sind. Die Wissensdatenbanken für Amazon Bedrock verwenden einen OpenSearch serverlosen Index als Grundlage für ihre Vektordatenbank. Darüber hinaus generiert die `Agent executor` Funktion SQL-Abfragen, die über Amazon Athena für die AWS Glue Glue-Datenbank ausgeführt werden.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Foundation-Modelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue Glue-Crawler und eine AWS Glue Glue-Datenkatalogtabelle.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon OpenSearch Serverless ist eine serverlose On-Demand-Konfiguration für Amazon OpenSearch Service. In diesem Muster dient ein OpenSearch serverloser Index als Vektordatenbank für die Wissensdatenbanken für Amazon Bedrock.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Streamlit ist ein Open-Source-Python-Framework zur Erstellung von Datenanwendungen.

Code-Repository

Der Code für dieses Muster ist im GitHub genai-bedrock-agent-chatbotRepository verfügbar. Das Code-Repository enthält die folgenden Dateien und Ordner:

- `assets`Ordner — Die statischen Elemente, wie das Architekturdiagramm und der öffentliche Datensatz.
- `code/lambdas/action-lambda`folder — Der Python-Code für die Lambda-Funktion, die als Aktion für den Amazon Bedrock-Agenten fungiert.
- `code/lambdas/create-index-lambda`folder — Der Python-Code für die Lambda-Funktion, die den OpenSearch Serverless-Index erstellt.
- `code/lambdas/invoke-lambda`folder — Der Python-Code für die Lambda-Funktion, die den Amazon Bedrock-Agenten aufruft, der direkt aus der Streamlit-Anwendung aufgerufen wird.
- `code/lambdas/update-lambda`folder — Der Python-Code für die Lambda-Funktion, die Ressourcen aktualisiert oder löscht, nachdem die AWS-Ressourcen über das AWS-CDK bereitgestellt wurden.
- `code/layers/boto3_layer`folder — Der AWS-CDK-Stack, der eine Boto3-Ebene erstellt, die von allen Lambda-Funktionen gemeinsam genutzt wird.
- `code/layers/opensearch_layer`folder — Der AWS-CDK-Stack, der eine OpenSearch serverlose Schicht erstellt, die alle Abhängigkeiten installiert, um den Index zu erstellen.
- `code/streamlit-app`folder — Der Python-Code, der als Container-Image in Amazon ECS ausgeführt wird
- `code/code_stack.py`— Das AWS CDK erstellt Python-Dateien, die AWS-Ressourcen erstellen.
- `app.py`— Der AWS-CDK-Stapel von Python-Dateien, die AWS-Ressourcen im AWS-Zielkonto bereitstellen.
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die für das AWS-CDK installiert werden müssen.

- `cdk.json`— Die Eingabedatei zur Bereitstellung der Werte, die für die Erstellung von Ressourcen erforderlich sind. Außerdem können Sie die Lösung in den `context/config` Feldern entsprechend anpassen. Weitere Informationen zur Anpassung finden Sie im Abschnitt Zusätzliche Informationen.

Bewährte Methoden

- Das hier bereitgestellte Codebeispiel dient nur proof-of-concept (PoC) oder Pilotzwecken. Wenn Sie den Code für die Produktion verwenden möchten, sollten Sie unbedingt die folgenden bewährten Methoden anwenden:
  - Amazon S3 S3-Zugriffsprotokollierung aktivieren
  - VPC-Flow-Logs aktivieren
- Richten Sie die Überwachung und Warnung für die Lambda-Funktionen ein. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen. Bewährte Methoden finden Sie unter Bewährte Methoden für die Arbeit mit AWS Lambda Lambda-Funktionen.

Epen

AWS-Anmeldeinformationen auf Ihrer lokalen Workstation einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die Region.	Führen Sie die folgenden Befehle aus, um AWS-Anmel deinformationen für das AWS-CDK mithilfe von Umgebungs variablen bereitzustellen.
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<Region>`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das AWS-CLI mit dem Namen profile ein.	Um das benannte AWS-CLI-Profil für das Konto einzurichten, folgen Sie den Anweisungen unter Konfiguration und Einstellungen der Anmeldeinformationsdatei.	AWS DevOps, DevOps Ingenieur

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihre lokale Workstation.	Um das Repository zu klonen, führen Sie den folgenden Befehl in Ihrem Terminal aus. `git clone https://github.com/awslabs/genai-bedrock-agent-chatbot.git`	DevOps Ingenieur, AWS DevOps

Richten Sie die virtuelle Python-Umgebung ein.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd genai-bedrock-agent-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Führen Sie den folgenden Befehl aus, um die erforderlichen Abhängigkeiten einzurichten.
		DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pip3 install -r requirements.txt`	
Richten Sie die AWS-CDK-Umgebung ein.	Führen Sie den Befehl aus, um den Code in eine CloudFormation AWS-Vorlage zu konvertieren`cdk synth`.	AWS DevOps, DevOps Ingenieur

Konfiguration und Bereitstellung der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe des AWS-CDK bereitzustellen: 1. Geben Sie im Stammverzeichnis des geklonten Repositorys in der `cdk.json` Datei Eingaben für die Protokollierungsparameter ein. Beispielwerte sind`INFO`, `DEBUG`, `WARN`, und`ERROR`. Diese Werte definieren Nachrichten auf Protokollebene für die Lambda-Funktionen und die Streamlit-Anwendung. 2. Die `cdk.json` Datei im Stammverzeichnis des geklonten Repositorys	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthält den CloudFormation AWS-Stack-Namen, der für die Bereitstellung verwendet wird. Der Standard-Stack-Name ist`chatbot-stack` . Der Standardname des Amazon Bedrock-Agenten ist`ChatbotBedrockAgent` , und der Standard-Alias für Amazon Bedrock-Agenten ist. `Chatbot_Agent` 3. Führen Sie den Befehl aus, um Ressourcen bereitzustellen. `cdk deploy` Der `cdk deploy` Befehl verwendet Layer-3-Konstrukte, um mehrere Lambda-Funktionen zum Kopieren von Dokumenten und CSV-Datensatzdateien in S3-Buckets zu erstellen . Außerdem werden der Amazon Bedrock-Agent, die Wissensdatenbanken und die `Action group` Lambda-Funktion für den Amazon Bedrock-Agenten bereitgestellt. 4. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole unter https://console.aws.amazon.com/cloudformation/. 5. Vergewissern Sie sich, dass der Stack erfolgreich bereitgestellt wurde. Anweisungen finden Sie unter Überprüfen Ihres Stacks auf der CloudFormation AWS-Konsole. Nach erfolgreicher Bereitstellung können Sie über die URL auf der Registerkarte Outputs in der Konsole auf die Chat-basierte Assistentenanwendung zugreifen. CloudFormation	

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	Nachdem Sie die Lösung getestet haben, führen Sie den Befehl aus, um die Ressourcen zu bereinigen`cdk destroy`.	AWS DevOps, DevOps Ingenieur

Zugehörige Ressourcen

AWS-Dokumentation

- Ressourcen von Amazon Bedrock:

  - Modellzugriff
  - Inferenzparameter für Fundamentmodelle
  - Agenten für Amazon Bedrock
  - Wissensdatenbanken für Amazon Bedrock
- Lambda-Funktionen mit Python erstellen
- AWS-CDK-Ressourcen:
  - Erste Schritte mit dem AWS CDK
  - Behebung häufiger AWS-CDK-Probleme
  - Arbeiten mit dem AWS-CDK in Python
- Generativer KI-Anwendungsgenerator auf AWS

Andere AWS-Ressourcen

- Vector Engine für Amazon OpenSearch Serverless

Sonstige Ressourcen

- LlamaIndex Dokumentation
- Rationalisierte Dokumentation

Zusätzliche Informationen

Passen Sie den Chat-basierten Assistenten mit Ihren eigenen Daten an

Folgen Sie diesen strukturierten Richtlinien, um Ihre benutzerdefinierten Daten für die Bereitstellung der Lösung zu integrieren. Diese Schritte sollen einen nahtlosen und effizienten Integrationsprozess gewährleisten, sodass Sie die Lösung effektiv mit Ihren maßgeschneiderten Daten implementieren können.

Für die Datenintegration in der Wissensdatenbank

Datenaufbereitung

1. Suchen Sie das `assets/knowledgebase_data_source/` Verzeichnis.
2. Platzieren Sie Ihren Datensatz in diesem Ordner.

Anpassungen der Konfiguration

1. Öffnen Sie die `cdk.json` Datei.
2. Navigieren Sie zu dem `context/configure/paths/knowledgebase_file_name` Feld und aktualisieren Sie es dann entsprechend.
3. Navigieren Sie zu dem `bedrock_instructions/knowledgebase_instruction` Feld, und aktualisieren Sie es dann, damit es die Nuancen und den Kontext Ihres neuen Datensatzes genau wiedergibt.

Für die Integration von Strukturdaten

Organisation der Daten

1. Erstellen Sie innerhalb des `assets/data_query_data_source/` Verzeichnisses ein Unterverzeichnis, z. B. `tabular_data`
2. Platzieren Sie Ihren strukturierten Datensatz (akzeptable Formate umfassen CSV, JSON, ORC und Parquet) in diesem neu erstellten Unterordner.
3. Wenn Sie eine Verbindung zu einer vorhandenen Datenbank herstellen, aktualisieren Sie die Funktion `create_sql_engine()` unter So stellen Sie eine Verbindung `code/lambda/action-lambda/build_query_engine.py` zu Ihrer Datenbank her.

Konfiguration und Code-Updates

1. Aktualisieren Sie das `context/configure/paths/athena_table_data_prefix` Feld in der `cdk.json` Datei so, dass es dem neuen Datenpfad entspricht.
2. Überarbeiten Sie, `code/lambda/action-lambda/dynamic_examples.csv` indem Sie neue Text-to-SQL-Beispiele einbeziehen, die Ihrem Datensatz entsprechen.
3. Überarbeiten Sie`code/lambda/action-lambda/prompt_templates.py`, um die Attribute Ihres strukturierten Datensatzes widerzuspiegeln.
4. Aktualisieren Sie das `context/configure/bedrock_instructions/action_group_description` Feld in der `cdk.json` Datei, um den Zweck und die Funktionalität der `Action group` Lambda-Funktion zu erläutern.
5. Erläutern Sie in der `assets/agent_api_schema/artifacts_schema.json` Datei die neuen Funktionen Ihrer `Action group` Lambda-Funktion.

Allgemeines Update

Geben Sie in der `cdk.json` Datei im `context/configure/bedrock_instructions/agent_instruction` Abschnitt eine umfassende Beschreibung der beabsichtigten Funktionalität und des Entwurfszwecks des Amazon Bedrock-Agenten unter Berücksichtigung der neu integrierten Daten.

Dokumentieren Sie institutionelles Wissen anhand von Spracheingaben mithilfe von Amazon Bedrock und Amazon Transcribe

Erstellt von Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Megan Wu (AWS) und Rajiv Upadhyay (AWS)

Code-Repository: genai-knowledge-capture	Umgebung: PoC oder Pilotprojekt	Technologien: Maschinelles Lernen und KI; Unternehmensproduktivität; Cloud-nativ
AWS-Services: Amazon Bedrock; AWS CDK; AWS Lambda; Amazon SNS; AWS Step Functions; Amazon Transcribe		

Übersicht

Die Erfassung von institutionellem Wissen ist für den Erfolg und die Widerstandsfähigkeit von Unternehmen von größter Bedeutung. Institutionelles Wissen steht für das kollektive Wissen, die Erkenntnisse und die Erfahrungen, die Mitarbeiter im Laufe der Zeit gesammelt haben. Diese sind oft stillschweigend und werden informell weitergegeben. Diese Fülle an Informationen umfasst einzigartige Ansätze, bewährte Verfahren und Lösungen für komplizierte Probleme, die möglicherweise an anderer Stelle nicht dokumentiert sind. Durch die Formalisierung und Dokumentation dieses Wissens können Unternehmen das institutionelle Gedächtnis bewahren, Innovationen fördern, Entscheidungsprozesse verbessern und die Lernkurven neuer Mitarbeiter beschleunigen. Darüber hinaus fördert es die Zusammenarbeit, befähigt Einzelpersonen und fördert eine Kultur der kontinuierlichen Verbesserung. Letztlich hilft die Nutzung von institutionellem Wissen Unternehmen dabei, ihr wertvollstes Kapital — die kollektive Intelligenz ihrer Belegschaft — zu nutzen, um Herausforderungen zu bewältigen, Wachstum voranzutreiben und Wettbewerbsvorteile in dynamischen Geschäftsumgebungen zu wahren.

Dieses Muster erklärt, wie institutionelles Wissen mithilfe von Sprachaufzeichnungen von leitenden Mitarbeitern erfasst werden kann. Es verwendet Amazon Transcribe und Amazon Bedrock für die

systematische Dokumentation und Überprüfung. Indem Sie dieses informelle Wissen dokumentieren, können Sie es bewahren und an nachfolgende Mitarbeiterkohorten weitergeben. Dieses Bestreben unterstützt betriebliche Exzellenz und verbessert die Effektivität von Schulungsprogrammen durch die Einbeziehung von praktischem Wissen, das durch direkte Erfahrung erworben wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Docker, installiert
- AWS Cloud Development Kit (AWS CDK) Version 2.114.1 oder höher, installiert und in die AWS-Regionen oder als Bootstrapping ausgeführt `us-east-1` `us-west-2`
- AWS CDK Toolkit Version 2.114.1 oder höher, installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert
- Python Version 3.12 oder höher, installiert
- Berechtigungen zum Erstellen von Ressourcen für Amazon Transcribe, Amazon Bedrock, Amazon Simple Storage Service (Amazon S3) und AWS Lambda

Einschränkungen

- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.
- Diese Lösung kann nur in AWS-Regionen eingesetzt werden, in denen Amazon Bedrock und Amazon Transcribe verfügbar sind. Informationen zur Verfügbarkeit finden Sie in der Dokumentation für Amazon Bedrock und Amazon Transcribe.
- Die Audiodateien müssen in einem Format vorliegen, das Amazon Transcribe unterstützt. Eine Liste der unterstützten Formate finden Sie unter Medienformate in der Transcribe-Dokumentation.

Produktversionen

- AWS-SDK SDK for Python (Boto3) Version 1.34.57 oder höher
- LangChain Version 0.1.12 oder höher

Architektur

Die Architektur stellt einen serverlosen Workflow auf AWS dar. AWS Step Functions orchestriert Lambda-Funktionen für die Audioverarbeitung, Textanalyse und Dokumentgenerierung. Das folgende Diagramm zeigt den Step Functions Functions-Workflow, der auch als Zustandsmaschine bezeichnet wird.

Jeder Schritt in der Zustandsmaschine wird von einer eigenen Lambda-Funktion behandelt. Im Folgenden sind die Schritte im Prozess der Dokumentgenerierung aufgeführt:

1. Die `preprocess` Lambda-Funktion validiert die an Step Functions übergebenen Eingaben und listet alle Audiodateien auf, die im angegebenen Amazon S3 S3-URI-Ordnerpfad vorhanden sind. Downstream-Lambda-Funktionen im Workflow verwenden die Dateiliste, um das Dokument zu validieren, zusammenzufassen und zu generieren.
2. Die `transcribe` Lambda-Funktion verwendet Amazon Transcribe, um Audiodateien in Texttranskripte umzuwandeln. Diese Lambda-Funktion ist dafür verantwortlich, den Transkriptionsprozess einzuleiten und Sprache präzise in Text umzuwandeln, der dann für die nachfolgende Verarbeitung gespeichert wird.
3. Die `validate` Lambda-Funktion analysiert die Texttranskripte und bestimmt die Relevanz der Antworten auf die ersten Fragen. Durch die Verwendung eines großen Sprachmodells (LLM) über Amazon Bedrock werden themenbezogene Antworten identifiziert und von themenfremden Antworten getrennt.
4. Die `summarize` Lambda-Funktion verwendet Amazon Bedrock, um eine kohärente und präzise Zusammenfassung der themenbezogenen Antworten zu erstellen.
5. Die `generate` Lambda-Funktion fasst die Zusammenfassungen zu einem gut strukturierten Dokument zusammen. Es kann das Dokument gemäß vordefinierten Vorlagen formatieren und alle zusätzlichen erforderlichen Inhalte oder Daten enthalten.
6. Wenn eine der Lambda-Funktionen ausfällt, erhalten Sie eine E-Mail-Benachrichtigung über Amazon Simple Notification Service (Amazon SNS).

Während dieses Prozesses stellt AWS Step Functions sicher, dass jede Lambda-Funktion in der richtigen Reihenfolge initiiert wird. Diese Zustandsmaschine kann parallel verarbeitet werden, um die Effizienz zu erhöhen. Ein Amazon S3 S3-Bucket fungiert als zentrales Speicher-Repository

und unterstützt den Arbeitsablauf durch die Verwaltung der verschiedenen beteiligten Medien- und Dokumentenformate.

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Foundation-Modelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- Amazon Transcribe ist ein automatischer Spracherkennungsdienst, der Modelle für maschinelles Lernen verwendet, um Audio in Text umzuwandeln.

Andere Tools

- LangChainist ein Framework für die Entwicklung von Anwendungen, die auf Large Language Models (LLMs) basieren.

Code-Repository

Der Code für dieses Muster ist im GitHub genai-knowledge-captureRepository verfügbar.

Das Code-Repository enthält die folgenden Dateien und Ordner:

- `assets`Ordner — Die statischen Ressourcen für die Lösung, z. B. das Architekturdiagramm und der öffentliche Datensatz

- `code/lambdas`folder — Der Python-Code für alle Lambda-Funktionen
  - `code/lambdas/generate`folder — Der Python-Code, der aus den zusammengefassten Daten im S3-Bucket ein Dokument generiert
  - `code/lambdas/preprocess`folder — Der Python-Code, der die Eingaben für die Step Functions Functions-Zustandsmaschine verarbeitet
  - `code/lambdas/summarize`folder — Der Python-Code, der die transkribierten Daten mithilfe des Amazon Bedrock-Service zusammenfasst
  - `code/lambdas/transcribe`folder — Der Python-Code, der Sprachdaten (Audiodatei) mithilfe von Amazon Transcribe in Text konvertiert
  - `code/lambdas/validate`folder — Der Python-Code, der überprüft, ob sich alle Antworten auf dasselbe Thema beziehen
- `code/code_stack.py`— Die AWS-CDK-Konstrukt-Python-Datei, die zur Erstellung von AWS-Ressourcen verwendet wird
- `app.py`— Die Python-Datei der AWS-CDK-App, die zur Bereitstellung von AWS-Ressourcen im AWS-Zielkonto verwendet wird
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die für das AWS-CDK installiert werden müssen
- `cdk.json`— Die Eingabedatei zur Bereitstellung von Werten, die für die Erstellung von Ressourcen erforderlich sind

Bewährte Methoden

Das bereitgestellte Codebeispiel dient nur proof-of-concept (PoC) oder Pilotzwecken. Wenn Sie die Lösung in der Produktion einsetzen möchten, wenden Sie die folgenden bewährten Methoden an:

- Amazon S3 S3-Zugriffsprotokollierung aktivieren
- VPC-Flow-Logs aktivieren

Epen

AWS-Anmeldeinformationen auf Ihrer lokalen Workstation einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie Variablen für das Konto und die AWS-Regio n.	Führen Sie die folgenden Befehle aus, um AWS-Anmel deinformationen für das AWS-CDK mithilfe von Umgebungs variablen bereitzustellen. `export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number> export CDK_DEFAU LT_REGION=<Region>`	AWS DevOps, DevOps Ingenieur
Richten Sie das AWS-CLI mit dem Namen profile ein.	Um das benannte AWS-CLI-Profil für das Konto einzurich ten, folgen Sie den Anweisung en unter Konfiguration und Einstellungen der Anmeldein formationsdatei.	AWS DevOps, DevOps Ingenieur

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihre lokale Workstation.	Um das genai-knowledge-ca ptureRepository zu klonen, führen Sie den folgenden Befehl in Ihrem Terminal aus. `git clone https://g ithub.com/aws-samp`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/genai-knowledge-capture`	
(Optional) Ersetzen Sie die Audiodateien.	Gehen Sie wie folgt vor, um die Beispielanwendung so anzupassen, dass sie Ihre eigenen Daten einbezieht: 1. Navigieren Sie zu dem `assets/audio_samples` Ordner im geklonten Repository. 2. Löschen Sie die Ordner, die die Beispiel-Audiodateien enthalten. 3. Erstellen Sie einen Ordner für jedes Thema, das Sie analysieren möchten. 4. Übertragen Sie Ihre Audiodateien in die entsprechenden Ordner.	AWS DevOps, DevOps Ingenieur

Richten Sie die virtuelle Python-Umgebung ein.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd genai-knowledge-capture`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synthetisieren Sie den AWS-CDK-Code.	Führen Sie den folgenden Befehl aus, um den Code in eine CloudFormation AWS-Stack-Konfiguration zu konvertieren. `cdk synth`	AWS DevOps, DevOps Ingenieur

Konfiguration und Bereitstellung der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Zugriff auf das Basismodell bereit.	Aktivieren Sie den Zugriff auf das Modell Anthropic Claude 3 Sonnet für Ihr AWS-Konto. Anweisungen finden Sie in der Bedrock-Dokumentation unter Modellzugriff hinzufügen.	AWS DevOps
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe des AWS-CDK bereitzustellen: 1. (Optional) Aktualisieren Sie im Stammverzeichnis des geklonten Repositorys in der `app.py` Datei den CloudFormation AWS-Stack -Namen. Der Standard-Stack-Name lautet`genai-knowledge-capture-stack` .	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Führen Sie den Befehl aus, um Ressourcen bereitzustellen `cdk deploy`. Der `cdk deploy` Befehl verwendet Layer-3-Konstrukte, um eine Reihe von Lambda-Funktionen, einen S3-Bucket, ein Amazon SNS SNS-Thema und eine Step Functions Functions-Zustandsmaschine zu erstellen. Die Audiodateien im `assets/audio_samples` Ordner werden während der Bereitstellung in den S3-Bucket kopiert. 3. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 4. Vergewissern Sie sich, dass der Stack erfolgreich bereitgestellt wurde. Anweisungen finden Sie unter Überprüfen Ihres Stacks auf der CloudFormation AWS-Konsole.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das Amazon-SNS-Thema.	Gehen Sie wie folgt vor, um das Amazon SNS SNS-Thema für Benachrichtigungen zu abonnieren: 1. Wählen Sie in der CloudFormation Konsole im Navigationsbereich Stacks aus. 2. Wählen Sie den `genai-knowledge-capture-stack` Stapel aus. 3. Wählen Sie die Registerkarte Outputs. 4. Suchen Sie den Namen des Amazon SNS SNS-Themas mit dem Schlüssel `SNSTopicName` . 5. Konfigurieren Sie eine E-Mail-Adresse für den Empfang von Benachrichtigungen, indem Sie den Anweisungen unter Abonnieren einer E-Mail-Adresse für ein Amazon SNS SNS-Thema folgen.	Allgemeines AWS

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Zustandsmaschine aus.	1. Öffnen Sie die Step Functions Functions-Konsole. 2. Wählen Sie auf der Seite State Machines die Option genai-knowledge-capture-stack-state-machine aus. 3. Wählen Sie Start execution (Ausführung starten) aus. 4. (Optional) Geben Sie im Feld Name einen Namen für die Ausführung ein. 5. Geben Sie im Eingabebereich das folgende JSON-Objekt ein, indem Sie den Platzhaltertext ersetzen. Dabei gilt: • `<Name>` ist der Name, den Sie dem Dokument geben möchten. • `<S3 bucket name>` ist der Name des Amazon S3 S3-Buckets, der die Audiodateien enthält. • `<Folder path>` ist das Verzeichnis, das die Audiodateien enthält. `{ "documentName": "<Name>",`	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"audioFileFolderUri": "s3://<S3 bucket name>/<Folder path>"
	}</pre>
	6. Wählen Sie Start Execution aus.
	7. Überprüfen Sie auf der Seite mit den Ausführungsdetails die Ergebnisse und warten Sie, bis die Ausführung abgeschlossen ist.	

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	Nachdem Sie die Lösung getestet haben, bereinigen Sie die Ressourcen: 1. Löschen Sie alle Objekte aus dem S3-Bucket und anschließend den Bucket. Weitere Informationen finden Sie unter Löschen eines Buckets. 2. Führen Sie im geklonten Repository den Befehl `cdk destroy` aus.	AWS DevOps, DevOps Ingenieur

Zugehörige Ressourcen

AWS-Dokumentation

- Ressourcen von Amazon Bedrock:
  - Modellzugriff
  - Inferenzparameter für Fundamentmodelle
- AWS-CDK-Ressourcen:
  - Erste Schritte mit dem AWS CDK
  - Arbeiten mit dem AWS-CDK in Python
  - Behebung häufiger AWS-CDK-Probleme
  - Toolkit-Befehle
- Ressourcen für AWS Step Functions:
  - Erste Schritte mit AWS Step Functions
  - Fehlersuche
- Lambda-Funktionen mit Python erstellen
- Generativer KI-Anwendungsgenerator auf AWS

Sonstige Ressourcen

- LangChain Dokumentation

Generieren Sie personalisierte und neu eingestufte Empfehlungen mit Amazon Personalize

Erstellt von Bol Calaze (AWS), Matthew Chasse (AWS) und Taio Olajide (AWS)

Code-Repository: personalize-pet-recommendations	Umgebung: PoC oder Pilotprojekt	Technologien: Machine Learning und KI; Cloudnativ; DevOpsInfrastruktur; Serverless
Workload: Open-Source	AWS-Services: AWS CloudFormation; Amazon Kinesis Data Firehose ; AWS Lambda ; Amazon Personalize; AWS Step Functions	

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Amazon Personalize verwenden, um personalisierte Empfehlungen – einschließlich neu eingestufter Empfehlungen – für Ihre Benutzer zu generieren, die auf der Aufnahme von Echtzeit-Benutzerinteraktionsdaten dieser Benutzer basieren. Das in diesem Muster verwendete Beispielszenario basiert auf einer Website zur Einführung von Haustieren, die Empfehlungen für seine Benutzer auf der Grundlage ihrer Interaktionen generiert (z. B. welche Haustiere ein Benutzer besucht). Wenn Sie dem Beispielszenario folgen, erfahren Sie, wie Sie Amazon Kinesis Data Streams verwenden, um Interaktionsdaten aufzunehmen, AWS Lambda, um Empfehlungen zu generieren und die Empfehlungen neu anzuordnen, und Amazon Data Firehose, um die Daten in einem Amazon Simple Storage Service (Amazon S3)-Bucket zu speichern. Sie lernen auch, AWS Step Functions zu verwenden, um einen Zustandsautomaten zu erstellen, der die Lösungsversion (d. h. ein trainiertes Modell) verwaltet, die Ihre Empfehlungen generiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einem bootstrapped AWS Cloud Development Kit (AWS CDK)
- AWS Command Line Interface (AWS CLI) mit konfigurierten Anmeldeinformationen

- Python 3.9

Produktversionen

- Python 3.9
- AWS CDK 2.23.0 oder höher
- AWS CLI 2.7.27 oder höher

Architektur

Technologie-Stack

- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Personalize
- Amazon Simple Storage Service (Amazon S3)
- AWS Cloud Development Kit (AWS-CDK)
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- AWS Lambda
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm veranschaulicht eine Pipeline für die Aufnahme von Echtzeitdaten in Amazon Personalize. Die Pipeline verwendet diese Daten dann, um personalisierte und neu eingestufte Empfehlungen für Benutzer zu generieren.

Das Diagramm zeigt den folgenden Workflow:

1. Kinesis Data Streams nimmt Echtzeit-Benutzerdaten (z. B. Ereignisse wie besuchte Haustiere) zur Verarbeitung durch Lambda und Firehose auf.
2. Eine Lambda-Funktion verarbeitet die Datensätze aus Kinesis Data Streams und führt einen API-Aufruf durch, um die Benutzerinteraktion im Datensatz einem Ereignis-Tracker in Amazon Personalize hinzuzufügen.

3. Eine zeitbasierte Regel ruft einen Step-Functions-Zustandsautomaten auf und generiert neue Lösungsversionen für die Empfehlung und die Neurangierung von Modellen, indem die Ereignisse aus dem Ereignis-Tracker in Amazon Personalize verwendet werden.
4. Amazon-Personalize-Kampagnen werden vom Zustandsautomaten aktualisiert, um die neue Lösungsversion zu verwenden.
5. Lambda sortiert die Liste der empfohlenen Elemente neu, indem es die Kampagne zum erneuten Rangwechsel von Amazon Personalize aufruft.
6. Lambda ruft die Liste der empfohlenen Elemente ab, indem es die Amazon-Personalize-Empfehlungskampagne aufruft.
7. Firehose speichert die Ereignisse in einem S3-Bucket, in dem auf sie als historische Daten zugegriffen werden kann.

Tools

AWS-Tools

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Data Firehose unterstützt Sie bei der Bereitstellung von Echtzeit-Streaming-Daten an andere AWS-Services, benutzerdefinierte HTTP-Endpunkte und HTTP-Endpunkte, die unterstützten Drittanbietern gehören.
- Amazon Kinesis Data Streams hilft Ihnen, große Streams von Datensätzen in Echtzeit zu sammeln und zu verarbeiten.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Personalize ist ein vollständig verwalteter Machine Learning (ML)-Service, mit dem Sie Elementempfehlungen für Ihre Benutzer basierend auf Ihren Daten generieren können.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Andere Tools

- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.
- Python ist eine Allzweck-Computer-Programmiersprache.

Code

Der Code für dieses Muster ist im GitHub Bol Recommender-Repository verfügbar. Sie können die AWS- CloudFormation Vorlage aus diesem Repository verwenden, um die Ressourcen für die Beispiellösung bereitzustellen.

Hinweis: Die Amazon-Personalize-Lösungsversionen, der Ereignis-Tracker und Kampagnen werden durch benutzerdefinierte Ressourcen (innerhalb der -Infrastruktur) unterstützt, die sich auf native CloudFormation Ressourcen erweitern.

Sekunden

Erstellen der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine isolierte Python-Umgebung.	Mac/Linux-Einrichtung 1. Um eine virtuelle Umgebung manuell zu erstellen, führen Sie den `$ python3 -m venv .venv` Befehl von Ihrem Terminal aus aus. 2. Führen Sie nach Abschluss des Initialisierungsvorgangs den `$ source .venv/bin/activate` Befehl aus, um die virtuelle Umgebung zu aktivieren. Windows-Einrichtung Um eine virtuelle Umgebung manuell zu erstellen, führen	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den `% .venv\Scripts \activate.bat` Befehl von Ihrem Terminal aus aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synthetisieren Sie die CloudFormation Vorlage.	1. Um die erforderlichen Abhängigkeiten zu installieren, führen Sie den `$ pip install -r requirements.txt` Befehl von Ihrem Terminal aus aus. 2. Legen Sie in der AWS CLI die folgenden Umgebungsvariablen fest: • `export ACCOUNT_ID=123456789` • `export CDK_DEPLOY_REGION=us-east-1` • `export CDK_ENVIRONMENT=dev` 3. Aktualisieren Sie `vpcId` in der `-config/{env}.yml` Datei so, dass sie Ihrer Virtual Private Cloud (VPC)-ID entspricht. 4. Um die CloudFormation Vorlage für diesen Code zu synthetisieren, führen Sie den `$ cdk synth` Befehl aus. Hinweis: In Schritt 2 `CDK_ENVIRONMENT` bezieht sich auf die `-config/{env}.yml` Datei.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen bereit und erstellen Sie eine Infrastruktur.	Um die Lösungsressourcen bereitzustellen, führen Sie den `./deploy.sh` Befehl von Ihrem Terminal aus aus. Mit diesem Befehl werden die erforderlichen Python-Abhängigkeiten installiert. Ein Python-Skript erstellt einen S3-Bucket und einen AWS Key Management Service (AWS KMS)-Schlüssel und fügt dann die Seed-Daten für die ersten Modellerstellungen hinzu. Schließlich wird das Skript ausgeführt, `cdk deploy` um die verbleibende Infrastruktur zu erstellen. Hinweis: Das erste Modelltraining findet während der Stack-Erstellung statt. Es kann bis zu zwei Stunden dauern, bis der Stack die Erstellung abgeschlossen hat.	DevOps Techniker

Zugehörige Ressourcen

- Bol Empfehlung (GitHub)
- AWS-CDK-Referenzdokumentation
- Boto3-Dokumentation
- Optimieren Sie personalisierte Empfehlungen für eine Geschäftsmetrik Ihrer Wahl mit Amazon Personalize (AWS Machine Learning Blog)

Zusätzliche Informationen

Beispiel für Nutzlasten und Antworten

Empfehlungs-Lambda-Funktion

Um Empfehlungen abzurufen, senden Sie eine Anfrage an die Empfehlungs-Lambda-Funktion mit einer Nutzlast im folgenden Format:

```
{
  "userId": "3578196281679609099",
  "limit": 6
}
```

Die folgende Beispielantwort enthält eine Liste von Arztgruppen:

```
[{"id": "1-domestic short hair-1-1"},
{"id": "1-domestic short hair-3-3"},
{"id": "1-domestic short hair-3-2"},
{"id": "1-domestic short hair-1-2"},
{"id": "1-domestic short hair-3-1"},
{"id": "2-beagle-3-3"},
```

Wenn Sie das `userId` Feld auslassen, gibt die Funktion allgemeine Empfehlungen zurück.

Neuranging der Lambda-Funktion

Um das Re-Ranking zu verwenden, senden Sie eine Anfrage an die Re-Ranking-Lambda-Funktion. Die Nutzlast enthält die `userId` aller Element-IDs, die neu eingestuft werden sollen, und ihre Metadaten. Die folgenden Beispieldaten verwenden die Pets-Klassen für `animal_species_id` (1=cat, 2=dog) und Ganzzahlen 1-5 für `animal_age_id` und `animal_size_id`:

```
{
   "userId":"12345",
   "itemMetadataList":[
      {
         "itemId":"1",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
```

```
            "animal_age_id":"2"
         }
      },
      {
         "itemId":"2",
         "animalMetadata":{
            "animal_species_id":"1",
            "animal_primary_breed_id":"Egyptian_Mau",
            "animal_size_id":"1",
            "animal_age_id":"1"
         }
      },
      {
         "itemId":"3",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      }
   ]
}
```

Die Lambda-Funktion sortiert diese Elemente neu und gibt dann eine geordnete Liste zurück, die die Element-IDs und die direkte Antwort von Amazon Personalize enthält. Dies ist eine Rangliste der Arztgruppen, in denen sich die Elemente befinden, und ihrer Punktzahl. Amazon Personalize verwendet User-Personalization- und Personalized-Ranking-Rezepte, um eine Punktzahl für jedes Element in die Empfehlungen aufzunehmen. Diese Punktzahlen stellen die relative Sicherheit dar, die Amazon Personalize darüber hat, welches Element der Benutzer als Nächstes auswählen wird. Höhere Punktzahlen bedeuten eine größere Gewissheit.

```
{
   "ranking":[
      "1",
      "3",
      "2"
   ],
   "personalizeResponse":{
      "ResponseMetadata":{
         "RequestId":"a2ec0417-9dcd-4986-8341-a3b3d26cd694",
         "HTTPStatusCode":200,
```

```
         "HTTPHeaders":{
            "date":"Thu, 16 Jun 2022 22:23:33 GMT",
            "content-type":"application/json",
            "content-length":"243",
            "connection":"keep-alive",
            "x-amzn-requestid":"a2ec0417-9dcd-4986-8341-a3b3d26cd694"
         },
         "RetryAttempts":0
      },
      "personalizedRanking":[
         {
            "itemId":"2-Saint_Bernard-3-2",
            "score":0.8947961
         },
         {
            "itemId":"1-Siamese-1-1",
            "score":0.105204
         }
      ],
      "recommendationId":"RID-d97c7a87-bd4e-47b5-a89b-ac1d19386aec"
   }
}
```

Amazon Kinesis-Nutzlast

Die Nutzlast, die an Amazon Kinesis gesendet werden soll, hat das folgende Format:

```
{
    "Partitionkey": "randomstring",
    "Data": {
        "userId": "12345",
        "sessionId": "sessionId4545454",
        "eventType": "DetailView",
        "animalMetadata": {
            "animal_species_id": "1",
            "animal_primary_breed_id": "Russian_Blue",
            "animal_size_id": "1",
            "animal_age_id": "2"
        },
        "animal_id": "98765"

    }
}
```

Hinweis: Das `userId` Feld wird für einen nicht authentifizierten Benutzer entfernt.

Trainieren und implementieren Sie ein benutzerdefiniertes GPU-unterstütztes ML-Modell auf Amazon SageMaker

Umgebung: PoC oder Pilotprojekt	Technologien: Maschinelles Lernen und KI; Container und Microservices	AWS-Dienste: Amazon ECS; Amazon SageMaker

Übersicht

Um die Vorteile von NVIDIA-GPUs voll auszuschöpfen, müssen zunächst bestimmte Umgebungsvariablen eingerichtet und bereitgestellt werden, die von Grafikprozessoren (GPU) unterstützt werden. Es kann jedoch zeitaufwändig sein, die Umgebung einzurichten und sie mit der SageMaker Amazon-Architektur in der Amazon Web Services (AWS) Cloud kompatibel zu machen.

Dieses Muster hilft Ihnen, mithilfe von Amazon ein benutzerdefiniertes GPU-unterstütztes ML-Modell zu trainieren und zu erstellen. SageMaker Es enthält Schritte zum Trainieren und Bereitstellen eines benutzerdefinierten CatBoost Modells, das auf einem Open-Source-Datensatz mit Amazon-Rezensionen basiert. Anschließend können Sie die Leistung auf einer `p3.16xlarge` Amazon Elastic Compute Cloud (Amazon EC2) -Instance vergleichen.

Dieses Muster ist nützlich, wenn Ihr Unternehmen bestehende GPU-gestützte ML-Modelle einsetzen möchte. SageMaker Ihre Datenwissenschaftler können den Schritten in diesem Muster folgen, um NVIDIA-GPU-unterstützte Container zu erstellen und ML-Modelle auf diesen Containern bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Quell-Bucket von Amazon Simple Storage Service (Amazon S3) zum Speichern der Modellartefakte und Prognosen.
- Ein Verständnis von SageMaker Notebook-Instances und Jupyter-Notebooks.
- Ein Verständnis dafür, wie eine AWS Identity and Access Management (IAM) -Rolle mit grundlegenden SageMaker Rollenberechtigungen, S3-Bucket-Zugriffs- und

Aktualisierungsberechtigungen sowie zusätzlichen Berechtigungen für Amazon Elastic Container Registry (Amazon ECR) erstellt wird.

Einschränkungen

- Dieses Muster ist für überwachte ML-Workloads mit einem in Python geschriebenen Train-and-Deploy-Code vorgesehen.

Architektur

Technologie-Stack

- SageMaker
- Amazon ECR

Tools

Tools

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon SageMaker — SageMaker ist ein vollständig verwalteter ML-Service.
- Docker — Docker ist eine Softwareplattform zum schnellen Erstellen, Testen und Bereitstellen von Anwendungen.
- Python — Python ist eine Programmiersprache.

Code

Der Code für dieses Muster ist unter GitHub Implementierung eines Bewertungsklassifikationsmodells mit Catboost und SageMaker Repository verfügbar.

Epen

Vorbereitung der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle und fügen Sie die erforderl ichen Richtlinien hinzu.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die IAM-Konsole und erstellen Sie eine neue IAM-Rolle. Weisen Sie der IAM-Rolle die folgenden Richtlinien zu: • `AmazonEC2Container RegistryFullAccess` • `AmazonS3FullAccess` • `AmazonSageMakerFul lAccess` Weitere Informationen dazu finden Sie in der SageMaker Amazon-Dokumentation unter Eine Notebook-Instance erstellen.	Data Scientist
Erstellen Sie die SageMaker Notebook-Instanz.	Öffnen Sie die SageMaker Konsole, wählen Sie Notebook-Instanzen und dann Notebook-Instanz erstellen aus. Wählen Sie für die IAM-Rolle die IAM-Rolle aus, die Sie zuvor erstellt haben. Konfigurieren Sie die Notebook-Instanz gemäß Ihren Anforderungen und	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Notebook-Instanz erstellen. Ausführliche Schritte und Anweisungen finden Sie in der SageMaker Amazon-Dokumentation unter Eine Notebook-Instance erstellen.	
Klonen Sie das Repository	Öffnen Sie das Terminal in der SageMaker Notebook-Instance und klonen Sie das Klassifizierungsmodell GitHub Implementing a review with Catboost and SageMaker repository, indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samples/review-classification-using-catboost-sagemaker.git`	
Starten Sie das Jupyter-Notebook.	Starten Sie das `Review classification model with Catboost and SageMaker.ipynb` Jupyter-Notebook, das die vordefinierten Schritte enthält.	Data Scientist

Feature-Engineering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Befehle im Jupyter-Notebook aus.	Öffnen Sie das Jupyter-Notizbuch und führen Sie die Befehle aus den folgenden Geschichten aus, um die Daten für das Training Ihres ML-Modells vorzubereiten.	Data Scientist

Lesen Sie die Daten aus dem S3-Bucket.	`import pandas as pd`
	`import csv`
	`fname = 's3://amazon-reviews-pds/tsv/amazon_reviews_us_Digital_Video_Download_v1_00.tsv.gz'`
	`df = pd.read_csv(fname, sep='\t',delimiter='\t',error_bad_lines=False)`
		Data Scientist

Verarbeiten Sie die Daten vor.	`import numpy as np`
	`def pre_process(df):`
	
	`  df.fillna(value={'review_body': '', 'review_headline': ''}, inplace=True)`
	`  df.fillna( value={'verified_purchase': 'Unk'}, inplace=True)`
	
	`  df.fillna(0, inplace=True)`
	`  return df`
	`df = pre_process(df)`
	`df.review_date = pd.to_datetime(df.review_date)`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`df['target'] = np.where(df['star_rating']>=4,1,0)` Hinweis: Dieser Code ersetzt Nullwerte in der `'review_body'` durch eine leere Zeichenfolge und ersetzt die `'verified_purchase'` Spalte durch `'Unk'`, was „unbekannt“ bedeutet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Teilen Sie die Daten in Trainings-, Validierungs- und Testdatensätze auf.	Um die Verteilung des Ziellabels über die aufgeteilten Datensätze hinweg identisch zu halten, müssen Sie die Stichprobe mithilfe der Scikit-Learn-Bibliothek stratifizieren.
	`from sklearn.model_selection import StratifiedShuffleSplit`
	`sss = StratifiedShuffleSplit(n_splits=2, test_size=0.10, random_state=0)`
	`sss.get_n_splits(df, df['target'])`
	`for train_index, test_index in sss.split(df, df['target']):`
	`X_train_vallid , X_test = df.iloc[train_index], df.iloc[test_index]`
	
	`sss.get_n_splits(X_train_vallid, X_train_vallid['target'])`
	`for train_index, test_index in sss.split(X_train_vallid, X_train_vallid['target']):`
	`X_train , X_valid = X_train_vallid.iloc[train_index],`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`X_train_vallid.ilo c[test_index]`	

Docker-Image erstellen, ausführen und auf Amazon ECR übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das Docker-Im age vor und übertragen Sie es.	Führen Sie im Jupyter-N otizbuch die Befehle aus den folgenden Storys aus, um das Docker-Image vorzubereiten und es an Amazon ECR zu übertragen.	ML-Ingenieur

Erstellen Sie ein Repository in Amazon ECR.	`%%sh`
	
	`algorithm_name=s agemaker-catboost- github-gpu-img`
	
	`chmod +x code/train chmod +x code/serve`
	
	`account=$(aws sts get- caller-identity -- query Account --output text)`
	
	`# Get the region defined in the current configuration (default to us-west-2 if none defined) region=$(aws configure get region) region=${region:-us- east-1}`
		ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`fullname="${accou nt}.dkr.ecr.${regi on}.amazonaws.com/ ${algorithm_name}: latest"`
	
	`aws ecr create-re pository --repository- name "${algorithm_name} " > /dev/nul`	

Erstellen Sie lokal ein Docker-Image.	`docker build -t "${algorithm_name}" . docker tag ${algorit hm_name} ${fullname}`	ML-Ingenieur
Führen Sie das Docker-Image aus und übertragen Sie es an Amazon ECR.	`docker push ${fullname}`	ML-Ingenieur

Training

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SageMaker Hyperparameter-Tuning-Job.	Führen Sie im Jupyter-N otebook die Befehle aus den folgenden Storys aus, um mithilfe Ihres Docker-Images einen SageMaker Hyperpara meter-Tuning-Job zu erstellen.	Data Scientist
SageMaker Erstellen Sie einen Schätzer.	Erstellen Sie einen SageMaker Schätzer, indem Sie den Namen des Docker-Im ages verwenden.	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`import sagemaker as sage`
	`from time import gmtime,`
	` strftime`
	`sess = sage.Session()`
	`from sagemaker.tuner`
	` import IntegerPa`
	`rameter, Categoric`
	`alParameter, Continuou`
	`sParameter, Hyperpara`
	`meterTuner`
	
	`account = sess.boto`
	`_session.client('s`
	`ts').get_caller_id`
	`entity()['Account']`
	`region = sess.boto`
	`_session.region_name`
	`image = '{}.dkr.e`
	`cr.{}.amazonaws.co`
	`m/sagemaker-catboo`
	`st-github-gpu-img:`
	`latest'.format(acc`
	`ount, region)`
	`tree_hpo = sage.esti`
	`mator.Estimator(im`
	`age,`
	
	` role, 1,`
	
	` 'ml.p3.16xlarge',`
	
	`  train_volume_size =`
	` 100,`
	
	`  output_path="s3://`
	`{}/sagemaker/DEMO-`
	`GPU-Catboost/outpu`
	`t".format(bucket),`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`  sagemaker_session=sess)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen HPO-Job.	Erstellen Sie einen Tuning-Job für Hyperparameter-Optimierung (HPO) mit Parameterbereichen und übergeben Sie die Train- und Validierungssätze als Parameter an die Funktion.
	
	`hyperparameter_ranges = {'iterations': IntegerParameter(80000, 130000),`
	
	`'max_depth': IntegerParameter(6, 10),`
	
	`'max_ctr_complexity': IntegerParameter(4, 10),`
	
	`'learning_rate': ContinuousParameter(0.01, 0.5)}`
	
	`objective_metric_name = 'auc'`
	`metric_definitions = [{'Name': 'auc',`
	
	`'Regex': 'auc: ([0-9\.]+)'}]`
	
	`tuner = HyperparameterTuner(tree_hpo,`
	
	`objective_metric_name,`
	
	`hyperparameter_ranges,`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`metric_definitions ,`
	
	`objective_type='Maximize',`
	
	`max_jobs=50,`
	
	`max_parallel_jobs=2)`	

Führen Sie den HPO-Job aus.	`train_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/train/'`
	`valid_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/valid/'`
	
	`tuner.fit({'train': train_location, 'validation': valid_location })`
		Data Scientist

Erhalte den Trainingsjob mit der besten Leistung.	`import sagemaker as sage`
	`from time import gmtime, strftime`
	`sess = sage.Session()`
	
	`best_job =tuner.best_training_job()`
		Data Scientist

Batch-Transformation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SageMaker Batch-Transformationsjob für Testdaten zur Modellvorhersage.	Führen Sie im Jupyter-Notizbuch die Befehle aus den folgenden Geschichten aus, um das Modell aus Ihrem SageMaker Hyperparameter-Tuning-Job zu erstellen, und senden Sie einen SageMaker Batch-Transformationsjob für die Testdaten zur Modellvorhersage.	Data Scientist

Erstellen Sie das Modell. SageMaker	Erstellen Sie ein Modell im SageMaker Modell mit dem besten Trainingsjob.
	`attached_estimator = sage.estimator.Estimator.attach(best_job)`
	`output_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/'`
	`input_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test/'`
	`transformer = attached_estimator.transformer(instance_count=1,`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`instance_type='ml.p3.16xlarge',`
	
	`assemble_with='Line',`
	
	`accept='text/csv',`
	
	`max_payload=1,`
	
	`output_path=output_path,`
	
	`env = {'SAGEMAKER_MODEL_SERVER_TIMEOUT' : '3600' })`	

Erstellen Sie einen Batch-Transformationsauftrag.	Erstellen Sie einen Batch-Transformationsauftrag für den Testdatensatz.
	
	`transformer.transform(input_path,`
	
	`content_type='text/csv',`
	
	`split_type='Line')`
		Data Scientist

Analysieren Sie die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lesen Sie die Ergebnisse und bewerten Sie die Leistung des Modells.	Führen Sie im Jupyter-N otizbuch die Befehle aus den folgenden Geschichten aus, um die Ergebnisse zu lesen und die Leistung des Modells anhand der Modellmetriken Area Under the ROC Curve (ROC-AUC) und Area Under the Precision Recall Curve (PR-AUC) zu bewerten. Weitere Informationen dazu finden Sie unter Amazon Machine Learning-Schlüssel konzepte in der Dokumenta tion zu Amazon Machine Learning (Amazon ML).	Data Scientist

Lesen Sie die Ergebnisse des Batch-Transformationsauftra gs.	Lesen Sie die Ergebnisse des Batch-Transformationsauftra gs in einen Datenrahmen ein.
	
	`file_name = 's3://'+b ucket+'/sagemaker/ DEMO-GPU-Catboost/ data/test-predicti ons/file_1.out'`
	
	`results = pd.read_csv(file_n ame, names=['r eview_id','target' ,'score'] ,sep='\t' ,escapechar ='\\' , quoting=csv.QUOTE_ NONE,`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`lineterminator='\n',quotechar='"').dropna()`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bewerten Sie die Leistungskennzahlen.	Bewerten Sie die Leistung des Modells auf ROC-AUC und PR-AUC.
	
	`from sklearn import metrics`
	`import matplotlib`
	`import pandas as pd`
	`matplotlib.use('agg', warn=False, force=True)`
	`from matplotlib import pyplot as plt`
	
	`%matplotlib inline`
	
	`def analyze_results(labels, predictions):`
	`precision, recall, thresholds = metrics.precision_recall_curve(labels, predictions)`
	`auc = metrics.auc(recall, precision)`
	
	`fpr, tpr, _ = metrics.roc_curve(labels, predictions)`
	`roc_auc_score = metrics.roc_auc_score(labels, predictions)`
	
	`print('Neural-Nets: ROC auc=%.3f' % (roc_auc_score))`
	
	`plt.plot(fpr, tpr, label="data 1, auc=" + str(roc_auc_score))`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`    plt.xlabel('1-Specificity')`
	`    plt.ylabel('Sensitivity')`
	`    plt.legend(loc=4)`
	`    plt.show()`
	
	`    lr_precision, lr_recall, _ = metrics.precision_recall_curve(labels, predictions)`
	`    lr_auc = metrics.auc(lr_recall, lr_precision)`
	`    # summarize scores`
	`    print('Neural-Nets: PR auc=%.3f' % ( lr_auc))`
	`    # plot the precision-recall curves`
	`    no_skill = len(labels[labels==1.0]) / len(labels)`
	`    plt.plot([0, 1], [no_skill, no_skill], linestyle='--', label='No Skill')`
	
	`    plt.plot(lr_recall, lr_precision, marker='.', label='Neural-Nets')`
	`    # axis labels`
	`    plt.xlabel('Recall')`
	`    plt.ylabel('Precision')`
	`    # show the legend`
	`    plt.legend()`
	`    # show the plot`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`plt.show()`
	
	`return auc`
	
	`analyze_results(results['target'].values,results['score'].values)`	

Zugehörige Ressourcen

- Trainieren und hosten Sie Scikit-Learn-Modelle in Amazon, SageMaker indem Sie einen Scikit-Docker-Container erstellen

Zusätzliche Informationen

Die folgende Liste zeigt die verschiedenen Elemente der Docker-Datei, die im Docker-Image Build, Run und Push in Amazon ECR Epic ausgeführt wird.

Installieren Sie Python mit aws-cli.

```
FROM amazonlinux:1

 RUN yum update -y && yum install -y python36 python36-devel python36-libs python36-
tools python36-pip && \
 yum install gcc tar make wget util-linux kmod man sudo git -y && \
 yum install wget -y && \
 yum install aws-cli -y && \
 yum install nginx -y && \
yum install gcc-c++.noarch -y && yum clean all
```

Installieren Sie die Python-Pakete

```
RUN pip-3.6 install --no-cache-dir --upgrade pip && \pip3 install --no-cache-dir --
upgrade setuptools && \
```

```
pip3 install Cython && \
pip3 install --no-cache-dir numpy==1.16.0 scipy==1.4.1 scikit-learn==0.20.3
 pandas==0.24.2 \
flask gevent gunicorn boto3 s3fs  matplotlib joblib catboost==0.20.2
```

Installieren Sie CUDA und cuDNN

```
RUN wget https://developer.nvidia.com/compute/cuda/9.0/Prod/local_installers/
cuda_9.0.176_384.81_linux-run \
&& chmod u+x cuda_9.0.176_384.81_linux-run \
&& ./cuda_9.0.176_384.81_linux-run --tmpdir=/data --silent --toolkit --override \
&& wget https://custom-gpu-sagemaker-image.s3.amazonaws.com/installation/cudnn-9.0-
linux-x64-v7.tgz \
&& tar -xvzf cudnn-9.0-linux-x64-v7.tgz \
&& cp /data/cuda/include/cudnn.h /usr/local/cuda/include \
&& cp /data/cuda/lib64/libcudnn* /usr/local/cuda/lib64 \

&& chmod a+r /usr/local/cuda/include/cudnn.h /usr/local/cuda/lib64/libcudnn* \
&&  rm -rf /data/*
```

Erstellen Sie die erforderliche Verzeichnisstruktur für SageMaker

```
RUN mkdir /opt/ml /opt/ml/input /opt/ml/input/config /opt/ml/input/data /opt/ml/input/
data/training /opt/ml/model /opt/ml/output /opt/program
```

Stellen Sie die NVIDIA-Umgebungsvariablen ein

```
ENV PYTHONPATH=/opt/program
ENV PYTHONUNBUFFERED=TRUE
ENV PYTHONDONTWRITEBYTECODE=TRUE
ENV PATH="/opt/program:${PATH}"

# Set NVIDIA mount environments
ENV LD_LIBRARY_PATH=/usr/local/nvidia/lib:/usr/local/nvidia/lib64:$LD_LIBRARY_PATH
ENV NVIDIA_VISIBLE_DEVICES="all"
ENV NVIDIA_DRIVER_CAPABILITIES="compute,utility"
ENV NVIDIA_REQUIRE_CUDA "cuda>=9.0"
```

Kopieren Sie Trainings- und Inferenzdateien in das Docker-Image

```
COPY code/* /opt/program/
```

```
WORKDIR /opt/program
```

Verwenden Sie SageMaker Verarbeitung für verteiltes Feature-Engineering von ML-Datensätzen im Terabyte-Bereich

Erstellt von Bol Boom Hower (AWS)

Umgebung: Produktion	Technologien: Machine Learning und KI; Big Data	AWS-Services: Amazon SageMaker

Übersicht

Viele Datensätze im Terabyte-Bereich oder größer bestehen häufig aus einer hierarchischen Ordnerstruktur, und die Dateien im Datensatz teilen sich manchmal Abhängigkeiten. Aus diesem Grund müssen Techniker und Datenwissenschaftler für Machine Learning (ML) sorgfältige Designentscheidungen treffen, um solche Daten auf das Modelltraining und die Inferenz vorzubereiten. Dieses Muster zeigt, wie Sie manuelle Makro-Sharding- und Microsharding-Techniken in Kombination mit Amazon SageMaker Processing und virtueller CPU (vCPU)-Parallelisierung verwenden können, um Feature-Engineering-Prozesse für komplizierte Big-Data-ML-Datensätze effizient zu skalieren.

Dieses Muster definiert Makro-Sharding als die Aufteilung von Datenverzeichnissen auf mehrere Maschinen zur Verarbeitung und Micro-Sharding als die Aufteilung von Daten auf jedem Computer auf mehrere Verarbeitungs-Threads. Das Muster demonstriert diese Techniken, indem Amazon SageMaker mit Beispieldatensätzen für Zeitreihen aus dem PhysioNet MIMIC--Datensatz verwendet wird. Durch die Implementierung der Techniken in diesem Muster können Sie die Verarbeitungszeit und die Kosten für Feature Engineering minimieren und gleichzeitig die Ressourcennutzung und Durchsatzeffizienz maximieren. Diese Optimierungen basieren auf verteilter SageMaker Verarbeitung auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances und vCPUs für ähnliche, große Datensätze, unabhängig vom Datentyp.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zugriff auf SageMaker Notebook-Instances oder SageMaker Studio, wenn Sie dieses Muster für Ihren eigenen Datensatz implementieren möchten. Wenn Sie Amazon SageMaker zum ersten Mal

verwenden, finden Sie weitere Informationen unter Erste Schritte mit Amazon SageMaker in der AWS-Dokumentation.

- SageMaker Studio, wenn Sie dieses Muster mit den PhysioNet MIMIC- Beispieldaten implementieren möchten.
- Das Muster verwendet SageMaker Verarbeitung, erfordert jedoch keine Erfahrung mit der Ausführung von SageMaker Verarbeitungsaufträgen.

Einschränkungen

- Dieses Muster eignet sich gut für ML-Datensätze, die voneinander abhängige Dateien enthalten. Diese Abhängigkeiten profitieren am meisten vom manuellen Makro-Sharding und der parallelen Ausführung mehrerer Einzel-Instance- SageMaker Verarbeitungsaufträge. Für Datensätze, in denen solche Abhängigkeiten nicht vorhanden sind, ist das `ShardedByS3Key` Feature in SageMaker Processing möglicherweise eine bessere Alternative zu Makro-Sharding, da es Sharded-Daten an mehrere Instances sendet, die von demselben Verarbeitungsauftrag verwaltet werden. Sie können jedoch die Microsharding-Strategie dieses Musters in beiden Szenarien implementieren, um Instance-vCPUs optimal zu nutzen.

Produktversionen

- Amazon SageMaker Python SDK Version 2

Architektur

Zieltechnologie-Stack

- Amazon Simple Storage Service (Amazon S3)
- Amazon SageMaker

Zielarchitektur

Makro-Sharding und verteilte EC2-Instances

Die 10 parallelen Prozesse, die in dieser Architektur dargestellt werden, spiegeln die Struktur des MIMIC- Datensatzes wider. (Prozesse werden zur Vereinfachung des Diagramms durch Ellipsen dargestellt.) Eine ähnliche Architektur gilt für jeden Datensatz, wenn Sie manuelles Makro-

Sharding verwenden. Im Fall von MIMIC- können Sie die Rohstruktur des Datensatzes zu Ihrem Vorteil verwenden, indem Sie jeden Ordner der Patientengruppe mit minimalem Aufwand separat verarbeiten. Im folgenden Diagramm wird der Datensatzgruppenblock auf der linken Seite angezeigt (1). Angesichts der verteilten Natur der Daten ist es sinnvoll, nach Patientengruppe zu fragmentieren.

Das manuelle Sharding nach Patientengruppe bedeutet jedoch, dass für jeden Ordner der Patientengruppe ein separater Verarbeitungsauftrag erforderlich ist, wie Sie im mittleren Abschnitt des Diagramms (2) sehen können, anstatt einen einzelnen Verarbeitungsauftrag mit mehreren EC2-Instances. Da die Daten von MIMIC- sowohl binäre microSD-Dateien als auch übereinstimmende textbasierte Header-Dateien enthalten und eine erforderliche Abhängigkeit von der wfdb-Bibliothek für die binäre Datenextraktion besteht, müssen alle Datensätze für einen bestimmten Patienten auf derselben Instance verfügbar gemacht werden. Die einzige Möglichkeit, sicherzustellen, dass auch die zugehörige Header-Datei jeder binären microSD-Datei vorhanden ist, besteht darin, manuelles Sharding zu implementieren, um jeden Shard innerhalb seines eigenen Verarbeitungsauftrags auszuführen und anzugeben, `s3_data_distribution_type='FullyReplicated'` wann Sie die Eingabe für den Verarbeitungsauftrag definieren. Wenn alternativ alle Daten in einem einzigen Verzeichnis verfügbar waren und zwischen Dateien keine Abhängigkeiten vorlagen, kann es sinnvoller sein, einen einzelnen Verarbeitungsauftrag mit mehreren EC2-Instances zu starten und `s3_data_distribution_type='ShardedByS3Key'` anzugeben. Die Angabe von `ShardedByS3Key` als Amazon S3-Datenverteilungstyp weist SageMaker an, Daten-Sharding automatisch über Instances hinweg zu verwalten.

Das Starten eines Verarbeitungsauftrags für jeden Ordner ist eine kosteneffiziente Methode zur Vorverarbeitung der Daten, da das gleichzeitige Ausführen mehrerer Instances Zeit spart. Für zusätzliche Kosten und Zeiteinsparungen können Sie Microsharding in jedem Verarbeitungsauftrag verwenden.

Microsharding und parallele vCPUs

Innerhalb jedes Verarbeitungsauftrags werden die gruppierten Daten weiter unterteilt, um die Nutzung aller verfügbaren vCPUs auf der SageMaker vollständig verwalteten EC2-Instance zu maximieren. Die Blöcke im mittleren Abschnitt des Diagramms (2) zeigen, was innerhalb jedes primären Verarbeitungsauftrags passiert. Der Inhalt der Ordner für Patientendaten wird je nach Anzahl der verfügbaren vCPUs auf der Instance abgeflacht und gleichmäßig aufgeteilt. Nachdem der Inhalt des Ordners aufgeteilt wurde, wird der gleich große Satz von Dateien zur Verarbeitung auf alle vCPUs verteilt. Wenn die Verarbeitung abgeschlossen ist, werden die Ergebnisse jeder vCPU für jeden Verarbeitungsauftrag zu einer einzigen Datendatei zusammengefasst.

Im angehängten Code werden diese Konzepte im folgenden Abschnitt der -`src/feature-engineering-pass1/preprocessing.py`Datei dargestellt.

```
def chunks(lst, n):
    """
    Yield successive n-sized chunks from lst.

    :param lst: list of elements to be divided
    :param n: number of elements per chunk
    :type lst: list
    :type n: int
    :return: generator comprising evenly sized chunks
    :rtype: class 'generator'
    """
    for i in range(0, len(lst), n):
        yield lst[i:i + n]


# Generate list of data files on machine
data_dir = input_dir
d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]
file_list = []
for ds in d_subs:
    file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))
dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in
 file_list if f[-4:] == '.dat']

# Split list of files into sub-lists
cpu_count = multiprocessing.cpu_count()
splits = int(len(dat_list) / cpu_count)
if splits == 0: splits = 1
dat_chunks = list(chunks(dat_list, splits))

# Parallelize processing of sub-lists across CPUs
ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in
 dat_chunks)

# Compile and pickle patient group dataframe
ws_df_group = pd.concat(ws_df_list)
ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})
ws_df_group.to_json(os.path.join(output_dir, group_data_out))
```

Eine Funktion, `chunks`, ist zunächst so definiert, dass sie eine bestimmte Liste verbraucht, indem sie sie in gleichmäßig dimensionierte Blöcke der Länge unterteilt `n` und diese Ergebnisse als Generator zurückgibt. Als Nächstes werden die Daten in allen Patientenordnern abgeflacht, indem eine Liste aller vorhandenen binärenTelefoniedateien kompiliert wird. Danach wird die Anzahl der auf der EC2-Instance verfügbaren vCPUs abgerufen. Die Liste der binären microSD-Dateien wird gleichmäßig auf diese vCPUs aufgeteilt`chunks`, indem aufgerufen wird. Anschließend wird jede microSD-Unterliste mithilfe der parallelen Klasse von joblib auf ihrer eigenen vCPU verarbeitet. Die Ergebnisse werden vom Verarbeitungsauftrag automatisch zu einer einzigen Liste von Datenrahmen kombiniert, die SageMaker dann weiter verarbeitet, bevor sie nach Abschluss des Auftrags in Amazon S3 geschrieben werden. In diesem Beispiel werden von den Verarbeitungsaufträgen 10 Dateien in Amazon S3 geschrieben (eine für jeden Auftrag).

Wenn alle anfänglichen Verarbeitungsaufträge abgeschlossen sind, kombiniert ein sekundärer Verarbeitungsauftrag, der im -Block rechts neben dem Diagramm angezeigt wird (3), die von jedem primären Verarbeitungsauftrag erzeugten Ausgabedateien und schreibt die kombinierte Ausgabe in Amazon S3 (4).

Tools

Tools

- Python – Der für dieses Muster verwendete Beispielcode ist Python (Version 3).
- SageMaker Studio – Amazon SageMaker Studio ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für Machine Learning, mit der Sie Ihre Machine-Learning-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können. Sie führen SageMaker Verarbeitungsaufträge mithilfe von Jupyter-Notebooks in SageMaker Studio aus.
- SageMaker Verarbeitung – Amazon SageMaker Processing bietet eine vereinfachte Möglichkeit, Ihre Datenverarbeitungs-Workloads auszuführen. In diesem Muster wird der Feature-Engineering-Code mithilfe von SageMaker Verarbeitungsaufträgen in großem Umfang implementiert.

Code

Die angehängte ZIP-Datei stellt den vollständigen Code für dieses Muster bereit. Im folgenden Abschnitt werden die Schritte zum Erstellen der Architektur für dieses Muster beschrieben. Jeder Schritt wird durch Beispielcode aus dem Anhang veranschaulicht.

Polen

Einrichten Ihrer SageMaker Studio-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf Amazon SageMaker Studio zu.	Integrieren Sie SageMaker Studio in Ihrem AWS-Konto, indem Sie den Anweisungen in der Amazon- SageMaker Dokumentation folgen.	Datenwissenschaftler, ML-Techniker
Installieren Sie das Dienstprogramm wget.	Installieren Sie wget, wenn Sie sich mit einer neuen SageMaker Studio-Konfiguration integriert haben oder diese Dienstprogramme noch nie in SageMaker Studio verwendet haben. Öffnen Sie zum Installieren von ein Terminalfenster in der SageMaker Studio-Konsole und führen Sie den folgenden Befehl aus: `sudo yum install wget`	Datenwissenschaftler, ML-Techniker
Laden Sie den Beispielcode herunter und entpacken Sie ihn.	Laden Sie die `attachments.zip` Datei im Abschnitt Anhänge herunter. Navigieren Sie in einem Terminalfenster zu dem Ordner, in den Sie die Datei heruntergeladen haben, und extrahieren Sie deren Inhalt:	Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`unzip attachment.zip`
	
	Navigieren Sie zu dem Ordner, in den Sie die ZIP-Datei extrahiert haben, und extrahieren Sie den Inhalt der `Scaled-Processing.zip` Datei.
	
	`unzip Scaled-Processing.zip`	

Laden Sie den Beispield atensatz von physionet.org herunter und laden Sie ihn in Amazon S3 hoch.	Führen Sie das `get_data.ipynb` Jupyter-Notebook in dem Ordner aus, der die `Scaled-Processing` Dateien enthält. Dieses Notebook lädt einen MIMIC--Beispieldatensatz von physionet.org herunter und lädt ihn in Ihren SageMaker Studio-Sitzungs-Bucket in Amazon S3 hoch.	Datenwissenschaftler, ML-Techniker

Konfigurieren des ersten Vorverarbeitungsskripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verflacht die Dateihierarchie in allen Unterverzeichnissen.	In großen Datensätzen wie MIMIC- werden Dateien häufig über mehrere Unterverz eichnisse verteilt, auch innerhalb einer logischen übergeordneten Gruppe. Ihr	Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Skript sollte so konfiguriert sein, dass alle Gruppenda teien in allen Unterverz eichnissen reduziert werden, wie der folgende Code zeigt.
	
	`# Generate list of .dat files on machine`
	`data_dir = input_dir`
	`d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]`
	`file_list = []`
	`for ds in d_subs:`
	`file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))`
	`dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in file_list if f[-4:] == '.dat']`
	
	Beachten Sie, dass die Beispielcodeausschnitte in diesem Epics aus der `src/feature-engineering-pass1/preprocessing.py` Datei stammen, die in der Anfügung bereitgestellt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Teilen Sie Dateien basierend auf der vCPU-Anzahl in Untergruppen auf.	Dateien sollten in gleich große Untergruppen oder Blöcke unterteilt werden, je nach Anzahl der vCPUs, die auf der Instance vorhanden sind, auf der das Skript ausgeführt wird. In diesem Schritt können Sie Code ähnlich dem folgenden implementieren.
	`# Split list of files into sub-lists`
	`cpu_count = multiprocessing.cpu_count()`
	`splits = int(len(dat_list) / cpu_count)`
	`if splits == 0: splits = 1`
	`dat_chunks = list(chunks(dat_list, splits))`
		Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Parallelisieren Sie die Verarbeitung von Untergrup pen über vCPUs hinweg.	Die Skriptlogik sollte so konfiguriert werden, dass alle Untergruppen parallel verarbeitet werden. Verwenden Sie dazu die `Parallel` Klasse und `delayed` Methode der Joblib-Bibliothek wie folgt. `# Parallelize processin g of sub-lists across CPUs ws_df_list = Parallel( n_jobs=-1, verbose=0) (delayed(run_process) (dc) for dc in dat_chunk s)`	Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Speichern Sie die Ausgabe einer einzelnen Dateigruppe in Amazon S3.	Wenn die parallele vCPU-Verarbeitung abgeschlossen ist, sollten die Ergebnisse jeder vCPU kombiniert und in den S3-Bucket-Pfad der Dateigruppe hochgeladen werden. Für diesen Schritt können Sie Code ähnlich dem folgenden verwenden.
	`# Compile and pickle patient group dataframe`
	`ws_df_group = pd.concat(ws_df_list)`
	`ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})`
	`ws_df_group.to_json(os.path.join(output_dir, group_data_out))`
		Datenwissenschaftler, ML-Techniker

Konfigurieren des zweiten Vorverarbeitungsskripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kombinieren Sie Datendateien, die über alle Verarbeitungsaufträge hinweg erzeugt wurden, auf denen das erste Skript ausgeführt wurde.	Das vorherige Skript gibt für jeden SageMaker Verarbeitungsauftrag, der eine Gruppe von Dateien aus dem Datensatz verarbeitet, eine einzelne Datei aus. Als Nächstes müssen Sie diese Ausgabedateien zu einem	Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	einzigen Objekt kombinieren und einen einzelnen Ausgabedatensatz in Amazon S3 schreiben. Dies wird in der `-src/feature-engineering-pass1p5/preprocessing.py` Datei, die im Anhang bereitgestellt wird, wie folgt demonstriert.
	
	`def write_parquet(wavs_df, path):`
	`    """`
	`    Write waveform summary dataframe to S3 in parquet format.`
	
	`    :param wavs_df: waveform summary dataframe`
	`    :param path: S3 directory prefix`
	`    :type wavs_df: pandas dataframe`
	`    :type path: str`
	`    :return: None`
	`    """`
	`    extra_args = {"ServerSideEncryption": "aws:kms"}`
	`    wr.s3.to_parquet(`
	`        df=wavs_df,`
	`        path=path,`
	`        compression='snappy',`
	`        s3_additional_kwargs=extra_args)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`def combine_data():`
	`"""`
	`Get combined data and write to parquet.`
	
	`:return: waveform summary dataframe`
	`:rtype: pandas dataframe`
	`"""`
	`wavs_df = get_data()`
	`wavs_df = normalize_signal_names(wavs_df)`
	`write_parquet(wavs_df, "s3://{}/{}/{}".format(bucket_xform, dataset_prefix, pass1p5out_data))`
	
	`return wavs_df`
	
	`wavs_df = combine_data()`	

Ausführen von Verarbeitungsaufträgen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den ersten Verarbeitungsauftrag aus.	Um Makrosharding durchzuführen, führen Sie für jede Dateigruppe einen separaten Verarbeitungsauftrag aus. Microsharding wird innerhalb jedes Verarbeitungsauftrags	Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	durchgeführt, da jeder Auftrag Ihr erstes Skript ausführt. Der folgende Code zeigt, wie ein Verarbeitungsauftrag für jedes Dateigruppenverzeichnis im folgenden Ausschnitt gestartet wird (in enthaltennotebooks/FeatExtract_Pass1.ipynb).
	
	`pat_groups = list(range(30,40))`
	`ts = str(int(time.time()))`
	
	`for group in pat_groups:`
	`  sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`  role=role,`
	
	`  instance_type='ml.m5.4xlarge',`
	
	`  instance_count=1,`
	
	`  volume_size_in_gb=5)`
	`  sklearn_processor.run(`
	`  code='../src/feature-engineering-pass1/preprocessing.py',`
	`  job_name='-'.join(['scaled-`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	processing-p1', str(group), ts]), arguments=["input_path", "/opt/ml/processing/input", "output_path", "/opt/ml/processing/output", "group_data_out", "ws_df_group.json"], inputs= [ProcessingInput(source=f's3://{sess.default_bucket()}/data_inputs/{group}', destination='/opt/ml/processing/input', s3_data_distribution_type='FullyReplicated')], outputs= [ProcessingOutput(source='/opt/ml/processing/output', destination=f's3://{sess.default_bucket()}/data_outputs/{group}'	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>)
	        ],
	        wait=False
	    )</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie den zweiten Verarbeitungsauftrag aus.	Um die vom ersten Satz von Verarbeitungsaufträgen generierten Ausgaben zu kombinieren und zusätzlic he Berechnungen für die Vorverarbeitung durchzufü hren, führen Sie Ihr zweites Skript mithilfe eines einzelnen SageMaker Verarbeitungsauftr ags aus. Der folgende Code zeigt dies (in enthalten `notebooks/FeatExtr act_Pass1p5.ipynb`).
	
	`ts = str(int(time.time( )))`
	`bucket = sess.defa ult_bucket()`
	
	`sklearn_processor =  SKLearnProcessor(f ramework_version=' 0.20.0',`
	
	`role=role,`
	
	`instance_ type='ml.t3.2xlarge',`
	
	`instance_ count=1,`
	
	`volume_si ze_in_gb=5)`
	`sklearn_processor.run(`
	`code='../src/featu re-engineering-pas s1p5/preprocessing .py',`
		Datenwissenschaftler, ML-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`job_name='-'.join(['scaled-processing', 'p1p5', ts]), arguments=['bucket', bucket, 'pass1out_prefix', 'data_outputs', 'pass1out_data', 'ws_df_group.json', 'pass1p5out_data', 'waveform_summary.parquet', 'statsdata_name', 'signal_stats.csv'], wait=True )`	

Zugehörige Ressourcen

- Integrieren von Amazon SageMaker Studio mithilfe von Schnellstart (SageMaker Dokumentation)
- Prozessdaten (SageMaker Dokumentation)
- Datenverarbeitung mit scikit-learn (SageMaker Dokumentation)
- joblib.Parallel-Dokumentation
- Moody, B., Moody, G., Bolrroel, M., Clifford, G. D. und Silva, I. (2020). MIMIC- Waveform Database (Version 1.0). PhysioNet.
- Bol, A. E. W., Pollard, T. J., Shen, L., Lehman, L. H., Feng, M., Ghassemi, M., Moody, B., Sovits, P., Celi, L. A. und Mark, R. G. (2016). MIMIC-, eine frei zugängliche Datenbank für medizinische Pflege . Daten zu , 3, 160035.
- MIMIC- Waveform Database-Lizenz

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Visualisieren Sie KI/ML-Modellergebnisse mit Flask und AWS Elastic Beanstalk

Erstellt von Chris Caudill (AWS) und Durga Sury

Umgebung: PoC oder Pilotprojekt	Technologien: Maschinelles Lernen und KI; Analytik DevOps; Web- und mobile Apps	Arbeitslast: Open Source
AWS-Services: Amazon Comprehend; AWS Elastic Beanstalk		

Übersicht

Die Visualisierung der Ergebnisse von Diensten für künstliche Intelligenz und maschinelles Lernen (AI/ML) erfordert häufig komplexe API-Aufrufe, die von Ihren Entwicklern und Technikern angepasst werden müssen. Dies kann ein Nachteil sein, wenn Ihre Analysten schnell einen neuen Datensatz untersuchen möchten.

Sie können die Zugänglichkeit Ihrer Dienste verbessern und eine interaktivere Form der Datenanalyse bereitstellen, indem Sie eine webbasierte Benutzeroberfläche (UI) verwenden, über die Benutzer ihre eigenen Daten hochladen und die Modellergebnisse in einem Dashboard visualisieren können.

Dieses Muster verwendet Flask und Plotly, um Amazon Comprehend in eine benutzerdefinierte Webanwendung zu integrieren und Stimmungen und Entitäten anhand von Benutzerdaten zu visualisieren. Das Muster enthält auch die Schritte zur Bereitstellung einer Anwendung mithilfe von AWS Elastic Beanstalk. Sie können die Anwendung mithilfe der KI-Services von Amazon Web Services (AWS) oder mithilfe eines speziell trainierten Modells anpassen, das auf einem Endpunkt (z. B. einem SageMaker Amazon-Endpunkt) gehostet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), auf Ihrem lokalen Computer installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Grundlagen der Konfiguration in der AWS-CLI-Dokumentation. Sie können auch eine integrierte Entwicklungsumgebung (IDE) von AWS Cloud9 verwenden. Weitere Informationen dazu finden Sie im Python-Tutorial für AWS Cloud9 und unter Vorschau laufender Anwendungen in der AWS Cloud9 Cloud9-IDE in der AWS Cloud9 Cloud9-Dokumentation.
- Ein Verständnis des Webanwendungs-Frameworks von Flask. Weitere Informationen zu Flask finden Sie im Schnellstart in der Flask-Dokumentation.
- Python Version 3.6 oder höher, installiert und konfiguriert. Sie können Python installieren, indem Sie den Anweisungen unter Einrichten Ihrer Python-Entwicklungsumgebung in der Dokumentation zu AWS Elastic Beanstalk folgen.
- Elastic Beanstalk Command Line Interface (EB CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Dokumentation zu AWS Elastic Beanstalk unter Installieren der EB-CLI und Konfigurieren der EB-CLI.

Einschränkungen

- Die Flask-Anwendung dieses Musters wurde für die Arbeit mit CSV-Dateien entwickelt, die eine einzige Textspalte verwenden und auf 200 Zeilen beschränkt sind. Der Anwendungscode kann an andere Dateitypen und Datenmengen angepasst werden.
- Die Anwendung berücksichtigt keine Datenspeicherung und aggregiert weiterhin hochgeladene Benutzerdateien, bis sie manuell gelöscht werden. Sie können die Anwendung in Amazon Simple Storage Service (Amazon S3) für persistenten Objektspeicher integrieren oder eine Datenbank wie Amazon DynamoDB für die serverlose Speicherung von Schlüsselwerten verwenden.
- Die Anwendung berücksichtigt nur Dokumente in englischer Sprache. Sie können Amazon Comprehend jedoch verwenden, um die Hauptsprache eines Dokuments zu ermitteln. Weitere Informationen zu den unterstützten Sprachen für jede Aktion finden Sie in der API-Referenz in der Amazon Comprehend Comprehend-Dokumentation.
- Eine Liste zur Fehlerbehebung, die häufig auftretende Fehler und deren Lösungen enthält, finden Sie im Abschnitt Zusätzliche Informationen.

Architektur

Die Architektur der Flask-Anwendung

Flask ist ein leichtes Framework für die Entwicklung von Webanwendungen in Python. Es wurde entwickelt, um die leistungsstarke Datenverarbeitung von Python mit einer umfangreichen Weboberfläche zu kombinieren. Die Flask-Anwendung des Musters zeigt Ihnen, wie Sie eine Webanwendung erstellen, mit der Benutzer Daten hochladen, die Daten zur Inferenz an Amazon Comprehend senden und dann die Ergebnisse visualisieren können. Die Anwendung hat die folgende Struktur:

- `static`— Enthält alle statischen Dateien, die die Weboberfläche unterstützen (z. JavaScript B. CSS und Bilder)
- `templates`— Enthält alle HTML-Seiten der Anwendung
- `userData`— Speichert hochgeladene Benutzerdaten
- `application.py`— Die Flask-Anwendungsdatei
- `comprehend_helper.py`— Funktionen zum Durchführen von API-Aufrufen an Amazon Comprehend
- `config.py`— Die Konfigurationsdatei der Anwendung
- `requirements.txt`— Die von der Anwendung benötigten Python-Abhängigkeiten

Das `application.py` Skript enthält die Kernfunktionalität der Webanwendung, die aus vier Flask-Routen besteht. Das folgende Diagramm zeigt diese Flask-Routen.

- `/`ist das Stammverzeichnis der Anwendung und leitet Benutzer auf die `upload.html` Seite weiter (die im `templates` Verzeichnis gespeichert ist).
- `/saveFile`ist eine Route, die aufgerufen wird, nachdem ein Benutzer eine Datei hochgeladen hat. Diese Route empfängt eine `POST` Anfrage über ein HTML-Formular, das die vom Benutzer hochgeladene Datei enthält. Die Datei wird im `userData` Verzeichnis gespeichert und die Route leitet Benutzer zur `/dashboard` Route weiter.
- `/dashboard`sendet Benutzer auf die `dashboard.html` Seite. Im HTML-Code dieser Seite wird der JavaScript Code ausgeführt, der `static/js/core.js` Daten aus der `/data` Route liest und dann Visualisierungen für die Seite erstellt.
- `/data`ist eine JSON-API, die die zu visualisierenden Daten im Dashboard präsentiert. Diese Route liest die vom Benutzer bereitgestellten Daten und verwendet die Funktionen, um die Benutzerdaten `comprehend_helper.py` zur Stimmungsanalyse und Named Entity Recognition (NER) an

Amazon Comprehend zu senden. Die Antwort von Amazon Comprehend wird formatiert und als JSON-Objekt zurückgegeben.

Architektur der Bereitstellung

Weitere Informationen zu Designüberlegungen für Anwendungen, die mit Elastic Beanstalk in der AWS-Cloud bereitgestellt werden, finden Sie in der Dokumentation zu AWS Elastic Beanstalk.

Überlegungen zum Entwurf

Technologie-Stack

- Amazon Comprehend
- Elastic Beanstalk
- Flask

Automatisierung und Skalierung

Elastic Beanstalk Beanstalk-Bereitstellungen werden automatisch mit Load Balancern und Auto Scaling-Gruppen eingerichtet. Weitere Konfigurationsoptionen finden Sie unter Konfiguration von Elastic Beanstalk-Umgebungen in der Dokumentation zu AWS Elastic Beanstalk.

Tools

- AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool, das eine konsistente Schnittstelle für die Interaktion mit allen Teilen von AWS bietet.
- Amazon Comprehend verwendet Natural Language Processing (NLP), um Erkenntnisse über den Inhalt von Dokumenten zu gewinnen, ohne dass eine spezielle Vorverarbeitung erforderlich ist.
- Mit AWS Elastic Beanstalk können Sie Anwendungen in der AWS-Cloud schnell bereitstellen und verwalten, ohne sich mit der Infrastruktur vertraut machen zu müssen, auf der diese Anwendungen ausgeführt werden.
- Elastic Beanstalk CLI (EB CLI) ist eine Befehlszeilenschnittstelle für AWS Elastic Beanstalk, die interaktive Befehle bereitstellt, um die Erstellung, Aktualisierung und Überwachung von Umgebungen aus einem lokalen Repository zu vereinfachen.
- Das Flask-Framework führt Datenverarbeitung und API-Aufrufe mit Python durch und bietet interaktive Webvisualisierung mit Plotly.

Code

Der Code für dieses Muster ist im GitHub Visualize AI/ML-Modellergebnisse mithilfe von Flask und AWS Elastic Beanstalk Repository verfügbar.

Epen

Richten Sie die Flask-Anwendung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Rufen Sie den Anwendung scode aus den GitHub Visualize AI/ML-Modellergebnissen mithilfe von Flask und dem AWS Elastic Beanstalk Beanstalk-Repository ab, indem Sie den folgenden Befehl ausführen: `git clone git@github.com:aws-samples/aws-comprehend-elasticbeanstalk-for-flask.git` Hinweis: Stellen Sie sicher, dass Sie Ihre SSH-Schlüssel mit konfigurieren. GitHub	Developer
Installieren Sie die Python-Module.	Nachdem Sie das Repository geklont haben, wird ein neues lokales `aws-comprehend-elasticbeanstalk-for-flask` Verzeichnis erstellt. In diesem Verzeichnis enthält die `requirements.txt` Datei die Python-Module und -Versionen, die	Python-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die Anwendung ausführen. Verwenden Sie die folgenden Befehle, um die Module zu installieren:
	
	`cd aws-comprehend-elasticbeanstalk-for-flask`
	
	`pip install -r requirements.txt`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Anwendung lokal.	Starten Sie den Flask-Server, indem Sie den folgenden Befehl ausführen:
	
	`python application.py`
	
	Dies gibt Informationen über den laufenden Server zurück. Sie sollten auf die Anwendung zugreifen können, indem Sie einen Browser öffnen und http://localhost:5000 aufrufen
	
	Hinweis: Wenn Sie die Anwendung in einer AWS Cloud9 Cloud9-IDE ausführen, müssen Sie den `application.run()` Befehl in der `application.py` Datei durch die folgende Zeile ersetzen:
	
	`application.run(host=os.getenv('IP', '0.0.0.0'),port=int(os.getenv('PORT', 8080)))`
	
	Sie müssen diese Änderung vor der Bereitstellung rückgängig machen.
		Python-Entwickler

Stellen Sie die Anwendung auf Elastic Beanstalk bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Elastic Beanstalk Beanstalk-Anwendung.	Um Ihr Projekt als Elastic Beanstalk Beanstalk-Anwendung zu starten, führen Sie den folgenden Befehl im Stammverzeichnis Ihrer Anwendung aus: `eb init -p python-3.6 comprehend_flask --region us-east-1` Wichtig • `comprehend_flask` ist der Name der Elastic Beanstalk Beanstalk-Anwendung und kann entsprechend Ihren Anforderungen geändert werden. • Sie können die AWS-Region durch eine Region Ihrer Wahl ersetzen. Die Standardregion in AWS CLI wird verwendet, wenn Sie keine Region angeben. • Die Anwendung wurde mit Python Version 3.6 erstellt. Wenn Sie andere Python-Versionen verwenden, können Fehler auftreten.	Architekt, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie den `eb init -i` Befehl aus, um weitere Konfigurationsoptionen für die Bereitstellung zu erhalten.	
Stellen Sie die Elastic Beanstalk Beanstalk-Umgebung bereit.	Führen Sie den folgenden Befehl im Stammverzeichnis der Anwendung aus: `eb create comprehend-flask-env` Hinweis: `comprehend-flask-env` ist der Name der Elastic Beanstalk Beanstalk -Umgebung und kann entsprechend Ihren Anforderungen geändert werden. Der Name darf nur Buchstaben, Zahlen und Bindestriche enthalten.	Architekt, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Autorisieren Sie Ihre Bereitstellung für die Verwendung von Amazon Comprehend.	Obwohl Ihre Anwendung möglicherweise erfolgreich bereitgestellt wurde, sollten Sie Ihrer Bereitstellung auch Zugriff auf Amazon Comprehend gewähren. `ComprehendFullAccess` ist eine von AWS verwaltete Richtlinie, die der bereitgestellten Anwendung Berechtigungen zum Durchführen von API-Aufrufen an Amazon Comprehend gewährt. Fügen Sie die `ComprehendFullAccess` Richtlinie hinzu `aws-elasticbeanstalk-ec2-role` (diese Rolle wird automatisch für die Amazon Elastic Compute Cloud (Amazon EC2) -Instances Ihrer Bereitstellung erstellt), indem Sie den folgenden Befehl ausführen: `aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/ComprehendFullAccess --role-name aws-elasticbeanstalk-ec2-role`	Entwickler, Sicherheitsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: `aws-elasticbeanstalk-ec2-role` wird erstellt, wenn Ihre Anwendung bereitgestellt wird. Sie müssen den Bereitstellungsprozess abschließen, bevor Sie die AWS Identity and Access Management (IAM) -Richtlinie anhängen können.	
Besuchen Sie Ihre bereitgestellte Anwendung.	Nachdem Ihre Anwendung erfolgreich bereitgestellt wurde, können Sie sie aufrufen, indem Sie den `eb open` Befehl ausführen. Sie können den `eb status` Befehl auch ausführen, um Details zu Ihrer Bereitstellung zu erhalten. Die Bereitstellungs-URL ist unter `CNAME` aufgeführt.	Architekt, Entwickler

(Optional) Passen Sie die Anwendung an Ihr ML-Modell an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Autorisieren Sie Elastic Beanstalk, auf das neue Modell zuzugreifen.	Stellen Sie sicher, dass Elastic Beanstalk über die erforderlichen Zugriffsberechtigungen für Ihren neuen Modellendpunkt verfügt. Wenn Sie beispielsweise einen SageMaker Amazon-Endpunkt	Entwickler, Sicherheitsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, benötigt Ihre Bereitstellung die Erlaubnis, den Endpunkt aufzurufen. Weitere Informationen dazu finden Sie InvokeEndpointin der SageMaker Amazon-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die Benutzerdaten an ein neues Modell.	Um das zugrunde liegende ML-Modell in dieser Anwendung zu ändern, müssen Sie die folgenden Dateien ändern: • `comprehend_helper.py` — Dies ist das Python-Skript, das eine Verbindung mit Amazon Comprehend herstellt, die Antwort verarbeitet und das Endergebnis an die Anwendung zurückgibt. In diesem Skript können Sie die Daten entweder an einen anderen KI-Service in der AWS-Cloud weiterleiten oder Sie können die Daten an einen benutzerdefinierten Modellendpunkt senden. Wir empfehlen, dass Sie die Ergebnisse auch in diesem Skript formatieren, um die logische Trennung und die Wiederverwendbarkeit dieses Musters zu gewährleisten. • `application.py` — Wenn Sie den Namen des `comprehend_helper.py` Skripts oder der Funktionen ändern, müssen Sie das `application.py` Anwendungsskript aktualisi	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eren, um diese Änderungen widerzuspiegeln.	
Aktualisieren Sie die Dashboard-Visualisierungen.	In der Regel bedeutet die Integration eines neuen ML-Modells, dass die Visualisierungen aktualisiert werden müssen, um die neuen Ergebnisse widerzuspiegeln. Diese Änderungen werden in den folgenden Dateien vorgenommen: • `templates/dashboard.html` — Die vorgefertigte Anwendung unterstützt nur zwei grundlegende Visualisierungen. Das gesamte Layout der Seite kann in dieser Datei angepasst werden. • `static/js/core.js` — Dieses Skript erfasst die formatierte Ausgabe der `/data` Route des Flask-Servers und verwendet Plotly, um Visualisierungen zu erstellen. Sie können die Diagramme der Seite hinzufügen oder aktualisieren.	Web-Entwickler

(Optional) Stellen Sie die aktualisierte Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Anforderungsdatei Ihrer Bewerbung.	Bevor Sie Änderunge n an Elastic Beanstalk senden, aktualisieren Sie die `requirements.txt` Datei, sodass sie alle neuen Python-Module widerspiegelt, indem Sie den folgenden Befehl im Stammverzeichnis Ihrer Anwendung ausführen: `pip freeze > requireme nts.txt`	Python-Entwickler
Stellen Sie die Elastic Beanstalk Beanstalk-Umgebung erneut bereit.	Um sicherzustellen, dass Ihre Anwendungsänderung en in Ihrem Elastic Beanstalk -Deployment widergesp iegelt werden, navigieren Sie zum Stammverzeichnis Ihrer Anwendung und führen Sie den folgenden Befehl aus: `eb deploy` Dadurch wird die neueste Version des Anwendung scodes an Ihr vorhandenes Elastic Beanstalk-Deployment gesendet.	Systemadministrator, Architekt

Zugehörige Ressourcen

- Rufen Sie mit Amazon API Gateway und AWS Lambda einen SageMaker Amazon-Modellendpunkt auf
- Bereitstellung einer Flask-Anwendung auf Elastic Beanstalk
- EB CLI-Befehlsreferenz
- Einrichtung Ihrer Python-Entwicklungsumgebung

Zusätzliche Informationen

Liste der Problemlösungen

Im Folgenden finden Sie sechs häufig auftretende Fehler und deren Lösungen.

Fehler 1

```
Unable to assume role "arn:aws:iam::xxxxxxxxxx:role/aws-elasticbeanstalk-ec2-role".
 Verify that the role exists and is configured correctly.
```

Lösung: Wenn dieser Fehler bei der Ausführung auftritt`eb create`, erstellen Sie eine Beispielanwendung auf der Elastic Beanstalk Beanstalk-Konsole, um das Standard-Instance-Profil zu erstellen. Weitere Informationen dazu finden Sie in der Dokumentation zu AWS Elastic Beanstalk unter Creating an Elastic Beanstalk Environment.

Fehler 2

```
Your WSGIPath refers to a file that does not exist.
```

Lösung: Dieser Fehler tritt in den Bereitstellungsprotokollen auf, weil Elastic Beanstalk erwartet, dass der Flask-Code benannt wird. `application.py` Wenn Sie einen anderen Namen gewählt haben, führen Sie den WSGIPath aus `eb config` und bearbeiten Sie ihn, wie im folgenden Codebeispiel gezeigt:

```
aws:elasticbeanstalk:container:python:
     NumProcesses: '1'
     NumThreads: '15'
     StaticFiles: /static/=static/
```

```
    WSGIPath: application.py
```

Stellen Sie sicher, dass Sie ihn durch Ihren Dateinamen `application.py` ersetzen.

Sie können auch Gunicorn und ein Profil nutzen. Weitere Informationen zu diesem Ansatz finden Sie unter Konfiguration des WSGI-Servers mit einem Profil in der AWS Elastic Beanstalk Beanstalk-Dokumentation.

Fehler 3

```
Target WSGI script '/opt/python/current/app/application.py' does not contain WSGI
 application 'application'.
```

Lösung: Elastic Beanstalk erwartet, dass die Variable, die Ihre Flask-Anwendung repräsentiert, benannt wird. `application` Stellen Sie sicher, dass die `application.py` Datei `application` als Variablennamen verwendet:

```
application = Flask(__name__)
```

Fehler 4

```
The EB CLI cannot find your SSH key file for keyname
```

Lösung: Verwenden Sie die EB-CLI, um anzugeben, welches key pair verwendet werden soll, oder um ein key pair für die EC2-Instances Ihrer Bereitstellung zu erstellen. Um den Fehler zu beheben, führen Sie den `eb init -i` Befehl aus und eine der Optionen wird Sie fragen:

```
Do you want to set up SSH for your instances?
```

Antworten Sie mitY, um entweder ein key pair zu erstellen oder ein vorhandenes key pair anzugeben.

Fehler 5

Ich habe meinen Code aktualisiert und erneut bereitgestellt, aber meine Bereitstellung spiegelt meine Änderungen nicht wider.

Lösung: Wenn du ein Git-Repository mit deiner Bereitstellung verwendest, stelle sicher, dass du deine Änderungen hinzufügst und festschreibst, bevor du sie erneut bereitstellst.

Fehler 6

Sie zeigen eine Vorschau der Flask-Anwendung von einer AWS Cloud9 Cloud9-IDE aus und stoßen auf Fehler.

Lösung: Weitere Informationen dazu finden Sie unter Vorschau laufender Anwendungen in der AWS Cloud9 Cloud9-IDE in der AWS Cloud9 Cloud9-Dokumentation.

Verarbeitung natürlicher Sprache mit Amazon Comprehend

Wenn Sie sich für Amazon Comprehend entscheiden, können Sie benutzerdefinierte Entitäten in einzelnen Textdokumenten erkennen, indem Sie Echtzeitanalysen oder asynchrone Batch-Jobs ausführen. Mit Amazon Comprehend können Sie auch benutzerdefinierte Modelle zur Erkennung von Entitäten und zur Textklassifizierung trainieren, die in Echtzeit verwendet werden können, indem Sie einen Endpunkt erstellen.

Dieses Muster verwendet asynchrone Batch-Jobs, um Stimmungen und Entitäten aus einer Eingabedatei zu erkennen, die mehrere Dokumente enthält. Die in diesem Muster bereitgestellte Beispielanwendung ist so konzipiert, dass Benutzer eine CSV-Datei hochladen können, die eine einzelne Spalte mit einem Textdokument pro Zeile enthält. Die `comprehend_helper.py` Datei im GitHub Visualize AI/ML-Model Results using Flask and AWS Elastic Beanstalk Repository liest die Eingabedatei und sendet die Eingabe zur Verarbeitung an Amazon Comprehend.

BatchDetectEntitäten

Amazon Comprehend untersucht den Text eines Stapels von Dokumenten auf benannte Entitäten und gibt die erkannte Entität, den Standort, den Entitätstyp und eine Bewertung zurück, die das Vertrauensniveau von Amazon Comprehend angibt. In einem API-Aufruf können maximal 25 Dokumente gesendet werden, wobei jedes Dokument kleiner als 5.000 Byte ist. Sie können die Ergebnisse filtern, sodass nur bestimmte Entitäten angezeigt werden, die auf dem Anwendungsfall basieren. Sie könnten beispielsweise den `'quantity'` Entitätstyp überspringen und einen Schwellenwert für die erkannte Entität festlegen (z. B. 0,75). Wir empfehlen Ihnen, die Ergebnisse für Ihren speziellen Anwendungsfall zu untersuchen, bevor Sie einen Schwellenwert auswählen. Weitere Informationen dazu finden Sie unter BatchDetectEntitäten in der Amazon Comprehend Comprehend-Dokumentation.

BatchDetectStimmung

Amazon Comprehend prüft einen Stapel eingehender Dokumente und gibt die vorherrschende Stimmung für jedes Dokument zurück (`POSITIVE`,`NEUTRAL`, `MIXED` oder). `NEGATIVE` In einem API-

Aufruf können maximal 25 Dokumente gesendet werden, wobei jedes Dokument kleiner als 5.000 Byte ist. Die Stimmungsanalyse ist unkompliziert, und Sie wählen die Stimmung mit der höchsten Punktzahl aus, die in den Endergebnissen angezeigt werden soll. Weitere Informationen dazu finden Sie unter BatchDetectSentiment in der Amazon Comprehend Comprehend-Dokumentation.

Handhabung der Flask-Konfiguration

Flask-Server verwenden eine Reihe von Konfigurationsvariablen, um zu steuern, wie der Server läuft. Diese Variablen können Debug-Ausgaben, Sitzungstoken oder andere Anwendungseinstellungen enthalten. Sie können auch benutzerdefinierte Variablen definieren, auf die zugegriffen werden kann, während die Anwendung ausgeführt wird. Es gibt mehrere Ansätze zum Setzen von Konfigurationsvariablen.

In diesem Muster wird die Konfiguration definiert `config.py` und darin vererbt`application.py`.

- `config.py`enthält die Konfigurationsvariablen, die beim Start der Anwendung eingerichtet werden. In dieser Anwendung ist eine `DEBUG` Variable definiert, die der Anwendung mitteilt, den Server im Debug-Modus auszuführen. Hinweis: Der Debug-Modus sollte nicht verwendet werden, wenn eine Anwendung in einer Produktionsumgebung ausgeführt wird. `UPLOAD_FOLDER`ist eine benutzerdefinierte Variable, die so definiert ist, dass sie später in der Anwendung referenziert wird und sie darüber informiert, wo hochgeladene Benutzerdaten gespeichert werden sollen.
- `application.py`initiiert die Flask-Anwendung und erbt die in definierten Konfigurationseinstellungen. `config.py` Dies wird durch den folgenden Code ausgeführt:

```
application = Flask(__name__)
application.config.from_pyfile('config.py')
```

Mehr Muster

- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Gewähren Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Migrieren von ML Build, Training und Bereitstellung von Workloads zu Amazon SageMaker mithilfe von AWS-Entwicklertools
- Führen Sie erweiterte Analysen mit Amazon Redshift ML durch

Mainframe

Themen

Sichern und Archivieren von Mainframe-Daten in Amazon S3 mithilfe von AMI-Cloud-Daten

Erstellt von Santosh Kumar Singh (AWS), Mikhael Liberman (Model9 Mainframe Software), Gilberto Biondo (AWS) und Maggie Li (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Mainframe	Ziel: Amazon S3
R-Typ: N/A	Technologien: Mainframe; Speicherung und Sicherung; Modernisierung	AWS-Services: Amazon EC2; Amazon EFS ;Amazon S3; AWS Direct Connect

Übersicht

Dieses Muster zeigt, wie Mainframe-Daten direkt in Amazon Simple Storage Service (Amazon S3) gesichert und archiviert und diese Daten dann mithilfe von AMI-Cloud-Daten (früher als Model9 Manager bezeichnet) auf dem Mainframe abgerufen und wiederhergestellt werden. Wenn Sie im Rahmen eines Mainframe-Modernisierungsprojekts nach einer Möglichkeit suchen, Ihre Backup- und Archivlösung zu modernisieren oder die Compliance-Anforderungen zu erfüllen, kann dieses Muster dazu beitragen, diese Ziele zu erreichen.

In der Regel verwenden Organisationen, die Kerngeschäftsanwendungen auf Mainframes ausführen, eine virtuelle Bandbibliothek (VTL), um Datenspeicher wie Dateien und Protokolle zu sichern. Diese Methode kann teuer sein, da sie abrechenbares MIPS verbraucht und der Zugriff auf die auf Bändern außerhalb des Mainframes gespeicherten Daten nicht möglich ist. Um diese Probleme zu vermeiden, können Sie AMI-Clouddaten verwenden, um operative und historische Mainframe-Daten schnell und kostengünstig direkt an Amazon S3 zu übertragen. Sie können AMI-AMI-Clouddaten verwenden, um Daten über TCP/IP zu sichern und zu archivieren, AWS während Sie die z Integrated Information Processor (zIIP)-Engines von IBM nutzen, um Kosten, Parallelität und Übertragungszeiten zu reduzieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AMI-Cloud-Daten mit einem gültigen Lizenzschlüssel
- TCP/IP-Konnektivität zwischen dem Mainframe und AWS
- Eine AWS Identity and Access Management (IAM)-Rolle für den Lese-/Schreibzugriff auf einen S3-Bucket
- Zugriff auf Mainframe-Sicherheitsprodukte (RACF) zur Ausführung von AMI-Cloud-Prozessen
- Ein AMI Cloud z/OS-Agent (Java Version 8 64-Bit SR5 FP16 oder höher), der über verfügbare Netzwerkports, Firewall-Regeln, die den Zugriff auf S3-Buckets zulassen, und ein dediziertes z/FS-Dateisystem verfügt
- Erfüllen der Anforderungen für den AMI-Cloud-Verwaltungsserver

Einschränkungen

- AMI Cloud Data speichert seine Betriebsdaten in einer PostgreSQL-Datenbank, die als Docker-Container auf derselben Amazon Elastic Compute Cloud (Amazon EC2)-Instance wie der Verwaltungsserver ausgeführt wird. Amazon Relational Database Service (Amazon RDS) wird derzeit nicht als Backend für AMI-Cloud-Daten unterstützt. Weitere Informationen zu den neuesten Produktaktualisierungen finden Sie unter Was ist neu? in der Bol-Dokumentation.
- Dieses Muster sichert und archiviert nur Z/OS-Mainframe-Daten. AMI Cloud Data sichert und archiviert nur Mainframe-Dateien.
- Dieses Muster konvertiert keine Daten in offene Standardformate wie JSON oder CSV. Verwenden Sie einen zusätzlichen Transformationsservice wie AMI Cloud Analytics (früher bekannt als Model9 Gravity), um die Daten in offene Standardformate zu konvertieren. Cloudnative Anwendungen und Datenanalysetools können auf die Daten zugreifen, nachdem sie in die Cloud geschrieben wurden.

Produktversionen

- AMI Cloud Data Version 2.x

Architektur

Quelltechnologie-Stack

- Mainframe mit z/OS
- Mainframe-Dateien wie Datensätze und z/OS UNIX System Services (USS)-Dateien

- Mainframe-Festplatte, z. B. ein Direct Access Storage Device (DASD)
- Mainframe-Band (virtuelle oder physische Bandbibliothek)

Zieltechnologie-Stack

- Amazon S3
- Amazon EC2-Instance in einer Virtual Private Cloud (VPC)
- AWS Direct Connect
- Amazon Elastic File System (Amazon EFS)

Zielarchitektur

Das folgende Diagramm zeigt eine Referenzarchitektur, bei der AMI-Cloud-Data-Softwareagenten auf einem Mainframe die Legacy-Datensicherungs- und Archivprozesse steuern, die die Daten in Amazon S3 speichern.

Das Diagramm zeigt den folgenden Workflow:

1. AMI-Cloud-Data-Softwareagenten werden auf logischen Mainframe-Partitionen (LPARs) ausgeführt. Die Softwareagenten lesen und schreiben Mainframe-Daten von DASD oder Band direkt über TCP/IP in Amazon S3.
2. AWS Direct Connect richtet eine physische, isolierte Verbindung zwischen dem On-Premises-Netzwerk und ein AWS. Um die Sicherheit zu erhöhen, führen Sie zusätzlich zu ein site-to-site VPN aus, AWS Direct Connect um Daten während der Übertragung zu verschlüsseln.
3. Der S3-Bucket speichert Mainframe-Dateien als Objektspeicherdaten und die Agenten von AMI Cloud Data kommunizieren direkt mit den S3-Buckets. Zertifikate werden für die HTTPS-Verschlüsselung der gesamten Kommunikation zwischen dem Agenten und Amazon S3 verwendet. Die Amazon S3-Datenverschlüsselung wird verwendet, um die Daten im Ruhezustand zu verschlüsseln und zu schützen.
4. AMI Cloud Data Management-Server werden als Docker-Container auf EC2-Instances ausgeführt. Die Instances kommunizieren mit Agenten, die auf Mainframe-LPARs und S3-Buckets ausgeführt werden.
5. Amazon EFS wird sowohl auf aktiven als auch auf passiven EC2-Instances gemountet, um den Network File System (NFS)-Speicher gemeinsam zu nutzen. Dadurch wird sichergestellt, dass

Metadaten, die sich auf eine auf dem Verwaltungsserver erstellte Richtlinie beziehen, im Falle eines Failovers nicht verloren gehen. Im Falle eines Failovers durch den aktiven Server kann ohne Datenverlust auf den passiven Server zugegriffen werden. Wenn der passive Server ausfällt, kann ohne Datenverlust auf den aktiven Server zugegriffen werden.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) stellt skalierbare Rechenkapazität in der bereit AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie beim Erstellen und Konfigurieren gemeinsam genutzter Dateisysteme in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, mit dem Sie nahezu jede Datenmenge speichern, schützen und abrufen können.
- Amazon Virtual Private Cloud (Amazon VPC) unterstützt Sie beim Starten von AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.
- AWS Direct ConnectVerbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen - AWS Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre - AWS Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.

Werkzeuge

- Der AMI Cloud Management Server ist eine GUI-Anwendung, die als Docker-Container auf einem Amazon Linux Amazon Machine Image (AMI) für Amazon EC2 ausgeführt wird. Der Verwaltungsserver bietet die Funktionalität zum Verwalten von AMI-Cloud-Aktivitäten wie Berichterstellung, Erstellung und Verwaltung von Richtlinien, Ausführen von Archiven und Durchführen von Backups, Rückrufen und Wiederherstellungen.

- Der AMI-Cloud-Agent wird auf einem On-Premises-Mainframe-LPAR ausgeführt, der Dateien mithilfe von TCP/IP direkt liest und in den Objektspeicher schreibt. Eine gestartete Aufgabe wird auf einem Mainframe-LPAR ausgeführt und ist für das Lesen und Schreiben von Sicherungs- und Archivdaten in und von Amazon S3 verantwortlich.
- AMI Cloud Mainframe Command Line Interface (M9CLI) bietet Ihnen eine Reihe von Befehlen, um AMI-Cloud-Aktionen direkt von TSO/E oder in Batchoperationen auszuführen, ohne dass der Verwaltungsserver abhängig ist.

Sekunden

Erstellen eines S3-Buckets und einer IAM-Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket zum Speichern der Dateien und Volumes, die Sie aus Ihrer Mainframe-Umgebung sichern und archivieren möchten.	Allgemeines AWS
Erstellen Sie eine IAM-Richtlinie.	Alle AMI-Cloud-Verwaltungsserver und Agenten benötigen Zugriff auf den S3-Bucket, den Sie im vorherigen Schritt erstellt haben. Um den erforderlichen Zugriff zu gewähren, erstellen Sie die folgende IAM-Richtlinie: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Listfolder", "Action": [`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"s3:ListBucket", "s3:GetBucketLocation", "s3:ListBucketVersions"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<BucketName>"] }, { "Sid": "Objectaccess", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject", "s3:DeleteObjectVersion", "s3:DeleteObject", "s3:PutObjectAcl", "s3:GetObjectVersion"], "Resource": [	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"arn:aws:s3:::<Bucket Name>/*"
	            ]
	        }
	    ]
	}</pre>	

Holen Sie sich die Lizenz für die AMI-Cloud-Software und laden Sie die Software herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich eine AMI-Cloud -Softwarelizenz.	Um einen Softwarelizenzschl üssel zu erhalten, wenden Sie sich an das BMC-AMI-Cloud-Team . Die Ausgabe des `D M=CPU` Befehls z/OS ist erforderlich, um eine Lizenz zu generieren.	Leiter erstellen
Laden Sie die AMI-Cloud-Software und den Lizenzsch lüssel herunter.	Rufen Sie die Installat ionsdateien und den Lizenzschlüssel ab, indem Sie den Anweisungen in der Bol-Dokumentation folgen.	Mainframe-Infrastrukturadmi nistrator

Installieren des AMI-Cloud-Software-Agenten auf dem Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den AMI-Cloud -Software-Agenten.	1. Bevor Sie mit der Installat ion beginnen, stellen Sie sicher, dass die Mindestan forderungen an Software	Mainframe-Infrastrukturadmi nistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Hardware für den Agenten erfüllt sind. 2. Um den Agenten zu installieren, folgen Sie den Anweisungen in der Bol-Dokumentation. 3. Nachdem der Agent mit der Ausführung auf dem Mainframe LPAR begonnen hat, suchen Sie im Spool nach der `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` Nachricht. Stellen Sie sicher, dass die Verbindung zwischen dem Agenten und dem S3-Bucket erfolgreich hergestellt wurde, indem Sie nach der `Object store connectivity has been established successfully` Nachricht im STDOUT des Agenten suchen.	

Einrichten eines AMI-Cloud-Verwaltungsservers auf einer EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Amazon EC2 Linux 2-Instances.	Starten Sie zwei Amazon EC2 Linux 2-Instances in verschiedenen Availability Zones, indem Sie den Anweisungen aus Schritt 1: Starten einer	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instance in der Amazon EC2-Dokumentation folgen. Die Instance muss die folgenden empfohlenen Hardware- und Softwarea nforderungen erfüllen: • CPU – mindestens 4 Kerne • RAM – mindestens 8 GB • Laufwerk – 40 GB • Empfohlene EC2-Instance – C5.xlarge • Betriebssystem – Linux • Software – Docker, Entzip, vi/VIM • Netzwerkbandbreite – Minimum 1 GB Weitere Informationen finden Sie in der Bol-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	Erstellen Sie ein Amazon-EFS-Dateisystem, indem Sie den Anweisungen aus Schritt 1: Erstellen Ihres Amazon-EFS-Dateisystems in der Amazon-EFS-Dokumentation folgen. Gehen Sie beim Erstellen des Dateisystems wie folgt vor: • Wählen Sie die Speicherklasse Standard aus. • Wählen Sie dieselbe VPC aus, die Sie zum Starten Ihrer EC2-Instances verwendet haben.	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Docker und konfigurieren Sie den Verwaltungsserver.	Stellen Sie eine Verbindung zu Ihren EC2-Instances her:
	
	Stellen Sie eine Verbindung zu Ihren EC2-Instances her, indem Sie den Anweisungen unter Verbinden mit Ihrer Linux-Instance in der Amazon EC2-Dokumentation folgen.
	
	Konfigurieren Sie Ihre EC2-Instances:
	
	Gehen Sie für jede EC2-Instance wie folgt vor:
	
	1. Um Docker zu installieren, führen Sie den Befehl aus:
	
	`sudo yum install docker`
	
	2. Um Docker zu starten, führen Sie den Befehl aus:
	
	`sudo service docker start`
	
	3. Führen Sie den Befehl aus, um den Status von Docker zu überprüfen:
	
	`sudo service docker status`
	
	4. Ändern Sie im `/etc/selinux` Ordner die `config`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Datei in `SELINUX=permissive` .
	5. Laden Sie die `VerificationScripts.zip` Dateien `model9-v2.x.y_build_build-id-server.zip` und (die Sie zuvor heruntergeladen haben) in einen temporären Ordner in einer der EC2-Instances hoch (z. B. in den `/var/tmp` Ordner in Ihrer Instance).
	6. Führen Sie den Befehl aus, um zum `tmp` Ordner zu gelangen:
	`cd/var/tmp`
	7. Um das Verifizierungsskript zu entpacken, führen Sie den Befehl aus:
	`unzip VerificationScripts.zip`
	8. Um das Verzeichnis zu ändern, führen Sie den Befehl aus:
	`cd /var/tmp/sysutils/PrereqsScripts`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Um das Verifizierungsskript auszuführen, führen Sie den Befehl aus: `./M9VerifyPrereqs.sh` 10. Nachdem das Verifizierungsskript zur Eingabe aufgefordert wurde, geben Sie die Amazon S3-URL und die Portnummer ein. Geben Sie dann die z/OS-IP/DNS und die Portnummer ein. Hinweis: Das Skript führt eine Überprüfung durch, um zu bestätigen, dass die EC2-Instance eine Verbindung mit dem S3-Bucket und dem Agenten herstellen kann, die auf dem Mainframe ausgeführt werden. Wenn eine Verbindung hergestellt wird, wird eine Erfolgsmeldung angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Managementserver-Software.	1. Erstellen Sie einen Ordner und Unterordner im Stammverzeichnis (z. B. `/data/model9`) in der EC2-Instance, die Sie zum aktiven Server machen möchten.
	2. Führen Sie die `amazon-efs-utils` folgenden Befehle aus, um das Paket zu installieren und das zuvor erstellte Amazon-EFS-Dateisystem zu mounten:
	`sudo yum install -y amazon-efs-utils`
	`sudo mount -t efs -o tls <File System ID>:/ /data/model9`
	3. Um die Datei der EC2-`/etc/fstab` Instance mit einem Eintrag für das Amazon EFS-Dateisystem zu aktualisieren (sodass Amazon EFS beim Neustart von Amazon EC2 automatisch wieder gemountet wird), führen Sie den Befehl aus:
	`<Amazon-EFS-file-system-id>:/ /data/model9 efs defaults,_netdev 0 0`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Führen Sie die folgenden Befehle aus, um Variablen zu exportieren, um den Pfad zu den AMI-Cloud-Installationsdateien und den Zielinstallationsspeicherort zu definieren:
	`export MODEL9_HOME=/data/model9`
	`export M9INSTALL=/var/tmp`
	Hinweis: Wir empfehlen Ihnen, diese EXPORT-Befehle zu Ihrem `.bashrc`Skript hinzuzufügen.
	5. Um das Verzeichnis zu ändern, führen Sie den`cd $MODEL9_HOME` Befehl aus und erstellen Sie dann ein weiteres Unterverzeichnis, indem Sie den `mkdir diag` Befehl ausführen.
	6. Um die Installationsdatei zu entpacken, führen Sie den Befehl aus:
	`unzip $M9INSTALL/model9-<v2.x.y>_build_<build-id>-server.zip`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Hinweis: Ersetzen Sie `x.y` (die Version) und `build-id` durch Ihre Werte.
	7. Um die Anwendung bereitzustellen, führen Sie die folgenden Befehle aus:
	`docker load -i $MODEL9_HOME/model9-<v2.x.y>_build_<build-id>.docker`
	`docker load -i $MODEL9_HOME/postgres-12.10-x86.docker.gz`
	Hinweis: Ersetzen Sie `v2.x.y` (die Version) und `build-id` durch Ihre Werte.
	8. Aktualisieren Sie im`$MODEL9_HOME/conf` Ordner die`model9-local.yml` Datei .
	Hinweis: Einige der Parameter haben Standardwerte und andere können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie in den Anweisungen in der -`model9-local.yml` Datei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	9. Erstellen Sie eine Datei mit dem Namen `$MODEL9_HOME/conf` und fügen Sie der Datei dann die folgenden Parameter hinzu:
	`TZ=America/New_York`
	`EXTRA_JVM_ARGS=-Xmx2048m`
	10. Führen Sie den Befehl aus, um eine Docker-Netzwerk-Bridge zu erstellen:
	`docker network create -d bridge model9network`
	11. Führen Sie den folgenden Befehl aus, um den PostgreSQL-Datenbankcontainer für AMI Cloud zu starten:
	`docker run -p 127.0.0.1:5432:5432 \`
	`-v $MODEL9_HOME/db/data:/var/lib/postgresql/data:z \`
	`--name model9db --restart unless-stopped \`
	`--network model9network \`
	`-e POSTGRES_PASSWORD=model9 -e POSTGRES_`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DB=model9 -d postgres:12.10` 12. Nachdem der PostgreSQL-Container gestartet wurde, führen Sie den folgenden Befehl aus, um den Anwendungsserver zu starten: `docker run -d -p 0.0.0.0:443:443 -p 0.0.0.0:80:80 \ --sysctl net.ipv4.tcp_keepalive_time=600 \ --sysctl net.ipv4.tcp_keepalive_intvl=30 \ --sysctl net.ipv4.tcp_keepalive_probes=10 \ -v $MODEL9_HOME:/model9:z -h $(hostname) --restart unless-stopped \ --env-file $MODEL9_HOME/conf/model9.env \ --network model9network \ --name model9-v2.x.y model9:<v2.x.y>.<build-id>`  Hinweis: Ersetzen Sie `v2.x.y` (die Version) und `build-id` durch Ihre Werte.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	13. Führen Sie den Befehl aus, um den Zustand beider Container zu überprüfen: `docker ps -a` 14. Wiederholen Sie die Schritte 1–4, 7 und 10–13, um einen Verwaltungsserver auf den passiven EC2-Instances zu installieren. Hinweis: Um Probleme zu beheben, gehen Sie zu den im `/data/model9/logs/` Ordner gespeicherten Protokollen. Weitere Informationen finden Sie in der Bol-Dokumentation.	

Hinzufügen eines Agenten und Definieren einer Backup- oder Archivrichtlinie auf dem AMI-Cloud-Verwaltungsserver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen neuen Agenten hinzu.	Bevor Sie einen neuen Agenten hinzufügen, bestätigen Sie Folgendes: • Ein AMI-Cloud-Agent wird auf dem Mainframe LPAR ausgeführt und wurde vollständig initialisiert. Identifizieren Sie den	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Agenten, indem Sie im Spool nach der `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` Initialisierungsnachricht suchen. • Ein Docker-Container für den Verwaltungsserver ist vollständig initialisiert und wird ausgeführt. Sie müssen einen Agenten auf dem Verwaltungsserver erstellen, bevor Sie Backup- und Archivrichtlinien definieren. Gehen Sie wie folgt vor, um den Agenten zu erstellen: 1. Verwenden Sie einen Webbrowser, um auf den Verwaltungsserver zuzugreifen, der auf Ihrem Amazon EC2-Computer bereitgestellt wird, und melden Sie sich dann mit Ihren Mainframe-Anmeldeinformationen an. 2. Wählen Sie die Registerkarte AGENTS und dann NEUEN AGENT HINZUFÜGEN aus. 3. Geben Sie für Name den Agentennamen ein. 4. Geben Sie für Hostname/IP-Adresse den Hostnamen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder die IP-Adresse Ihres Mainframes ein. 5. Geben Sie für Port Ihre Portnummer ein. 6. Wählen Sie TEST CONNECTION aus. Sie können eine Erfolgsme ldung sehen, wenn die Verbindung erfolgreich hergestellt wurde. 7. Wählen Sie CREATE (Erstellen) aus. Nachdem der Agent erstellt wurde, sehen Sie den Verbindungsstatus für den Objektspeicher und den Mainframe-Agenten in einem neuen Fenster, das in der Tabelle angezeigt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Backup- oder Archivrichtlinie.	1. Wählen Sie POLICIES aus. 2. Wählen Sie POLICY ERSTELLEN aus. 3. Geben Sie auf der Seite CREATE A NEW POLICY Ihre Richtlinienspezifikationen ein. Hinweis: Weitere Informationen zu den verfügbaren Spezifikationen finden Sie unter Erstellen einer neuen Richtlinie in der Bol-Dokumentation. 4. Wählen Sie Finish (Abschließen). 5. Die neue Richtlinie ist jetzt als Tabelle aufgeführt. Um diese Tabelle anzuzeigen, wählen Sie die RegisterkartePOLICIES.	Mainframe-Speicheradministrator oder Entwickler

Ausführen der Backup- oder Archivrichtlinie vom Verwaltungsserver aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Backup- oder Archivrichtlinie aus.	Führen Sie die Datensicherungs- oder Archivrichtlinie aus, die Sie zuvor vom Verwaltungsserver aus erstellt haben, entweder manuell oder automatisch (basierend auf	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einem Zeitplan). So führen Sie die Richtlinie manuell aus: 1. Wählen Sie im Navigatio nsmenü die Registerk artePOLICIES aus. 2. Wählen Sie auf der rechten Seite der Tabelle für die Richtlinie, die Sie ausführen möchten, das Dreipunkt menü aus. 3. Wählen Sie Jetzt ausführen aus. 4. Wählen Sie im Popup-Bes tätigungsfensterYES, RUN POLICY NOW aus. 5. Nachdem die Richtlini e ausgeführt wurde, überprüfen Sie den Ausführungsstatus im Abschnitt Richtlinienaktivit ät. 6. Wählen Sie für die ausgeführte Richtlinie das Dreipunktmenü und dann Ausführungsprotoko ll anzeigen aus, um die Protokolle anzuzeigen. 7. Um zu überprüfen, ob das Backup erstellt wurde, überprüfen Sie den S3-Bucket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Backup- oder Archivrichtlinie wieder her.	1. Wählen Sie im Navigationsmenü die RegisterkartePOLICIES aus. 2. Wählen Sie die Richtlinie aus, für die Sie Ihren Wiederherstellungsprozess ausführen möchten. Dadurch werden alle Backup- oder Archivaktivitäten aufgeführt, die in der Vergangenheit für diese spezifische Richtlinie ausgeführt wurden. 3. Um die Backups auszuwählen, die Sie wiederherstellen möchten, wählen Sie die SpalteDate-time aus. Der`file/Volume/Storage` Gruppenname zeigt die Ausführungsdetails der Richtlinie an. 4. Wählen Sie auf der rechten Seite der Tabelle das Dreipunktmenü und dannRESTORE aus. 5. Geben Sie im Popup-Fenster Ihren Zielnamen, Ihr Volume und Ihre Speichergruppe ein und wählen Sie dann RESTORE aus. 6. Geben Sie Ihre Mainframe-Anmeldeinformationen ein	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und wählen Sie dann erneut RESTORE aus. 7. Um zu überprüfen, ob die Wiederherstellung erfolgreich war, überprüfen Sie die Protokolle oder den Mainframe.	

Ausführen der Backup- oder Archivrichtlinie vom Mainframe aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Backup- oder Archivrichtlinie mit M9CLI aus.	Verwenden Sie die M9CLI, um Sicherungs- und Wiederherstellungsprozesse von TSO/E, REXX oder über JCLs durchzuführen, ohne Regeln auf dem AMI-Cloud-Verwaltungsserver einzurichten. Verwenden von TSO/E: Wenn Sie TSO/E verwenden, stellen Sie sicher, dass mit verkettet `M9CLI REXX` ist`TSO`. Verwenden Sie den `TSO M9CLI BACKDSN <DSNAME>` Befehl , um einen Datensatz über TSO/E zu sichern. Hinweis: Weitere Informationen zu M9CLI-Befehlen finden Sie in der CLI-Referenz in der Bol-Dokumentation.	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Verwenden von JCLs:
	
	Um die Backup- und Archivric htlinie mithilfe von JCLs auszuführen, führen Sie den `M9CLI` Befehl aus.
	
	Verwenden von Batchoper ationen:
	
	Das folgende Beispiel zeigt, wie Sie einen Datensatz archivieren, indem Sie den `M9CLI` Befehl im Stapel ausführen:
	
	`//JOBNAME JOB …`
	`//M9CLI EXEC PGM=IKJEF T01`
	`//STEPLIB DD DISP=SHR, DSN=<MODEL9 LOADLIB>`
	`//SYSEXEC DD DISP=SHR, DSN=<MODEL9 EXEC LIB>`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSIN DD TSO M9CLI`
	` ARCHIVE`
	` M9CLI ARCHIVE <DSNNAME`
	` OR DSN PATTERN>`
	`/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Backup- oder Archivrichtlinie im JCL-Batch aus.	AMI Cloud bietet eine Beispiel-JCL-Routine namensM9SAPIJ. Sie können M9SAPIJ anpassen, um eine bestimmte Richtlinie auszuführen, die auf dem Verwaltungsserver mit einer JCL erstellt wurde. Dieser Auftrag kann auch Teil eines Batch-Schedulers für die automatische Ausführung von Backup- und Wiederherstellungsprozessen sein. Der Batch-Auftrag erwartet die folgenden obligatorischen Werte: • IP-Adresse/Hostname des Verwaltungsservers • Port-Nummer • Richtlinien-ID oder Richtlinienname (wird auf dem Verwaltungsserver erstellt) Hinweis: Sie können auch andere Werte ändern, indem Sie den Anweisungen zum Beispielauftrag folgen.	Mainframe-Speicheradministrator oder Entwickler

Zugehörige Ressourcen

- Mainframe Modernization with AWS (AWS-Dokumentation)

- So senkt Cloud Backup for Mainframes die Kosten mit Model9 und AWS (AWS Partner Network Blog)
- So aktivieren Sie Mainframe Data Analytics in AWS mit Model9 (AWS-Partnernetzwerk-Blog)
- AWS Direct Connect Resiliency Recommendations (AWS-Dokumentation)
- AMI-Cloud-Dokumentation (BMC-Website)

Erstellen eines erweiterten Mainframe-Datei-Viewers in der AWS Cloud

Erstellt von Bo microSD GOPALSAMY (AWS) und Jer Bolh O'Connor (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Mainframe; Migration; Serverless	Workload: IBM
AWS-Services: Amazon Athena ;AWS Lambda; Amazon OpenSearch Service; AWS Step Functions		

Übersicht

Dieses Muster enthält Codebeispiele und Schritte, mit denen Sie ein erweitertes Tool zum Durchsuchen und Überprüfen Ihrer Mainframe-Dateien im festen Format mithilfe von AWS Serverless-Services entwickeln können. Das Muster bietet ein Beispiel dafür, wie Sie eine Mainframe-Eingabedatei zum Durchsuchen und Durchsuchen in ein Amazon- OpenSearch Service-Dokument konvertieren. Das Dateianzeige-Tool kann Ihnen dabei helfen, Folgendes zu erreichen:

- Behalten Sie dieselbe Mainframe-Dateistruktur und dasselbe Layout für Konsistenz in Ihrer AWS-Zielmigrationsumgebung bei (Sie können beispielsweise dasselbe Layout für Dateien in einer Batch-Anwendung beibehalten, die Dateien an externe Parteien überträgt).
- Beschleunigen Sie die Entwicklung und das Testen während Ihrer Mainframe-Migration
- Unterstützung von Wartungsaktivitäten nach der Migration

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Virtual Private Cloud (VPC) mit einem Subnetz, das von Ihrer Legacy-Plattform erreichbar ist
- Eine Eingabedatei und die entsprechende COBOL-Kopie (Common Business-oriented Language) (Hinweis : Beispiele für Eingabedateien und COBOL-Kopien finden Sie unter gfs-mainframe-

solutions im GitHub Repository. Weitere Informationen zu COBOL-Kopierbooks finden Sie im Programmierhandbuch zu Enterprise COBOL für z/OS 6.3 auf der IBM-Website.)

Einschränkungen

- Das Copybook-Parsing ist auf maximal zwei verschachtelte Ebenen (OCCURS) beschränkt.

Architektur

Quelltechnologie-Stack

- Eingabedateien im FB-Format (Fixed Blocked)
- Layout des COBOL-Kopiers

Zieltechnologie-Stack

- Amazon Athena
- Amazon OpenSearch Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm zeigt den Prozess des Parsens und Konvertierens einer Mainframe-Eingabedatei in ein - OpenSearch Servicedokument zum Durchsuchen und Durchsuchen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Administratorbenutzer oder eine Anwendung überträgt Eingabedateien an einen S3-Bucket und COBOL-Kopierbücher an einen anderen S3-Bucket.
2. Der S3-Bucket mit den Eingabedateien ruft eine Lambda-Funktion auf, die einen Serverless Step Functions-Workflow startet. Hinweis: Die Verwendung eines S3-Ereignisauslösers und einer Lambda-Funktion, um den Step-Functions-Workflow in diesem Muster voranzutreiben, ist optional.

Die GitHub Codebeispiele in diesem Muster beinhalten nicht die Nutzung dieser Services, aber Sie können diese Services auf der Grundlage Ihrer Anforderungen verwenden.

3. Der Step-Functions-Workflow koordiniert alle Batch-Prozesse aus den folgenden Lambda-Funktionen:
   - Die `s3copybookparser.py` Funktion analysiert das Copybook-Layout und extrahiert Feldattribute, Datentypen und Offsets (erforderlich für die Verarbeitung von Eingabedaten).
   - Die `s3toathena.py` Funktion erstellt ein Athena-Tabellenlayout. Athena analysiert die Eingabedaten, die von der `s3toathena.py` Funktion verarbeitet werden, und konvertiert die Daten in eine CSV-Datei.
   - Die `s3toelasticsearch.py` Funktion nimmt die Ergebnisdatei aus dem S3-Bucket auf und überträgt die Datei an den OpenSearch Service.
4. Benutzer greifen auf OpenSearch Dashboards with OpenSearch Service zu, um die Daten in verschiedenen Tabellen- und Spaltenformaten abzurufen und dann Abfragen für die indizierten Daten auszuführen.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen. In diesem Muster verwenden Sie Lambda, um Kernlogik zu implementieren, z. B. das Analysieren von Dateien, das Konvertieren von Daten und das Laden von Daten in den OpenSearch Service für den interaktiven Dateizugriff.
- Amazon OpenSearch Service ist ein verwalteter Service, mit dem Sie OpenSearch Service-Cluster in der AWS Cloud bereitstellen, betreiben und skalieren können. In diesem Muster verwenden Sie OpenSearch Service, um die konvertierten Dateien zu indizieren und interaktive Suchfunktionen für Benutzer bereitzustellen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. In diesem Muster verwenden Sie Step Functions, um Lambda-Funktionen zu orchestrieren.

Andere Tools

- GitHub ist ein Code-Hosting-Service, der Tools für die Zusammenarbeit und Versionskontrolle bereitstellt.
- Python ist eine allgemeine Programmiersprache.

Code

Der Code für dieses Muster ist im GitHub gfs-mainframe-patternsRepository verfügbar.

Polen

Vorbereiten der Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Erstellen Sie einen S3-Bucket zum Speichern der Copybooks, Eingabeda teien und Ausgabedateien. Wir empfehlen die folgende Ordnerstruktur für Ihren S3-Bucket: • `copybook/` • `input/` • `output/` • `query/` • `results/`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Funktion s3copybookparser.	1. Erstellen Sie eine Lambda-Funktion mit dem Namen `s3copybookparser` und laden Sie den Quellcode (`s3copybookparser.py` und `copybook.py`) aus dem GitHubRepository hoch. 2. Fügen Sie die IAM-Richtlinie an die Lambda-Funktion `S3ReadOnly` an.	Allgemeines AWS
Erstellen Sie die Funktion s3toathena.	1. Erstellen Sie eine Lambda-Funktion mit dem Namen `s3toathena` und laden Sie den Quellcode (`s3toathena.py`) aus dem GitHubRepository hoch. Konfigurieren Sie das Lambda-Timeout auf > 60 Sekunden. 2. Um Zugriff auf die erforderlichen Ressourcen zu gewähren, fügen Sie die IAM-Richtlinien `AmazonAthenaFullAccess` und an die Lambda-Funktion `S3FullAccess` an.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Funktion s3toelasticsearch.	1. Fügen Sie Ihrer Lambda-Umgebung eine Python-Abhängigkeit hinzu. Wichtig: Um die `s3toelasticsearch` Funktion zu verwenden, müssen Sie die Python-Abhängigkeit hinzufügen, da die Lambda-Funktion Python-Elasticsearch-Clientabhängigkeiten (`Elasticsearch==7.9.0` und `requests_aws4auth`) verwendet. 2. Erstellen Sie eine Lambda-Funktion mit dem Namen `s3toelasticsearch` und laden Sie den Quellcode (`s3toelasticsearch.py`) aus dem GitHubRepository hoch. 3. Importieren Sie die Python-Abhängigkeit als Lambda-Ebene. 4. Fügen Sie die IAM-Richtlinien `S3ReadOnly` und an die Lambda-Funktion `AmazonOpenSearchServiceReadOnlyAccess` an.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den OpenSearch Service-Cluster.	Erstellen des Clusters 1. Erstellen Sie einen - OpenSearch Service-Cluster. Gehen Sie beim Erstellen des Clusters wie folgt vor: • Erstellen Sie einen Hauptbenutzer und ein Passwort für den Cluster, mit dem Sie sich bei OpenSearch Dashboards anmelden können. Hinweis: Dieser Schritt ist nicht erforderlich, wenn Sie die Authentifizierung über Amazon Cognito verwenden. • Wählen Sie eine differenzierte Zugriffskontrolle aus. Auf diese Weise haben Sie zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten im OpenSearch Service zu steuern. 2. Kopieren Sie die Domain-URL und übergeben Sie sie als Umgebungsvariable „HOST“ an die Lambda-Funktion `s3toelasticsearch` . Gewähren des Zugriffs auf die IAM-Rolle	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Gehen Sie wie folgt vor, um einen differenzierten Zugriff auf die IAM-Rolle (`arn:aws:iam::**:role/service-role/s3toelasticsearch-role-**`) der Lambda-Funktion zu ermöglichen: 1. Melden Sie sich als Hauptbenutzer bei OpenSearch Dashboards an. 2. Wählen Sie die Registerkarte Sicherheit und dann Rollen , all_access , Benutzer zuordnen, Backend-Rollen . 3. Fügen Sie den Amazon-Ressourcennamen (ARN) der IAM-Rolle der Lambda-Funktion hinzu und wählen Sie dann Speichern aus. Weitere Informationen finden Sie unter Zuordnen von Rollen zu Benutzern in der OpenSearch Service-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Step Functions für die Orchestrierung.	1. Erstellen Sie einen Step-Functions-Zustandsautomaten mit dem Standard-Flow. Die Definition ist im GitHub Repository enthalten. 2. Ersetzen Sie im JSON-Skript die ARNs der Lambda-Funktion durch die ARNs aus der Lambda-Funktion in Ihrer Umgebung.	Allgemeines AWS

Bereitstellen und Ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Eingabedateien und Kopierbücher in den S3-Bucket hoch.	Laden Sie Beispieldateien aus dem GitHub Repository-Beispielordner herunter und laden Sie die Dateien in den S3-Bucket hoch, den Sie zuvor erstellt haben. 1. Laden Sie `Mockedcopy.cpy` und `acctix.cpy` in den `<S3_Bucket>/copybook` Ordner hoch. 2. Laden Sie die `acctindex.cpy` Beispieleingabedateien `Modedupdate.txt` und in den `<S3_Bucket>/input` Ordner hoch.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie die Step Functions auf.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Step Functions-Konsole .
	2. Wählen Sie im Navigationsbereich Zustandsautomaten aus.
	3. Wählen Sie Ihren Zustandsautomaten und dann Ausführung starten aus.
	4. Geben Sie im Feld Eingabe den folgenden Kopierbuch-/Dateipfad als JSON-Variable für den S3-Bucket ein und wählen Sie dann Ausführung starten aus.
	
	`{ "s3_copybook_bucket_name": "<BUCKET NAME>", "s3_copybook_bucket_key": "<COPYBOOK PATH>", "s3_source_bucket_name": "<BUCKET NAME", "s3_source_bucket_key": "INPUT FILE PATH" }`
	
	Beispielsweise:
	
	`{`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"s3_copybook_bucket_name": "fileaidtest", "s3_copybook_bucket_key": "copybook/acctix.cpy", "s3_source_bucket_name": "fileaidtest", "s3_source_bucket_key": "input/acctindex" }	
Validieren Sie die Workflow-Ausführung in Step Functions.	Überprüfen Sie in der Step Functions-Konsole die Workflow-Ausführung im Graph Inspector . Die Ausführungsstatus sind farbenkodiert, um den Ausführungsstatus darzustellen. Zum Beispiel steht Blau für In Bearbeitung, Grün für Erfolgreich und Rot für Fehlgeschlagen. Sie können die Tabelle auch im Abschnitt Ausführungsereignisverlauf überprüfen, um detailliertere Informationen zu den Ausführungsereignissen zu erhalten. Ein Beispiel für eine grafische Workflow-Ausführung finden Sie unter Step Functions -Diagramm im Abschnitt Zusätzliche Informationen dieses Musters.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellungsprotokolle in Amazon CloudWatch.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Erweitern Sie im Navigationsbereich Protokolle und wählen Sie dann Protokollgruppen aus. 3. Suchen Sie im Suchfeld nach der Protokollgruppe der `s3toelasticsearch` Funktion. Ein Beispiel für erfolgreiche Zustellungsprotokolle finden Sie unter CloudWatch Zustellungsprotokolle im Abschnitt Zusätzliche Informationen dieses Musters.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die formatierte Datei in OpenSearch Dashboards und führen Sie Dateioperationen durch.	1. Melden Sie sich bei der AWS-Managementkonsole an. Wählen Sie unter Analyse die Option Amazon OpenSearch Service aus. 2. Wählen Sie im Navigationsbereich Domains aus. 3. Geben Sie im Suchfeld die URL für Ihre Domain in OpenSearch Dashboards ein. 4. Wählen Sie Ihr Dashboard aus und melden Sie sich dann als Hauptbenutzer an. 5. Durchsuchen Sie die indizierten Daten im Tabellenformat. 6. Vergleichen Sie die Eingabedatei mit der formatierten Ausgabedatei (indiziertes Dokument) in OpenSearch Dashboards. In der Dashboard-Ansicht werden die hinzugefügten Spaltenüberschriften für Ihre formatierten Dateien angezeigt. Vergewissern Sie sich, dass die Quelldaten aus Ihren unformatierten Eingabedateien mit den Zieldaten in der Dashboard-Ansicht übereinstimmen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Führen Sie Aktionen wie Suchen (z. B. mithilfe von Feldnamen, Werten oder Ausdrücken), Filter- und DQL-Operationen (Dashboard Query Language) für die indizierte Datei aus.	

Zugehörige Ressourcen

Referenzen

- Beispiel für ein COBOL-Kopierbook (IBM-Dokumentation)
- Bol File-AID (BMC-Dokumentation)

Tutorials

- Tutorial: Verwenden eines Amazon S3-Auslösers zum Aufrufen einer Lambda-Funktion (AWS Lambda-Dokumentation)
- Wie erstelle ich einen Serverless-Workflow mit AWS Step Functions und AWS Lambda (AWS-Dokumentation)
- Verwenden von OpenSearch Dashboards mit Amazon OpenSearch Service (AWS-Dokumentation)

Zusätzliche Informationen

Step-Functions-Diagramm

Das folgende Beispiel zeigt ein Step-Functions-Diagramm. Das Diagramm zeigt den Ausführungsstatus für die in diesem Muster verwendeten Lambda-Funktionen.

CloudWatch -Bereitstellungsprotokolle

Das folgende Beispiel zeigt erfolgreiche Zustellungsprotokolle für die Ausführung der `s3toelasticsearch` Ausführung.

2022-08-10T15:53:33.033-05:00	Anzahl der Verarbeitungsdokumente: 100	
	2022-08-10T15:53:33.171-05:00	[INFO] 2022-08-10T20:53:33.171Z a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 POST https://search-essearch-3h4uqclifeqaj2vg4mphe7ffle.us-east-2.es.amazonaws.com:443/_bulk [Status:200 request:0.100s]
	2022-08-10T15:53:33.172-05:00	Massenschreibvorgang erfolgreich: 100 Dokumente

Containerisieren Sie Mainframe-Workloads, die von Clari Age modernisiert wurden

Erstellt von Richard Milner-Watts (AWS)

Code-Repository: Beispiel für einen Blue Age Application Container	Umgebung: Produktion	Quelle: Mainframe-Workloads
Ziel: Container	R-Typ: Neuarchitektur	Workload: IBM; Alle anderen Workloads
Technologien: Mainframe; Container und Microservices; Migration; Modernisierung	AWS-Services: Amazon ECS; Amazon ECR	

Übersicht

Dieses Muster bietet ein Beispiel für eine Containerumgebung für die Ausführung von Mainframe-Workloads, die mit dem Clari Age-Tool modernisiert wurden. Blue Age konvertiert ältere Mainframe-Workloads in modernen Java-Code. Dieses Muster bietet einen Wrapper um die Java-Anwendung, sodass Sie sie mithilfe von Container-Orchestrierungsservices wie Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) ausführen können.

Weitere Informationen zur Modernisierung Ihrer Workloads mithilfe der Services Clari Age und AWS finden Sie in diesen Veröffentlichungen zu AWS Prescriptive Guidance:

- Ausführen modernisierter Mainframe-Workloads von Clari Age auf der Serverless-AWS-Infrastruktur
- Bereitstellen einer Umgebung für containerisierte Clari Age-Anwendungen mithilfe von Terraform

Wenn Sie Hilfe bei der Verwendung von Clari Age zur Modernisierung Ihrer Mainframe-Workloads benötigen, wenden Sie sich an das Clari Age-Team, indem Sie auf der Clari Age-Website die Option Kontaktieren Sie unsere Experten auswählen. https://www.bluage.com/ Um Unterstützung bei der Migration Ihrer modernisierten Workloads zu AWS, deren Integration in AWS-Services und deren

Umstellung in die Produktion zu erhalten, wenden Sie sich an Ihren AWS-Kundenbetreuer oder füllen Sie das AWS Professional Services-Formular aus.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine modernisierte Java-Anwendung, die von Clari Age erstellt wurde. Zu Testzwecken bietet dieses Muster eine Java-Beispielanwendung, die Sie als Machbarkeitsnachweis verwenden können.
- Eine Docker-Umgebung, mit der Sie den Container erstellen können.

Einschränkungen

Abhängig von der verwendeten Container-Orchestrierungsplattform können die Ressourcen, die dem Container zur Verfügung gestellt werden können (z. B. CPU, RAM und Speicher), eingeschränkt sein. Wenn Sie beispielsweise Amazon ECS mit AWS Fargate verwenden, finden Sie in der Amazon ECS-Dokumentation weitere Informationen zu Einschränkungen und Überlegungen.

Architektur

Quelltechnologie-Stack

- Blaues Alter
- Java

Zieltechnologie-Stack

- Docker

Zielarchitektur

Das folgende Diagramm zeigt die Architektur der Clari Age-Anwendung innerhalb eines Docker-Containers.

1. Der Einstiegspunkt für den Container ist das Wrapper-Skript. Dieses Bash-Skript ist für die Vorbereitung der Laufzeitumgebung für die Clari Age-Anwendung und die Verarbeitung von Ausgaben verantwortlich.
2. Umgebungsvariablen innerhalb des Containers werden verwendet, um Variablen im Wrapper-Skript zu konfigurieren, z. B. die Amazon Simple Storage Service (Amazon S3)-Bucket-Namen und Datenbankanmeldeinformationen. Umgebungsvariablen werden entweder von AWS Secrets Manager oder Parameter Store bereitgestellt, einer Funktion von AWS Systems Manager . Wenn Sie Amazon ECS als Container-Orchestrierungsservice verwenden, können Sie auch die Umgebungsvariablen in der Amazon-ECS-Aufgabendefinition fest codieren.
3. Das Wrapper-Skript ist dafür verantwortlich, alle Eingabedateien aus dem S3-Bucket in den Container zu ziehen, bevor Sie die Clari Age-Anwendung ausführen. Die AWS Command Line Interface (AWS CLI) ist im Container installiert. Dies bietet einen Mechanismus für den Zugriff auf Objekte, die in Amazon S3 über den Virtual Private Cloud (VPC)-Gateway-Endpunkt gespeichert sind.
4. Die Java Archive (JAR)-Datei für die Clari Age-Anwendung muss möglicherweise mit anderen Datenquellen wie Amazon Aurora kommunizieren.
5. Nach Abschluss liefert das Wrapper-Skript die resultierenden Ausgabedateien zur weiteren Verarbeitung an einen S3-Bucket (z. B. durch Amazon- CloudWatch Protokollierungsservices). Das Muster unterstützt auch die Bereitstellung von ZIP-Protokolldateien an Amazon S3, wenn Sie eine Alternative zur CloudWatch Standardprotokollierung verwenden.

Tools

AWS-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.

Tools

- Docker ist eine Softwareplattform zum Erstellen, Testen und Bereitstellen von Anwendungen. Docker verpackt Software in standardisierte Einheiten, die als Container bezeichnet werden und alles enthalten, was die Software zum Ausführen benötigt, einschließlich Bibliotheken,

Systemtools, Code und Laufzeit. Sie können Docker verwenden, um Anwendungen in jeder Umgebung bereitzustellen und zu skalieren.

- Bash ist eine Befehlssprachenschnittstelle (Shell) für das GNU-Betriebssystem.
- Java ist die Programmiersprache und die Entwicklungsumgebung, die in diesem Muster verwendet werden.
- Blue Age ist ein AWS Mainframe-Modernisierungstool, das ältere Mainframe-Workloads, einschließlich Anwendungscode, Abhängigkeiten und Infrastruktur, in moderne Workloads für die Cloud umwandelt.

Code-Repository

Der Code für dieses Muster ist im GitHub Blue Age-Beispielcontainer-Repository verfügbar.

Bewährte Methoden

- Externalisieren Sie die Variablen zur Änderung des Verhaltens Ihrer Anwendung mithilfe von Umgebungsvariablen. Diese Variablen ermöglichen es der Container-Orchestrierungslösung, die Laufzeitumgebung zu ändern, ohne den Container neu zu erstellen. Dieses Muster enthält Beispiele für Umgebungsvariablen, die für Blue Age-Anwendungen nützlich sein können.
- Validieren Sie alle Anwendungsabhängigkeiten, bevor Sie Ihre Clari Age-Anwendung ausführen. Stellen Sie beispielsweise sicher, dass die Datenbank verfügbar und die Anmeldeinformationen gültig sind. Schreiben Sie Tests in das Wrapper-Skript, um Abhängigkeiten zu überprüfen, und schlagen Sie frühzeitig fehl, wenn sie nicht erfüllt werden.
- Verwenden Sie die ausführliche Protokollierung innerhalb des Wrapper-Skripts. Die direkte Interaktion mit einem laufenden Container kann je nach Orchestrierungsplattform und der Dauer des Auftrags schwierig sein. Stellen Sie sicher, dass eine nützliche Ausgabe in geschrieben wird`STDOUT`, um Probleme zu diagnostizieren. Beispielsweise kann die Ausgabe den Inhalt des Arbeitsverzeichnisses der Anwendung sowohl vor als auch nach der Ausführung der Anwendung enthalten.

Polen

Anfordern einer JAR-Datei für eine Bol Age-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 – Arbeiten Sie mit Clari Age, um die JAR-Datei Ihrer Anwendung abzurufen.	Der Container in diesem Muster erfordert eine Blue Age-Anwendung. Alternati v können Sie die Java-Beis pielanwendung verwenden , die mit diesem Muster für einen Prototyp bereitgestellt wird. Arbeiten Sie mit dem Clari Age-Team zusammen, um eine JAR-Datei für Ihre Anwendung zu erhalten, die in den Container integriert werden kann. Wenn die JAR-Datei nicht verfügbar ist, lesen Sie die nächste Aufgabe, um stattdessen die Beispiela nwendung zu verwenden.	Cloud-Architekt
Option 2 – Erstellen oder verwenden Sie die bereitges tellte JAR-Beispielanwend ungsdatei.	Dieses Muster bietet eine vorgefertigte JAR-Beisp ieldatei. Diese Datei gibt die Umgebungsvariablen der Anwendung an aus, `STDOUT` bevor sie 30 Sekunden lang in den Ruhezustand versetzt und beendet wird. Diese Datei heißt `bluAgeSam ple.jar` und befindet sich	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Docker-Ordner des GitHub Repositorys. Wenn Sie den Code ändern und Ihre eigene Version der JAR-Datei erstellen möchten, verwenden Sie den Quellcode unter ./java_sample/src/sample_java_app.java im GitHub Repository. Sie können das Build-Skript unter ./java_sample/build.sh verwenden, um die Java-Quelle zu kompilieren und eine neue JAR-Datei zu erstellen.	

Erstellen Sie den Blue Age-Container

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Beispiel-Code-Repository mit dem Befehl : `git clone https://github.com/aws-samples/aws-blu-age-sample-container`	AWS DevOps
Verwenden Sie Docker, um den Container zu erstellen.	Verwenden Sie Docker, um den Container zu erstellen, bevor Sie ihn in eine Docker-Registrierung wie Amazon ECR verschieben:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Navigieren Sie von Ihrem ausgewählten Terminal aus zu dem `docker` Ordner in Ihrem lokalen GitHub Repository. 2. Verwenden Sie diesen Befehl, um den Container zu erstellen: `docker build -t <tag> .` wobei der Container name `<tag>` ist, den Sie verwenden möchten.	
Testen Sie den Blue Age-Container.	(Optional) Testen Sie den Container bei Bedarf lokal mit dem Befehl : `docker run -it <tag> / bin/bash`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizieren Sie sich bei Ihrem Docker-Repository.	Wenn Sie Amazon ECR verwenden möchten, folgen Sie den Anweisungen in der Amazon ECR-Dokumentation, um die AWS CLI zu installieren und zu konfigurieren und die Docker CLI bei Ihrer Standardregistrierung zu authentifizieren. Wir empfehlen, den -get-login-password Befehl für die Authentifizierung zu verwenden. Hinweis: Die Amazon-ECR-Konsole bietet eine vorausgefüllte Version dieses Befehls, wenn Sie die Schaltfläche Push-Befehle anzeigen verwenden. Weitere Informationen finden Sie in der Amazon-ECR-Dokumentation. `aws ecr get-login -password --region <region> | docker login --username AWS --password-stdin <account>.dkr.ecr.<region>.amazonaws.com` Wenn Sie Amazon ECR nicht verwenden möchten, folgen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Anweisungen für Ihr Container-Registry-System.	
Erstellen Sie ein Container-Repository.	Erstellen Sie ein Repository in Amazon ECR. Anweisungen finden Sie im Muster Bereitstellen einer Umgebung für containerisierte Clari Age-Anwendungen mithilfe von Terraform . Wenn Sie ein anderes Container-Registry-System verwenden, folgen Sie den Anweisungen für dieses System.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Markieren Sie Ihren Container und verschieben Sie ihn in das Ziel-Repository.	Wenn Sie Amazon ECR verwenden:
	1. Markieren Sie das lokale Docker-Image mit der Amazon-ECR-Registr ierung und dem Repository, damit Sie es in Ihr Remote-Repository verschieben können:
	`docker tag <tag>:lat est <account> .dkr.ecr.<region>. amazonaws.com/<rep ository>:<versionN umber>`
	2. Verschieben Sie das Image in das Remote-Repository:
	`docker push <account> .dkr.ecr.<region>. amazonaws.com/<rep ository>:<versionN umber>`
	Weitere Informationen finden Sie unter Übertragen eines Docker-Images im Amazon-ECR-Benutzerhandbuch.
		AWS DevOps

Zugehörige Ressourcen

AWS-Ressourcen

- AWS Clari Age-Beispielcontainer-Repository
- Ausführen modernisierter Mainframe-Workloads von Clari Age auf der Serverless-AWS-Infrastruktur
- Bereitstellen einer Umgebung für containerisierte Clari Age-Anwendungen mithilfe von Terraform
- Verwenden von Amazon ECR mit der AWS CLI (Amazon ECR-Benutzerhandbuch)
- Private Registrierungsauthentifizierung (Amazon-ECR-Benutzerhandbuch)
- Amazon-ECS-Dokumentation
- Amazon-EKS-Dokumentation

Weitere Ressourcen

- Blue Age-Website
- Docker-Website

EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken

Erstellt von Luis Gustavo Dantas (AWS)

Quellcode-Repository: Mainframe Data Utilities	Umgebung: PoC oder Pilotprojekt	Quelle: Mainframe-EBCDIC-Daten
Ziel: Verteilte oder in der Cloud modernisierte ASCII-Daten	R-Typ: Replatform	Arbeitslast: IBM
Technologien: Mainframe; Datenbanken; Speicher und Backup; Modernisierung	AWS-Dienste: Amazon EBS; Amazon EC2	

Übersicht

Da Mainframes in der Regel wichtige Geschäftsdaten hosten, ist die Modernisierung von Daten eine der wichtigsten Aufgaben bei der Migration von Daten in die Amazon Web Services (AWS) -Cloud oder eine andere American Standard Code for Information Interchange (ASCII) -Umgebung. Auf Mainframes werden Daten in der Regel im EBCDIC-Format (Extended Binary-Coded Decimal Interchange Code) codiert. Beim Exportieren von Datenbank-, Virtual Storage Access Method-(VSAM) oder Flatfiles werden im Allgemeinen gepackte, binäre EBCDIC-Dateien erzeugt, deren Migration komplexer ist. Die am häufigsten verwendete Lösung für die Datenbankmigration ist Change Data Capture (CDC), bei der in den meisten Fällen die Datenkodierung automatisch konvertiert wird. CDC-Mechanismen sind jedoch möglicherweise nicht für diese Datenbank-, VSAM-oder Flatfiles verfügbar. Für diese Dateien ist ein alternativer Ansatz zur Modernisierung der Daten erforderlich.

Dieses Muster beschreibt, wie EBCDIC-Daten modernisiert werden, indem sie in das ASCII-Format konvertiert werden. Nach der Konvertierung können Sie die Daten in verteilte Datenbanken laden oder Anwendungen in der Cloud die Daten direkt verarbeiten lassen. Das Muster verwendet das Konvertierungsskript und die Beispieldateien im mainframe-data-utilities GitHub Repository.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine EBCDIC-Eingabedatei und das dazugehörige COBOL-Copybook (Common Business-Oriented Language). Eine EBCDIC-Beispieldatei und ein COBOL-Copybook sind im Repository enthalten. mainframe-data-utilities GitHub Weitere Informationen zu COBOL-Copybooks finden Sie im Enterprise COBOL for z/OS 6.4 Programming Guide auf der IBM-Website.

Einschränkungen

- In COBOL-Programmen definierte Datei-Layouts werden nicht unterstützt. Sie müssen separat zur Verfügung gestellt werden.

Produktversionen

- Python Version 3.8 oder höher

Architektur

Quelltechnologie-Stack

- EBCDIC-Daten auf einem Mainframe
- COBOL-Copybook

Zieltechnologie-Stack

- Amazon Elastic Compute Cloud (Amazon EC2) -Instanz in einer virtuellen privaten Cloud (VPC)
- Amazon Elastic Block Store (Amazon EBS)
- Python und die erforderlichen Pakete, JavaScript Object Notation (JSON), sys und datetime
- ASCII-Flatdatei, die bereit ist, von einer modernen Anwendung gelesen oder in eine relationale Datenbanktabelle geladen zu werden

Zielarchitektur

Das Architekturdiagramm zeigt den Prozess der Konvertierung einer EBCDIC-Datei in eine ASCII-Datei auf einer EC2-Instance:

1. Mithilfe des Skripts parse_copybook_to_json.py konvertieren Sie das COBOL-Copybook in eine JSON-Datei.
2. Mithilfe der JSON-Datei und des Skripts extract_ebcdic_to_ascii.py konvertieren Sie die EBCDIC-Daten in eine ASCII-Datei.

Automatisierung und Skalierung

Sobald die für die ersten manuellen Dateikonvertierungen benötigten Ressourcen vorhanden sind, können Sie die Dateikonvertierung automatisieren. Dieses Muster enthält keine Anweisungen zur Automatisierung. Es gibt mehrere Möglichkeiten, die Konvertierung zu automatisieren. Im Folgenden finden Sie einen Überblick über einen möglichen Ansatz:

1. Kapseln Sie die AWS-Befehlszeilenschnittstelle (AWS CLI) und die Python-Skriptbefehle in ein Shell-Skript.
2. Erstellen Sie eine AWS-Lambda-Funktion, die den Shell-Skriptauftrag asynchron an eine EC2-Instance sendet. Weitere Informationen finden Sie unter SSH-Jobs mit AWS Lambda planen.
3. Erstellen Sie einen Amazon Simple Storage Service (Amazon S3) -Trigger, der die Lambda-Funktion jedes Mal aufruft, wenn eine Legacy-Datei hochgeladen wird. Weitere Informationen finden Sie unter Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und diese schnell nach oben oder unten skalieren.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Andere Tools

- GitHubist ein Code-Hosting-Dienst, der Tools für die Zusammenarbeit und Versionskontrolle bereitstellt.
- Python ist eine Programmiersprache auf hohem Niveau.

Code-Repository

Der Code für dieses Muster ist im mainframe-data-utilities GitHub Repository verfügbar.

Epen

Bereiten Sie die EC2-Instanz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten einer EC2-Instance.	Die EC2-Instance muss über ausgehenden Internetzugang verfügen. Dadurch kann die Instanz auf den Python-Qu ellcode zugreifen, der auf verfügbar ist GitHub. Um die Instanz zu erstellen: 1. Öffnen Sie die Amazon EC2 EC2-Konsole unter https://console.aws.amazon.com/ec2. 2. Starten Sie eine EC2-Linux -Instance. Verwenden Sie eine öffentliche IP-Adresse und erlauben Sie eingehend en Zugriff über Port 22.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass die Speichergröße der Instanz mindestens doppelt so groß ist wie die EBCDIC-Datendatei. Anweisungen finden Sie in der Amazon EC2 EC2-Dokumentation.	

Installieren Sie Git.	1. Stellen Sie mithilfe eines Secure Shell (SSH) -Clients eine Verbindung zu der EC2-Instance her, die Sie gerade gestartet haben. Weitere Informationen finden Sie unter Connect zu Ihrer Linux-Instance herstellen.
	2. Führen Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl aus. Dadurch wird Git auf der EC2-Instance installiert.
	`sudo yum install git`
	3. Führen Sie den folgenden Befehl aus und bestätige n Sie, dass Git erfolgreich installiert wurde.
	`git --version`
		Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Python.	1. Führen Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl aus. Dadurch wird Python auf der EC2-Instanz installiert.
	`sudo yum install python3`
	2. Führen Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl aus. Dadurch wird Pip3 auf der EC2-Instance installiert.
	`sudo yum install python3-pip`
	3. Führen Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl aus. Dadurch wird das AWS-SDK für Python (Boto3) auf der EC2-Instance installiert.
	`sudo pip3 install boto3`
	4. Führen Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl aus, in dem `<us-east-1>` sich der Code für Ihre AWS-Region befindet. Eine vollständige Liste der Regionscodes finden Sie
		Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Verfügbare Regionen in der Amazon EC2 EC2-Dokumentation. `export AWS_DEFAU LT_REGION=<us-east -1>`	
Klonen Sie das GitHub Repository.	1. Führen Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl aus. Dadurch wird das mainframe-data-uti litiesRepository aus dem Standard-Kopierort, dem Ordner, geklont GitHub und geöffnet. home `git clone https://g ithub.com/aws-samp les/mainframe-data- utilities.git` 2. Vergewissern Sie sichhome, dass der `mainframe-data-uti lities` Ordner in dem Ordner vorhanden ist.	Allgemeines AWS, GitHub

Erstellen Sie die ASCII-Datei aus den EBCDIC-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie das COBOL-Copybook in die JSON-Layo utdatei.	Führen Sie innerhalb des **`mainframe-data-uti lities`** Ordners das	Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Skript parse_copybook_to_json.py aus. Dieses Automatisierungsmodul liest das Datei-Layout aus einem COBOL-Copybook und erstellt eine JSON-Datei. Die JSON-Datei enthält die Informationen, die zum Interpretieren und Extrahieren der Daten aus der Quelldatei erforderlich sind. Dadurch werden die JSON-Metadaten aus dem COBOL-Copybook erstellt.
	
	Der folgende Befehl konvertiert das COBOL-Copybook in eine JSON-Datei.
	
	`python3 parse_copybook_to_json.py \ -copybook LegacyReference/COBPACK2.cpy \ -output sample-data/cobpack2-list.json \ -dict sample-data/cobpack2-dict.json \ -ebcdic sample-data/COBPACK.OUTFILE.txt \ -ascii sample-data/COBPACK.ASCII.txt \ -print 10000`
	
	Das Skript druckt die empfangenen Argumente.
	
	`---------- ----------`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ------------------ ---------------- Copybook file..... ....| LegacyRef erence/COBPACK2.cpy Parsed copybook (JSON List).| sample-data/ cobpack2-list.json JSON Dict (document ation)...| sample-da ta/cobpack2-dict.json ASCII file..... ....| sample- data/COBPACK.ASCII.t xt EBCDIC file..... ....| sample- data/COBPACK.OUTFILE .txt Print each..... ....| 10000 -------------------- ------------------ ------------------ -------------- ```	
	Weitere Informationen zu den Argumenten finden Sie in der README-Datei im GitHub Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen Sie die JSON-Layoutdatei.	1. Navigieren Sie zu dem im Skript parse_copybook_to_json.py definierten Ausgabepfad. 2. Überprüfen Sie die Erstellungszeit der Datei sample-data/cobpack2-list.json, um sicherzustellen, dass Sie die entsprechende JSON-Layoutdatei ausgewählt haben. 3. Untersuchen Sie die JSON-Datei und stellen Sie sicher, dass der Inhalt dem Folgenden ähnelt. `"input": "extract-ebcdic-to-ascii/COBPACK.OUTFILE.txt", "output": "extract-ebcdic-to-ascii/COBPACK.ASCII.txt", "max": 0, "skip": 0, "print": 10000, "lrecl": 150, "rem-low-values": true, "separator": "|", "transf": [ { "type": "ch", "bytes": 19, "name": "OUTFILE-TEXT" }`	Allgemein AWS, JSON

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die wichtigsten Attribute der JSON-Layoutdatei sind: • `input`— Enthält den Pfad der zu konvertierenden EBCDIC-Datei • `output`— Definiert den Pfad, in dem die ASCII-Datei generiert wird • `lrecl`— Gibt die Größe der logischen Datensatzlänge in Byte an • `transf`— Listet alle Felder und ihre Größe in Byte auf Weitere Informationen zur JSON-Layoutdatei finden Sie in der README-Datei im GitHub Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die ASCII-Datei.	Führen Sie das Skript extract_ebcdic_to_ascii.py aus, das im GitHub geklonten Repository enthalten ist. Dieses Skript liest die EBCDIC-Datei und schreibt eine konvertierte und lesbare ASCII-Datei.
	`python3 extract_ebcdic_to_ascii.py -local-json sample-data/cobpack2-list.json`
	Während das Skript die EBCDIC-Daten verarbeitet, druckt es für jeden Stapel von 10.000 Datensätzen eine Nachricht. Sehen Sie sich das folgende -Beispiel an.
	`---------- 2023-05-15 21:21:46.322253 | Local Json file | -local-json | sample-data/cobpack2-list.json 2023-05-15 21:21:47.034556 | Records processed | 10000 2023-05-15 21:21:47.736434 | Records processed | 20000`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2023-05-15 21:21:48. 441696 | Records processed | 30000 2023-05-15 21:21:49. 173781 | Records processed | 40000 2023-05-15 21:21:49. 874779 | Records processed | 50000 2023-05-15 21:21:50. 705873 | Records processed | 60000 2023-05-15 21:21:51. 609335 | Records processed | 70000 2023-05-15 21:21:52. 292989 | Records processed | 80000 2023-05-15 21:21:52. 938366 | Records processed | 89280 2023-05-15 21:21:52. 938448 Seconds 6.616232 Informationen zum Ändern der Druckfrequenz finden Sie in der README-Datei im Repository. GitHub	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen Sie die ASCII-Datei.	1. Überprüfen Sie die Erstellungszeit der Datei extract-ebcdic-to-ascii/CobPack.ASCII.txt, um sicherzustellen, dass sie kürzlich erstellt wurde. 2. Geben Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl ein. Dadurch wird der erste Datensatz der ASCII-Datei geöffnet. `head sample-data/COBPACK.ASCII.txt -n 1| xxd` 3. Untersuchen Sie den Inhalt des ersten Datensatzes. Da EBCDIC-Dateien normalerweise binär sind, enthalten sie keine CRLF-Sonderzeichen (Carriage Return and Line Feed). Das Skript extract_ebcdic_to_ascii.py fügt ein Pipezeichen als Spaltentrennzeichen hinzu, das in den Skriptparametern definiert ist. Wenn Sie die bereitgestellte EBCDIC-Beispieldatei verwendet haben, ist der folgende Datensatz der erste Datensatz in der ASCII-Datei.	Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	00000000: 2d30 3030 3030 3030 3030 3130 3030 3030 -000000000100000 00000010: 3030 307c 3030 3030 3030 3030 3031 3030 000|00000 0000100 00000020: 3030 3030 3030 7c2d 3030 3030 3030 3030 000000|-0 0000000 00000030: 3031 3030 3030 3030 3030 7c30 7c30 7c31 0100000000| 0|0|1 00000040: 3030 3030 3030 3030 7c2d 3130 3030 3030 00000000| -100000 00000050: 3030 307c 3130 3030 3030 3030 307c 2d31 000|10000 0000|-1 00000060: 3030 3030 3030 3030 7c30 3030 3030 7c30 00000000| 00000|0 00000070: 3030 3030 7c31 3030 3030 3030 3030 7c2d 0000|1000 00000|- 00000080: 3130 3030 3030 3030 307c 3030 3030 3030 100000000| 000000 00000090: 3030 3030 3130 3030 3030 3030 307c 2d30 000010000 0000|-0 000000a0: 3030 3030 3030 3030 3031 3030	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3030 3030 000000000 1000000 000000b0: 3030 7c41 7c41 7c0a 00|A|A|.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Evaluieren Sie die EBCDIC-Datei.	Geben Sie in der Amazon EC2 EC2-Konsole den folgenden Befehl ein. Dadurch wird der erste Datensatz der EBCDIC-Datei geöffnet.
	`head sample-data/COBPACK.OUTFILE.txt -c 150 | xxd`
	Wenn Sie die EBCDIC-Beispieldatei verwendet haben, ist das Ergebnis wie folgt.
	`00000000: 60f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 f0f0 `........ .... 00000010: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 ..... 00000020: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 ..... 00000030: f0f0 f0f0 f0f0 d000 0000 0005 f5e1 00fa ..... 00000040: 0a1f 0000 0000 0005 f5e1 00ff ffff fffa ..... 00000050: 0a1f 0000 000f 0000 0c10 0000 000f 1000 .....`
		Allgemein AWS, Linux, EBCDIC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	00000060: 0000 0d00 0000 0000 1000 0000 0f00 0000 .... 00000070: 0000 1000 0000 0dc1 c100 0000 0000 0000 .... 00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .... 00000090: 0000 0000 0000 ...... Um die Gleichwertigkeit zwischen den Quell- und Zieldateien zu bewerten, sind umfassende Kenntnisse über EBCDIC erforderlich. Das erste Zeichen der EBCDIC-Beispieldatei ist beispielsweise ein Bindestrich (). - In der hexadezimalen Schreibweise der EBCDIC-Datei wird dieses Zeichen durch dargestellt60, und in der hexadezimalen Schreibweise der ASCII-Datei wird dieses Zeichen durch dargestellt. 2D Eine Umrechnungstabelle von EBCDIC in ASCII finden Sie auf der IBM-Website unter EBCDIC in ASCII.	

Zugehörige Ressourcen

Referenzen

- Der EBCDIC-Zeichensatz (IBM-Dokumentation)
- EBCDIC zu ASCII (IBM-Dokumentation)
- COBOL (IBM-Dokumentation)
- Grundlegende JCL-Konzepte (IBM-Dokumentation)
- Connect zu Ihrer Linux-Instance her (Amazon EC2 EC2-Dokumentation)

Tutorials

- Planung von SSH-Jobs mit AWS Lambda (AWS-Blogbeitrag)
- Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion (AWS Lambda Lambda-Dokumentation)

Konvertieren von Mainframe-Dateien aus dem EBCDIC-Format in das zeichengetrennte ASCII-Format in Amazon S3 mit AWS Lambda

Erstellt von Luis Gustavo Dantas (AWS)

Code-Repository: Mainframe Data Utilities	Umgebung: PoC oder Pilotprojekt	Quelle: IBM EBCDIC-Dateien
Ziel: abgegrenzte ASCII-Dateien	R-Typ: Plattformwechsel	Workload: IBM
Technologien: Mainframe	AWS-Services: AWS CloudShell; AWS Lambda ; Amazon S3; Amazon CloudWatch	

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine AWS Lambda-Funktion starten, die automatisch Mainframe-EBCDIC-Dateien (Extended Binary Coded Decimal Interchange Code) in ASCII-Dateien (Class Standard Code for Information Interchange) mit Zeichenbegrenzung konvertiert. Die Lambda-Funktion wird ausgeführt, nachdem die ASCII-Dateien in einen Amazon Simple Storage Service (Amazon S3)-Bucket hochgeladen wurden. Nach der Dateikonvertierung können Sie die ASCII-Dateien auf x86-basierten Workloads lesen oder die Dateien in moderne Datenbanken laden.

Der in diesem Muster gezeigte Ansatz zur Dateikonvertierung kann Ihnen helfen, die Herausforderungen bei der Arbeit mit EBCDIC-Dateien in modernen Umgebungen zu bewältigen. In EBCDIC codierte Dateien enthalten häufig Daten, die im binären oder gepackten Dezimalformat dargestellt werden, und Felder haben eine feste Länge. Diese Merkmale verursachen Hindernisse, da moderne x86-basierte Workloads oder verteilte Umgebungen im Allgemeinen mit ASCII-kodierten Daten funktionieren und keine EBCDIC-Dateien verarbeiten können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket
- Ein AWS Identity and Access Management (IAM)-Benutzer mit Administratorberechtigungen
- AWS CloudShell
- Python 3.8.0 oder höher
- Eine flache Datei, die in EBCDIC und der entsprechenden Datenstruktur in einem gemeinsamen COBOL-Kopierbuch (Business-Orient Language) codiert ist

Hinweis: Dieses Muster verwendet eine EBCDIC-Beispieldatei (CLIENT.EBCDIC.txt) und das entsprechende COBOL-Kopierbook (COBKS05.cpy). Beide Dateien sind im GitHub mainframe-data-utilitiesRepository verfügbar.

Einschränkungen

- COBOL-Kopierbücher enthalten normalerweise mehrere Layoutdefinitionen. Das mainframe-data-utilities Projekt kann diese Art von Copybook analysieren, kann aber nicht ableiten, welches Layout bei der Datenkonvertierung berücksichtigt werden soll. Dies liegt daran, dass Copybooks diese Logik nicht enthalten (die stattdessen in COBOL-Programmen verbleibt). Folglich müssen Sie die Regeln für die Auswahl von Layouts manuell konfigurieren, nachdem Sie das Copybook analysiert haben.
- Dieses Muster unterliegt den Lambda-Kontingenten .

Architektur

Quelltechnologie-Stack

- IBM z/OS, IBM i und andere EBCDIC-Systeme
- Sequenzielle Dateien mit in EBCDIC codierten Daten (z. B. IBM-Db2-Entladungen)
- COBOL-Kopierbuch

Zieltechnologie-Stack

- Amazon S3
- Amazon S3-Ereignisbenachrichtigung
- IAM

- Lambda-Funktion
- Python 3.8 oder höher
- Mainframe-Datenauslastungen
- JSON-Metadaten
- ASCII-Dateien mit Trennzeichen

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur zum Konvertieren von Mainframe-EBCDIC-Dateien in ASCII-Dateien.

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer führt das Copybook-Parser-Skript aus, um das COBOL-Kopierbook in eine JSON-Datei zu konvertieren.
2. Der Benutzer lädt die JSON-Metadaten in einen S3-Bucket hoch. Dadurch sind die Metadaten für die Lambda-Funktion zur Datenkonvertierung lesbar.
3. Der Benutzer oder ein automatisierter Prozess lädt die EBCDIC-Datei in den S3-Bucket hoch.
4. Das S3-Benachrichtigungsereignis löst die Lambda-Funktion zur Datenkonvertierung aus.
5. AWS überprüft die Lese-/Schreibberechtigungen des S3-Buckets für die Lambda-Funktion.
6. Lambda liest die Datei aus dem S3-Bucket und konvertiert die Datei lokal von EBCDIC nach ASCII.
7. Lambda protokolliert den Prozessstatus in Amazon CloudWatch.
8. Lambda schreibt die ASCII-Datei zurück in Amazon S3.

Hinweis: Das Copybook-Parser-Skript wird nur einmal ausgeführt, nachdem die Metadaten in JSON konvertiert und diese Daten dann in einen S3-Bucket hochgeladen wurden. Nach der ersten Konvertierung verwendet jede EBCDIC-Datei, die dieselbe JSON-Datei verwendet, die in den S3-Bucket hochgeladen wird, dieselben Metadaten.

Tools

AWS-Tools

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS CloudShell ist eine browserbasierte Shell, mit der Sie AWS-Services mithilfe der AWS Command Line Interface (AWS CLI) und einer Reihe vorinstallierter Entwicklungstools verwalten können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die von Ihnen genutzte Rechenzeit bezahlen.

Andere Tools

- GitHub ist ein Code-Hosting-Service, der Tools für die Zusammenarbeit und Versionskontrolle bereitstellt.
- Python ist eine allgemeine Programmiersprache.

Code

Der Code für dieses Muster ist im GitHub mainframe-data-utilitiesRepository verfügbar.

Bewährte Methoden

Berücksichtigen Sie die folgenden bewährten Methoden:

- Legen Sie die erforderlichen Berechtigungen auf Ebene des Amazon-Ressourcennamens (ARN) fest.
- Erteilen Sie immer die geringsten Berechtigungen für IAM-Richtlinien. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in IAM in der IAM-Dokumentation.

Sekunden

Erstellen von Umgebungsvariablen und eines Arbeitsordners

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Umgebungs variablen.	Kopieren Sie die folgenden Umgebungsvariablen in einen Texteditor und ersetzen Sie dann die <placeholder>-Wert e im folgenden Beispiel durch Ihre Ressourcenwerte: `bucket=<your_bucke t_name> account=<your_accou nt_number> region=<your_reg ion_code>` Hinweis: Sie erstellen später Verweise auf Ihren S3-Bucket, Ihr AWS-Konto und Ihre AWS-Region. Um Umgebungsvariablen zu definieren, öffnen Sie die CloudShell -Konsole und kopieren Sie dann Ihre aktualisierten Umgebungs variablen und fügen Sie sie in die Befehlszeile ein. Hinweis: Sie müssen diesen Schritt bei jedem Neustart der CloudShell Sitzung wiederhol en.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Arbeitsordner.	Um den Vorgang der Ressourcenbereinigung zu einem späteren Zeitpunkt zu vereinfachen, erstellen Sie einen Arbeitsordner in , CloudShell indem Sie den folgenden Befehl ausführen: `mkdir workdir; cd workdir` Hinweis: Sie müssen das Verzeichnis jedes Mal in das Arbeitsverzeichnis (`workdir`) ändern, wenn Sie eine Verbindung zu Ihrer CloudShell Sitzung verlieren.	Allgemeines AWS

Definieren einer IAM-Rolle und -Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Vertrauensrichtlinie für die Lambda-Funktion.	Der EBCDIC-Konverter wird in einer Lambda-Funktion ausgeführt. Die Funktion muss über eine IAM-Rolle verfügen. Bevor Sie die IAM-Rolle erstellen, müssen Sie ein Vertrauensrichtliniendokument definieren, das es Ressourcen ermöglicht, diese Richtlinie zu übernehmen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellen Sie im CloudShell Arbeitsordner ein Richtlinendokument, indem Sie den folgenden Befehl ausführen: `E2ATrustPol=$(cat <<EOF { "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] } EOF ) printf "$E2ATrustPol" > E2ATrustPol.json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle für die Lambda-Konvertierung.	Um eine IAM-Rolle zu erstellen, führen Sie den folgenden AWS CLI-Befehl im CloudShell Arbeitsordner aus: `aws iam create-role --role-name E2AConvLambdaRole --assume-role-policy-document file://E2ATrustPol.json`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das IAM-Richtliniendokument für die Lambda-Funktion.	Die Lambda-Funktion muss über Lese-/Schreibzugriff auf den S3-Bucket und Schreibberechtigungen für Amazon CloudWatch Logs verfügen.
	
	Um eine IAM-Richtlinie zu erstellen, führen Sie den folgenden Befehl im CloudShell Arbeitsordner aus:
	
	`E2APolicy=$(cat <<EOF`
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Logs",`
	`"Effect": "Allow",`
	`"Action": [`
	`"logs:PutLogEvents",`
	`"logs:CreateLogStream",`
	`"logs:CreateLogGroup"`
	`],`
	`"Resource": [`
	`"arn:aws:logs:*:*:log-group:*",`
	`"arn:aws:logs:*:*:log-group:*:log-stream:*"`
	`]
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> },
	        {
	            "Sid": "S3",
	            "Effect":
	"Allow",
	            "Action": [
	
	"s3:GetObject",
	
	"s3:PutObject",
	
	"s3:GetObjectVersion"
	            ],
	            "Resource":
	[
	
	"arn:aws:s3:::%s/*",
	
	"arn:aws:s3:::%s"
	            ]
	        }
	    ]
	}
	EOF
	)
	printf "$E2APolicy"
	"$bucket" "$bucket"
	> E2AConvLambdaPolic
	y.json</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie das IAM-Richt liniendokument an die IAM-Rolle an.	Um die IAM-Richtlinie an die IAM-Rolle anzuhängen, führen Sie den folgenden Befehl aus Ihrem CloudShell Arbeitsor dner aus: `aws iam put-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy --policy-document file://E2AConvLambdaPolicy.json`	Allgemeines AWS

Erstellen der Lambda-Funktion für die EBCDIC-Konvertierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode der EBCDIC-Konvertierung herunter.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um den mainframe -data-utilities Quellcode von herunterzuladen GitHub: `git clone https://github.com/aws-samples/mainframe-data-utilities.git mdu`	Allgemeines AWS
Erstellen Sie das ZIP-Paket.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um das ZIP-Paket zu erstellen, das die Lambda-Funktion für die EBCDIC-Ko nvertierung erstellt:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd mdu; zip ../mdu.zip *.py; cd ..`	
So erstellen Sie die Lambda-Funktion:	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Lambda-Funktion für die EBCDIC-Konvertierung zu erstellen: `aws lambda create-function \ --function-name E2A \ --runtime python3.9 \ --zip-file fileb://mdu.zip \ --handler extract_ebcdic_to_ascii.lambda_handler \ --role arn:aws:iam::$account:role/E2AConvLambdaRole \ --timeout 10 \ --environment "Variables={layout=$bucket/layout/}"` Hinweis: Das Layout der Umgebungsvariablen teilt der Lambda-Funktion mit, wo sich die JSON-Metadaten befinden.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die ressourcenbasierte Richtlinie für die Lambda-Funktion.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, damit Ihre Amazon S3-Ereignisbenachrichtigung die Lambda-Funktion für die EBCDIC-Konvertierung auslösen kann:
	`aws lambda add-permission \`
	`--function-name E2A \`
	`--action lambda:InvokeFunction \`
	`--principal s3.amazonaws.com \`
	`--source-arn arn:aws:s3:::$bucket \`
	`--source-account $account \`
	`--statement-id 1`
		Allgemeines AWS

Erstellen der Amazon S3-Ereignisbenachrichtigung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Konfigurationsdokument für die Amazon S3-Ereignisbenachrichtigung.	Die Amazon S3-Ereignisbenachrichtigung initiiert die Lambda-Funktion zur EBCDIC-Konvertierung, wenn Dateien im Eingabeordner abgelegt werden. Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um das JSON-Dokument für die Amazon S3-	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ereignisbenachrichtigung zu erstellen: `{ "LambdaFunctionConfigurations": [{ "Id": "E2A", "LambdaFunctionArn": "arn:aws:lambda:%s:%s:function:E2A", "Events": ["s3:ObjectCreated:Put"], "Filter": { "Key": { "FilterRules": [{ "Name": "prefix", "Value": "input/" }] } } }] } EOF) printf "$S3E2AEvent" "$region" "$account" > S3E2AEvent.json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon S3-Ereignisbenachrichtigung.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Amazon S3-Ereignisbenachrichtigung zu erstellen: `aws s3api put-bucket-notification-configuration --bucket $bucket --notification-configuration file://S3E2AEvent.json`	Allgemeines AWS

Erstellen und Hochladen der JSON-Metadaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Parsen Sie das COBOL-Kopierbook.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um ein COBOL-Beispielkopierbuch in eine JSON-Datei zu parsen (in der definiert wird, wie die Datendatei korrekt gelesen und aufgeteilt wird):
	`python3 mdu/parse_copybook_to_json.py \`
	`-copybook mdu/LegacyReference/COBKS05.cpy \`
	`-output CLIENT.json \`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`-output-s3key CLIENT.AS CII.txt \`
	`-output-s3bkt $bucket \`
	`-output-type  s3 \`
	`-print  25`	

Fügen Sie die Transform ationsregel hinzu.	Die Beispieldatendatei und das entsprechende COBOL-Kopierbook sind eine Datei mit mehreren Layouts. Das bedeutet, dass die Konvertie rung Daten basierend auf bestimmten Regeln aufteilen muss. In diesem Fall definiere n Bytes an Position 3 und 4 in jeder Zeile das Layout.
	
	Bearbeiten Sie im CloudShell Arbeitsordner die `CLIENT.js on` Datei und ändern Sie den Inhalt von `"transf-rule": [],` in Folgendes:
	
	`"transf-rule": [`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0002",`
	`"transf": "transf1"`
	`},`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0000",`
	`"transf": "transf2"`
	`}`
	`],`
		Allgemeines AWS, IBM Mainframe, Cobol

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die JSON-Meta daten in den S3-Bucket hoch.	Führen Sie im CloudShell Arbeitsordner den folgenden AWS CLI-Befehl aus, um die JSON-Metadaten in Ihren S3-Bucket hochzuladen: `aws s3 cp CLIENT.json s3://$bucket/layout/CLIENT.json`	Allgemeines AWS

Konvertieren der EBCDIC-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die EBCDIC-Datei an den S3-Bucket.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die EBCDIC-Datei an den S3-Bucket zu senden: `aws s3 cp mdu/sample-data/CLIENT.EBCDIC.txt s3://$bucket/input/` Hinweis: Wir empfehlen, verschiedene Ordner für Eingabe- (EBCDIC) und Ausgabedateien (ASCII) festzulegen, damit die Lambda-Konvertierungsfunktion nicht erneut aufgerufen wird, wenn die ASCII-Datei in den S3-Bucket hochgeladen wird.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Ausgabe.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um zu überprüfe n, ob die ASCII-Datei in Ihrem S3-Bucket generiert wird:
	`awss3 ls s3://$bucket/`
	Hinweis: Die Datenkonv ertierung kann mehrere Sekunden dauern. Wir empfehlen Ihnen, einige Male nach der ASCII-Datei zu suchen.
	Nachdem die ASCII-Datei verfügbar ist, führen Sie den folgenden Befehl aus, um die Datei aus dem S3-Bucket in den aktuellen Ordner herunterzuladen:
	`aws s3 cp s3://$bucket/ CLIENT.ASCII.txt .`
	Überprüfen Sie den Inhalt der ASCII-Datei:
	`head CLIENT.ASCII.txt`
		Allgemeines AWS

Bereinigen der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

(Optional) Bereiten Sie die Variablen und den Ordner vor.	Wenn Sie die Verbindung mit verlieren CloudShell, stellen Sie erneut eine Verbindung her und führen Sie dann den folgenden Befehl aus, um das Verzeichnis in den Arbeitsordner zu ändern:
	`cd workdir`
	Stellen Sie sicher, dass die Umgebungsvariablen definiert sind:
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
		Allgemeines AWS

Entfernen Sie die Benachrichtigungskonfiguration für den Bucket.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Konfiguration der Amazon S3-Ereignisbenachrichtigung zu entfernen:
	`aws s3api put-bucket-notification-configuration \`
	`--bucket=$bucket \`
	`--notification-configuration="{}"`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Lambda-Funktion.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Lambda-Funktion für den EBCDIC-Konverter zu löschen: `awslambdadelete-function--function-nameE2A`	Allgemeines AWS

Löschen Sie die IAM-Rolle und -Richtlinie.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Rolle und Richtlinie des EBCDIC-Konverters zu entfernen:
	`aws iam delete-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy`
	
	`aws iam delete-role --role-name E2AConvLambdaRole`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie die im S3-Bucket generierten Dateien.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die im S3-Bucket generierten Dateien zu löschen:
	`aws s3 rm s3://$bucket/layout --recursive`
	`aws s3 rm s3://$bucket/input --recursive`
	`aws s3 rm s3://$bucket/CLIENT.ASCII.txt`
		Allgemeines AWS

Löschen Sie den Arbeitsordner.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um `workdir` und seinen Inhalt zu entfernen: `cd ..; rm -Rf workdir`	Allgemeines AWS

Zugehörige Ressourcen

- README für Mainframe Data Utilities (GitHub)
- Der EBCDIC-Zeichensatz (IBM-Dokumentation)
- EBCDIC zu ASCII (IBM-Dokumentation)
- COBOL (IBM-Dokumentation)
- Verwenden eines Amazon S3-Auslösers zum Aufrufen einer Lambda-Funktion (AWS Lambda-Dokumentation)

Konvertieren von Mainframe-Datendateien mit komplexen Datensatzlayouts mit Micro Focus

Erstellt von West

Umgebung: Produktion	Quelle: Mainframe-EBCDIC-Datendateien	Ziel: Micro Focus ASCII-Datendateien
R-Typ: Hostwechsel	Workload: Alle anderen Workloads	Technologien: Mainframe; Modernisierung
AWS-Services: AWS Mainframe Modernization		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Mainframe-Datendateien mit Nichttextdaten und komplexen Datensatzlayouts von der EBCDIC-Zeichenkodierung (Extended Binary Coded Decimal Interchange Code) in die ASCII-Zeichenkodierung (Speed Standard Code for Information Interchange) mithilfe einer Micro Focus-Strukturdatei konvertieren. Um die Dateikonvertierung abzuschließen, müssen Sie Folgendes tun:

1. Bereiten Sie eine einzelne Quelldatei vor, die alle Datenelemente und Datensatzlayouts in Ihrer Mainframe-Umgebung beschreibt.
2. Erstellen Sie eine Strukturdatei, die das Datensatzlayout der Daten enthält, indem Sie den Micro Focus Data File Editor als Teil der Micro Focus Classic Data File Tools oder Data File Tools verwenden. Die Strukturdatei identifiziert die Nicht-Textdaten, sodass Sie Ihre Mainframe-Dateien korrekt von EBCDIC nach ASCII konvertieren können.
3. Testen Sie die Strukturdatei mithilfe der Classic Data File Tools oder Data File Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Micro Focus Enterprise Developer für Windows, verfügbar über AWS Mainframe Modernization

Produktversionen

- Micro Focus Enterprise Server 7.0 und höher

Tools

- Micro Focus Enterprise Developer bietet die Ausführungsumgebung für Anwendungen, die mit jeder IDE-Variante (Integrated Development Environment) von Enterprise Developer erstellt wurden.
- Micro Focus Classic Data File Tools helfen Ihnen beim Konvertieren, Navigieren, Bearbeiten und Erstellen von Datendateien. Zu den Classic Data File Tools gehören Data File Converter , Record Layout Editor und Data File Editor .
- Micro Focus Data File Tools helfen Ihnen beim Erstellen, Bearbeiten und Verschieben von Datendateien. Zu den Datendatei-Tools gehören der Datendatei-Editor , Dateikonvertierungsdienstprogramme und das Befehlszeilen-Hilfsprogramm für die Datendateistruktur .

Polen

Vorbereiten der Quelldatei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Quellkomponenten.	Identifizieren Sie alle möglichen Datensatzlayouts für die Datei, einschließlich aller Neudefinitionen, die Nicht-Textdaten enthalten. Wenn Sie Layouts haben, die Neudefinitionen enthalten , müssen Sie diese Layouts auf eindeutige Layouts reduzieren, die jede mögliche	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Permutation der Datenstruktur beschreiben. In der Regel können die Datensatzlayouts einer Datendatei durch die folgenden Archetypen beschrieben werden: • Datensatzlayout nur mit Textdaten • Datensatzlayout mit Nicht-Textdaten • Datensatzlayout mit Nicht-Textdaten, die einer REDEFINES-Klausel untergeordnet sind Weitere Informationen zum Erstellen von vereinfachten Datensatzlayouts für Dateien, die komplexe Datensatzlayouts enthalten, finden Sie unter Hostwechsel von EBCDIC-Anwendungen in ASCII-Umgebungen für Mainframe-Migrationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Identifizieren Sie die Layoutbedingungen für Datensätze.	Identifizieren Sie für Dateien mit mehreren Datensatz layouts oder Dateien, die komplexe Layouts mit einer REDEFINES-Klausel enthalten, die Daten und Bedingungen innerhalb eines Datensatzes, mit denen Sie definieren können, welches Layout während der Konvertie rung verwendet werden soll. Wir empfehlen Ihnen, diese Aufgabe mit einem Fachexper ten (SME) zu besprechen, der die Programme zur Verarbeit ung dieser Dateien versteht.
	
	Beispielsweise kann eine Datei zwei Datensatztypen enthalten, die Nicht-Tex tdaten enthalten. Sie können die Quelle überprüfen und möglicherweise Code ähnlich dem folgenden finden:
	
	`MOVE "M" TO PART-TYPE`
	`MOVE "MAIN ASSEMBLY" TO`
	`PART-NAME`
	`MOVE "S" TO PART-TYPE`
	`MOVE "SUB ASSEMBLY 1"`
	`TO PART-NAME`
	
	Der Code hilft Ihnen, Folgendes zu identifizieren:
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Das Feld „PART-TYPE“ wird verwendet, um den Datensatztyp zu bestimmen • Der Wert „M“ wird für das „M-PART-RECORD“ verwendet • Der Wert „S“ wird für das „S-PART-RECORD“ verwendet Sie können die Werte dokumentieren, die von diesem Feld verwendet werden, um die Datensatz layouts den richtigen Datensätzen in der Datei zuzuordnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quelldatei.	Wenn die Datei über mehrere Quelldateien hinweg beschrieb en wird oder das Datensatz layout Nichttextdaten enthält, die einer REDEFINES-Klausel untergeordnet sind, erstellen Sie eine neue Quelldatei, die die Datensatzlayouts enthält. Das neue Programm muss die Datei nicht mithilfe von SELECT- und FD-Anweis ungen beschreiben. Das Programm kann einfach die Datensatzbeschreibungen als 01 Ebenen in Working-Storage enthalten. Hinweis: Sie können für jede Datendatei eine Quelldatei erstellen oder eine Master-Quelldatei erstellen, die alle Datendateien beschreibt.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kompilieren Sie die Quelldatei.	Kompilieren Sie die Quelldatei, um das Datenwörterbuch zu erstellen. Wir empfehlen, die Quelldatei mit dem EBCDIC-Zeichensatz zu kompilieren. Wenn die IBMCOMP- oder ODOSLIDE-Richtlinien verwendet werden, müssen Sie diese Richtlinien auch in der Quelldatei verwenden. Hinweis: IBMCOMP wirkt sich auf die Byte-Speicherung von COMP-Feldern aus und ODOSLIDE wirkt sich auf das Padding auf OCCURS VARYING-Strukturen aus. Wenn diese Anweisungen falsch festgelegt sind, liest das Konvertierungstool den Datensatz nicht korrekt. Dies führt zu fehlerhaften Daten in der konvertierten Datei.	App-Developer

(Option A) Erstellen der Strukturdatei mit Classic Data File Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie das Tool und laden Sie das Wörterbuch.	1. Wählen Sie das Windows-Startmenü-Symbol, suchen Sie nach und wählen Sie Micro Focus Enterprise Developer und dann Classic Data File Tools aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Datei und dann Layout aufzeichnen aus. 3. Wählen Sie im Dialogfeld Eine Datei auswählen, aus der die Layouts erstellt werden sollen für Dateiname die IDY-Datei (`.idy`) aus, die beim vorherigen Kompilieren der Quelldatei erstellt wurde. Wählen Sie dann Open (Öffnen) aus. 4. Um zu bestätigen, dass Classic Data File Tools EBCDIC verwendet, wählen Sie im Dialogfeld Data File Tools die Option YES aus, wenn die IDY-Datei auf EBCDIC und Datatools auf ANSI gesetzt ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Standard-Datensatzlayout.	Verwenden Sie das Standard-Datensatzlayout für alle Datensätze, die keinem bedingten Layout entsprechen. 1. Erweitern Sie im Fenster Layout die Datenstruktur und suchen Sie dann die Ebene 01, die für das Standardlayout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Neues Layout aus. 3. Wählen Sie im Dialogfeld Assistent für das neue Datensatzlayout die Option Standardlayout und dann Weiter aus. 4. Wählen Sie Finish (Abschließen). Das Standardlayout wird im Bereich Layouts angezeigt und kann durch das rote Ordnersymbol identifiziert werden.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein bedingtes Datensatzlayout.	Verwenden Sie das bedingte Datensatzlayout, wenn es mehr als ein Datensatzlayout in einer Datei gibt. 1. Erweitern Sie im Bereich Layouts die Datenstru ktur und suchen Sie dann die Ebene 01, die für das bedingte Layout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Neues Layout aus. 3. Wählen Sie im Dialogfel d Assistent für das neue Datensatzlayout die Option Bedingtes Layout und dann Weiter aus. 4. Wählen Sie Finish (Abschlie ßen). Das bedingte Layout wird im Bereich Layouts angezeigt und kann durch das gelbe Ordnersymbol identifiziert werden. 5. Erweitern Sie das bedingte Layout, klicken Sie mit der rechten Maustaste auf das Feld, in dem Sie eine Bedingung platziere n müssen, und wählen Sie dann Eigenschaften aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie im Dialogfel d Feldeigenschaften die Bedingung ein. Vergewiss ern Sie sich, dass der Zeichensatz auf EBCDIC festgelegt ist, und wählen Sie dann OK aus. Neben dem Feld mit einem Bedingungssatz wird ein Häkchen angezeigt. 7. Wiederholen Sie die Schritte 5 bis 6 für alle anderen Felder, die Bedingungen für dieses Layout erfordern. 8. Wiederholen Sie die Schritte 1 bis 6 für alle anderen bedingten Layouts, die hinzugefügt werden müssen. 9. Wählen Sie Datei, wählen Sie Speichern unter und speichern Sie die Strukturd atei dann auf der Festplatte.	

(Option B) Erstellen der Strukturdatei mit Datendatei-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie das Tool und laden Sie das Wörterbuch.	1. Wählen Sie das Windows-Startmenü-Symbol, suchen Sie nach und wählen Sie Micro Focus Enterprise	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Developer und wählen Sie dann Datendatei-Tools aus. 2. Wählen Sie Datei , Neu, Strukturdatei aus. 3. Wählen Sie im Dialogfeld Öffnen für Dateiname die IDY-Datei () aus, die erstellt wurde, als Sie die Quelldatei zuvor kompiliert haben. `.idy` Wählen Sie dann Open (Öffnen) aus. 4. Um zu bestätigen, dass Data File Tools EBCDIC verwendet, bestätigen Sie, dass das Dropdown-Menü im Abschnitt Debug File auf EBCDIC gesetzt ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Standard-Datensatzlayout.	Verwenden Sie das Standard-Datensatzlayout für alle Datensätze, die keinem bedingten Layout entsprechen. 1. Erweitern Sie im Abschnitt Verfügbare Layouts im linken Bereich die Datenstruktur und suchen Sie dann die Ebene 01, die für das Standardlayout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Standardlayout erstellen aus. Das Standardlayout wird im Bereich Layouts angezeigt und kann durch das blaue „D“-Symbol identifiziert werden.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein bedingtes Datensatzlayout.	Verwenden Sie das bedingte Datensatzlayout, wenn es mehr als ein Datensatzlayout in einer Datei gibt. 1. Erweitern Sie im Abschnitt Ausgewählte Layouts im rechten Bereich die Datenstruktur und suchen Sie dann die Ebene 01, die für das bedingte Layout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie Bedingtes Layout erstellen aus. Das bedingte Layout wird im Bereich Layouts auf der rechten Seite angezeigt und kann durch das grüne „C“-Symbol identifiziert werden. 3. Erweitern Sie das bedingte Layout, klicken Sie mit der rechten Maustaste auf das Feld, in dem Sie eine Bedingung platziere n müssen, und wählen Sie dann Eigenschaften aus. 4. Geben Sie im Dialogfel d Feldeigenschaften die Bedingung ein. Vergewiss ern Sie sich, dass der Zeichensatz auf EBCDIC	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	festgelegt ist, und wählen Sie dann OK aus. Neben dem Feld mit einem Bedingungssatz wird ein rotes „IF“-Symbol angezeigt . 5. Wiederholen Sie die Schritte 3 bis 4 für alle anderen Felder, die Bedingungen für dieses Layout erfordern. 6. Wiederholen Sie die Schritte 1 bis 4 für alle anderen bedingten Layouts, die hinzugefügt werden müssen. 7. Wählen Sie Datei , wählen Sie Speichern unter und speichern Sie die Strukturd atei dann auf der Festplatte.	

(Option A) Testen der Strukturdatei mit Classic Data File Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie eine EBCDIC-Da tendatei.	Vergewissern Sie sich, dass Sie Ihre Strukturdatei verwenden können, um eine EBCDIC-Testdatendatei korrekt anzuzeigen. 1. Wählen Sie das Windows-Startmenü-Symbol, suchen und wählen Sie Micro	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Focus Enterprise Developer und dann Classic Data Tools aus. 2. Wählen Sie Datei und dann Öffnen aus. 3. Wählen Sie im Dialogfeld Öffnen für Dateiname den EBCDIC-Datensatz aus und wählen Sie dann Öffnen aus. 4. Wählen Sie Datei , Datendatei-Editor und Datensatzlayouts laden aus. 5. Wählen Sie im Dialogfel d Öffnen für Dateiname die Strukturdatei aus und wählen Sie dann Öffnen aus. 6. Um zu bestätigen, dass der Zeichensatzmodus auf EBCDIC festgelegt ist, bestätigen Sie, dass das Dropdown-Menü auf EBCDIC festgelegt ist. Sie können die Rohdaten im linken Bereich und die formatierten Daten im rechten Bereich sehen. 7. Wählen Sie verschied ene Datensätze aus, um sicherzustellen, dass alle	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Formate mit dem richtigen Layout gerendert werden.	

(Option B) Testen der Strukturdatei mithilfe von Data File Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie eine EBCDIC-Datendatei.	Vergewissern Sie sich, dass Sie Ihre Strukturdatei verwenden können, um eine EBCDIC-Testdatendatei korrekt anzuzeigen. 1. Wählen Sie das Menüsymbol Windows Start, suchen und wählen Sie Micro Focus Enterprise Developer und dann Datendatei-Tools aus. 2. Wählen Sie Datei , Öffnen, Datendatei aus. 3. Wählen Sie im Dialogfeld Datendatei öffnen auf der Registerkarte Lokal für Dateiname die Option Durchsuchen aus, um den Speicherort der EBCDIC-Teststdatei zu finden. 4. Wählen Sie für Strukturdatei (optional) Durchsuchen aus, um den Speicherort der Strukturdatei zu finden. 5. Geben Sie im Abschnitt Dateidetails die Details der	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei ein und bestätigen Sie, dass die Kodierung auf EBCDIC festgelegt ist. 6. Wählen Sie je nach Ihren Anforderungen entweder Freigegebenen Modus öffnen oder Exklusiv öffnen aus. 7. Vergewissern Sie sich, dass das Dropdown-Menü im Bereich Darstellung der Symbolleiste auf EBCDIC gesetzt ist. Die Rohdaten werden im linken Bereich und die formatierten Daten im rechten Bereich angezeigt. 8. Wählen Sie verschied ene Datensätze aus, um sicherzustellen, dass alle Formate mit dem richtigen Layout gerendert werden.	

Konvertierung von Testdatendateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Konvertierung einer EBCDIC-Datei.	1. Wählen Sie das Windows-Startmenü-Symbol, suchen und wählen Sie Micro Focus Enterprise Developer und dann Classic Data Tools aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Tools und dann Konvertieren aus. 3. Wählen Sie im Dialogfeld Datendateikonvertierung im Abschnitt Eingabedatei für Dateiname die Option Durchsuchen aus, um die EBCDIC-Eingabedatei zu finden und auszuwählen. Vergewissern Sie sich, dass der Zeichensatz auf EBCDIC gesetzt ist. 4. Aktivieren Sie im Abschnitt Zeichensatzkonvertierung die Kontrollkästchen Zeichensatz konvertieren und Datensätze enthalten Nicht-Textdatenelemente. Wählen Sie Layout für die Konvertierung auswählen und dann Durchsuchen aus, um die Strukturdatei zu finden und auszuwählen. 5. Geben Sie im Abschnitt Neue Datei für Dateiname den Pfad und Dateiname n der ASCII-Ausgabedatei ein, die Sie erstellen möchten. Standardmäßig hat das Konvertierungstool standardmäßig dasselbe Format wie die Eingabeda tei. Belassen Sie zum	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Testen die Optionen auf ihren Standardwerten. 6. Wählen Sie Konvertieren aus. 7. Führen Sie die Schritte im Abschnitt (Option A) Testen der Strukturdatei mit Classic Data File Tools oder (Option B) Testen der Strukturdatei mit Data File Tools aus, laden Sie jedoch die ASCII-Ausgabedatei anstelle der EBCDIC-Datei. 8. Laden Sie sowohl die EBCDIC- als auch die ASCII-Dateien in den Datendatei-Editor und vergleichen Sie dann die Dateien nebeneinander, um die Genauigkeit der Konvertierung zu überprüfen.	

Zugehörige Ressourcen

- Micro Focus (Micro-Focus-Dokumentation)
- Mainframe- und Legacy-Code (AWS-Blogbeiträge)
- AWS Prescriptive Guidance (AWS-Dokumentation)
- AWS-Dokumentation (AWS-Dokumentation)
- Allgemeine AWS-Referenz (AWS-Dokumentation)
- AWS-Glossar (AWS-Dokumentation)

Bereitstellen einer Umgebung für containerisierte Clari Age-Anwendungen mithilfe von Terraform

Erstellt von Richard Milner-Watts (AWS)

Code-Repository: Blue Age-Beispiel-ECS-Infrastruktur (Terraform)	Umgebung: Produktion	Quelle: Mainframe
Ziel: Container	R-Typ: Plattformwechsel	Workload: IBM; Alle anderen Workloads
Technologien: Mainframe; Container und Microservices	AWS-Services: Amazon ECS; AWS Step Functions; Amazon VPC; Amazon Aurora	

Übersicht

Durch die Migration älterer Mainframe-Workloads in moderne Cloud-Architekturen können die Kosten für die Wartung eines Mainframes eliminiert werden – Kosten, die nur mit zunehmendem Alter der Umgebung steigen. Die Migration von Aufträgen von einem Mainframe kann jedoch zu besonderen Herausforderungen führen. Interne Ressourcen sind möglicherweise nicht mit der Auftragslogik vertraut, und die hohe Leistung von Mainframes bei diesen speziellen Aufgaben kann im Vergleich zu normalen, generalisierten CPUs schwierig zu replizieren sein. Das Umschreiben dieser Aufträge kann ein großes Unterfangen sein und viel Aufwand erfordern.

Blue Age konvertiert ältere Mainframe-Workloads in modernen Java-Code, den Sie dann als Container ausführen können.

Dieses Muster bietet eine Serverless-Beispielarchitektur für die Ausführung einer containerisierten Anwendung, die mit dem Clari Age-Tool modernisiert wurde. Die enthaltenen HashiCorp Terraform-Dateien bauen eine sichere Architektur für die Orchestrierung von Clari Age-Containern auf und unterstützen sowohl Batch-Aufgaben als auch Echtzeit-Services.

Weitere Informationen zur Modernisierung Ihrer Workloads mithilfe der Services Clari Age und AWS finden Sie in diesen Veröffentlichungen zu AWS Prescriptive Guidance:

- Ausführen von Mainframe-Workloads, die mit Clari Age auf der serverlosen AWS-Infrastruktur modernisiert wurden
- Containerisieren Sie Mainframe-Workloads, die von Clari Age modernisiert wurden

Wenn Sie Hilfe bei der Verwendung von Clari Age zur Modernisierung Ihrer Mainframe-Workloads benötigen, wenden Sie sich an das Clari Age-Team, indem Sie auf der Clari Age-Website die Option Kontaktieren Sie unsere Experten auswählen. https://www.bluage.com/ Um Unterstützung bei der Migration Ihrer modernisierten Workloads zu AWS, deren Integration in AWS-Services und deren Umstellung in die Produktion zu erhalten, wenden Sie sich an Ihren AWS-Kundenbetreuer oder füllen Sie das AWS Professional Services-Formular aus.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Die containerisierte Clari Age-Beispielanwendung, die von den Containerize-Mainframe-Workloads bereitgestellt wird, die durch das Clari Age-Muster modernisiert wurden. Die Beispielanwendung bietet die Logik, um die Verarbeitung von Eingabe und Ausgabe für die modernisierte Anwendung zu bewältigen, und kann in diese Architektur integriert werden.
- Terraform ist erforderlich, um diese Ressourcen bereitzustellen.

Einschränkungen

- Amazon Elastic Container Service (Amazon ECS) legt Beschränkungen für die Aufgabenressourcen fest, die dem Container zur Verfügung gestellt werden können. Zu diesen Ressourcen gehören CPU, RAM und Speicher. Wenn Sie beispielsweise Amazon ECS mit AWS Fargate verwenden, gelten die Limits für Aufgabenressourcen .

Produktversionen

Diese Lösung wurde mit den folgenden Versionen getestet:

- Terraform 1.3.6
- Terraform-AWS-Anbieter 4.46.0

Architektur

Quelltechnologie-Stack

- Blaues Alter
- Terraform

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-Compatible Edition
- AWS Backup
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- AWS Identity and Access Management Service (IAM)
- AWS Key Management Server (AWS KMS)
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager

Zielarchitektur

Das folgende Diagramm zeigt die Lösungsarchitektur.

1. Die Lösung stellt die folgenden IAM-Rollen bereit:
   - Batch-Aufgabenrolle
   - Batch-Aufgabenausführungsrolle
   - Serviceaufgabenrolle
   - Ausführungsrolle für Serviceaufgaben
   - Step Functions-Rolle
   - AWS Backup-Rolle

- RDS Enhanced Monitoring-Rolle.

Die Rollen entsprechen den Zugriffsprinzipien mit den geringsten Berechtigungen.

2. Amazon ECR wird verwendet, um das Container-Image zu speichern, das durch dieses Muster orchestriert wird.
3. AWS Systems Manager Parameter Store stellt der Amazon ECS-Aufgabendefinition zur Laufzeit Konfigurationsdaten zu jeder Umgebung bereit.
4. AWS Secrets Manager stellt vertrauliche Konfigurationsdaten über die Umgebung zur Laufzeit für die Amazon ECS-Aufgabendefinition bereit. Die Daten wurden mit AWS KMS verschlüsselt.
5. Die Terraform-Module erstellen Amazon-ECS-Aufgabendefinitionen für alle Echtzeit- und Batch-Aufgaben.
6. Amazon ECS führt eine Batch-Aufgabe aus, indem AWS Fargate als Rechen-Engine verwendet wird. Dies ist eine kurzlebige Aufgabe, die gemäß den Anforderungen von AWS Step Functions initiiert wird.
7. Amazon Aurora PostgreSQL – kompatibel bietet eine Datenbank zur Unterstützung der modernisierten Anwendung. Dadurch werden Mainframe-Datenbanken wie IBM Db2 oder IBM IMS DB ersetzt.
8. Amazon ECS führt einen langlebigen Service aus, um einen modernisierten Echtzeit-Workload bereitzustellen. Diese zustandslosen Anwendungen werden dauerhaft mit Containern ausgeführt, die über Availability Zones verteilt sind.
9. Ein Network Load Balancer wird verwendet, um Zugriff auf die Echtzeit-Workload zu gewähren. Der Network Load Balancer unterstützt frühere Protokolle wie IBM CICS. Alternativ können Sie einen Application Load Balancer mit HTTP-basierten Workloads verwenden.
10. Amazon S3 bietet Objektspeicher für Auftragseingaben und -ausgaben. Der Container sollte Pull- und Push-Operationen in Amazon S3 verarbeiten, um das Arbeitsverzeichnis für die Clari Age-Anwendung vorzubereiten.
11. Der AWS Step Functions-Service wird verwendet, um die Ausführung der Amazon ECS-Aufgaben zur Verarbeitung von Batch-Workloads zu orchestrieren.
12. SNS-Themen für jeden Batch-Workload werden verwendet, um die modernisierte Anwendung in andere Systeme wie E-Mail zu integrieren oder zusätzliche Aktionen zu initiieren, z. B. die Bereitstellung von Ausgabeobjekten von Amazon S3 an FTP.

Hinweis: Standardmäßig hat die Lösung keinen Zugriff auf das Internet. Bei diesem Muster wird davon ausgegangen, dass die Virtual Private Cloud (VPC) über einen Service wie AWS Transit

Gateway mit anderen Netzwerken verbunden wird. Daher werden mehrere Schnittstellen-VPC-Endpunkte bereitgestellt, um Zugriff auf die von der Lösung verwendeten AWS-Services zu gewähren. Um den direkten Internetzugang zu aktivieren, können Sie den Schalter im Terraform-Modul verwenden, um die VPC-Endpunkte durch ein Internet-Gateway und die zugehörigen Ressourcen zu ersetzen.

Automatisierung und Skalierung

Die Verwendung von Serverless-Ressourcen während dieses Musters trägt dazu bei, dass durch die horizontale Skalierung dieses Designs nur wenige Beschränkungen für den Umfang dieses Designs gelten. Dadurch werden die Bedenken des verrauschten Nachbarn reduziert, z. B. der Wettbewerb um Rechenressourcen, die auf dem ursprünglichen Mainframe auftreten könnten. Batch-Aufgaben können so geplant werden, dass sie nach Bedarf gleichzeitig ausgeführt werden.

Einzelne Container sind durch die von Fargate maximal unterstützten Größen begrenzt. Weitere Informationen finden Sie im Abschnitt Aufgaben-CPU und Arbeitsspeicher in der Amazon-ECS-Dokumentation.

Um Echtzeit-Workloads horizontal zu skalieren, können Sie Container hinzufügen.

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- AWS Backup ist ein vollständig verwalteter Service, der Sie bei der Zentralisierung und Automatisierung des Datenschutzes über AWS-Services, in der Cloud und On-Premises unterstützt.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.

- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- AWS Systems Manager Parameter Store bietet eine sichere, hierarchische Speicherung für die Verwaltung von Konfigurationsdaten und Secrets.

Andere -Services

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit dem Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können. Dieses Muster verwendet Terraform, um die Beispielarchitektur zu erstellen.

Code-Repository

Der Quellcode für dieses Muster ist im GitHub ECS-Infrastruktur-Repository des Typs Clari Age (Terraform) verfügbar.

Bewährte Methoden

- Verwenden Sie für Testumgebungen Funktionen wie die `forceDate` Option , um die modernisierte Anwendung so zu konfigurieren, dass konsistente Testergebnisse generiert werden, indem sie immer für einen bekannten Zeitraum ausgeführt wird.
- Optimieren Sie jede Aufgabe einzeln, um die optimale Menge an Ressourcen zu verbrauchen. Sie können Amazon CloudWatch Container Insights verwenden, um Anleitungen zu potenziellen Engpässen zu erhalten.

Polen

Vorbereiten der Umgebung für die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie den Lösungsquellcode.	Klonen Sie den Lösungscode aus dem GitHub Projekt .	DevOps Techniker
Bootstrappen Sie die Umgebung, indem Sie Ressourcen zum Speichern des Terraform-Status bereitstellen.	1. Öffnen Sie ein Terminalfenster und bestätigen Sie, dass Terraform installiert ist und dass AWS-Anmeldeinformationen verfügbar sind. 2. Navigieren Sie zum Verzeichnis `bootstrap-terraform` . 3. Bearbeiten Sie die Datei`main.tf`, wenn Sie die Namen des S3-Buckets (`<accountId>-terraform-backend`) und der Amazon-DynamoDB-Tabelle () ändern möchten`terraform-lock`. 4. Führen Sie den `terraform apply` Befehl aus, um die Ressourcen bereitzustellen. Notieren Sie sich die Namen des S3-Buckets und der DynamoDB-Tabelle.	DevOps Techniker

Bereitstellen der Lösungsinfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und aktualisieren Sie die Terraform-Konfigur ation.	Öffnen Sie im Stammverz eichnis die Datei und `main.tf`, überprüfen Sie den Inhalt. Erwägen Sie, die folgenden Aktualisierungen vorzunehmen: 1. Aktualisieren Sie die AWS-Region, indem Sie nach der Zeichenfolge suchen und sie durch die `eu-west-1` gewünschte Region ersetzen, die Sie verwenden möchten. 2. Aktualisieren Sie den Bucket-Namen im `-Terraform Backend` Block, wenn der Standardw ert im vorherigen Epi geändert wurde. 3. Aktualisieren Sie den `dynamodb_table` Wert, wenn der Standardwert im vorherigen Epi geändert wurde. 4. Aktualisieren Sie den Wert der `stack_pre fix` Variablen auf die gewünschte Zeichenfolge. Diese Zeichenfolge wird den Namen aller Ressource n vorangestellt, die durch	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieses Muster erstellt wurden. 5. Aktualisieren Sie den Wert von `vpc_cidr` Dies sollte mindestens ein `/24` Adressbereich sein. 6. Überprüfen Sie den `Locals` Abschnitt . Dies wird verwendet, um die Blue Age-Aufgaben zu definieren, die bereitgestellt werden. Die Lösung iteriert über das Listenobjekt und `bluage_batch_modules` erstellt die zugehörigen Ressourcen (Zustandsautomat von Step Functions, Aufgabendefinition und SNS-Thema) für jedes Element der Liste. In einigen Fällen möchten Sie möglicherweise Variablen für verschiedene Umgebungen anpassen. Um beispielsweise die Laufzeit in Testumgebungen zu erzwingen, können Sie den Wert der `force_execution_time` Variable ändern. 7. Um den Internetzugang zu aktivieren, ändern Sie den Wert für `direct_internet_access_requ`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ired` von `false` in `true`. Dadurch wird ein Internet-Gateway zusammen mit den NAT-Gateways und Routing-Tabellen bereitgestellt, die den öffentlichen Internetzugang für die Infrastruktur aktivieren. Standardmäßig stellt die Lösung Schnittstellen-VPC-Endpunkte in einer VPC ohne direkten Internetzugang bereit. 8. Um Zugriff auf alle Client-Server-Workloads zu gewähren, die über Elastic Load Balancing bereitgestellt werden, aktualisieren Sie die Werte von `additional_nlb_ingress_cidrs` mit den CIDR-Netzwerken, die zugelassen werden sollen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Terraform-Datei bereit.	Führen Sie in Ihrem Terminal den `terraform apply` Befehl aus, um alle Ressourcen bereitzustellen. Überprüfen Sie die von Terraform generierten Änderungen und geben Sie Ja ein, um den Build zu initiieren. Beachten Sie, dass es mehr als 15 Minuten dauern kann, diese Infrastruktur bereitzustellen.	DevOps Techniker

(Optional) Stellen Sie eine gültige containerisierte Blue Age-Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschieben Sie das Clari Age-Container-Image zu Amazon ECR.	Verschieben Sie den Container in das Amazon-ECR-Repository, das Sie im vorherigen Epos erstellt haben. Anweisungen finden Sie in der Amazon-ECR-Dokumentation. Notieren Sie sich den Container-Image-URI.	DevOps Techniker
Aktualisieren Sie Terraform , um auf das microSD Age-Container-Image zu verweisen .	Aktualisieren Sie die Datei`main.tf` , um auf das Container-Image zu verweisen , das Sie hochgeladen haben.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Terraform-Datei erneut bereit.	Führen Sie von Ihrem Terminal aus, `terraform apply` um alle Ressourcen bereitzustellen. Überprüfen Sie die vorgeschlagenen Aktualisierungen von Terraform und geben Sie dann Ja ein, um mit der Bereitstellung fortzufahren.	DevOps Techniker

Zugehörige Ressourcen

- Blaues Alter
- Ausführen von Mainframe-Workloads, die mit Clari Age auf der serverlosen AWS-Infrastruktur modernisiert wurden
- Containerisieren Sie Mainframe-Workloads, die von Clari Age modernisiert wurden

Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight

Umgebung: PoC oder Pilotprojekt	Technologien: Mainframe; Analytik; Migration; Modernisierung; Maschinelles Lernen und KI	Arbeitslast: IBM
AWS-Services: AWS Lambda; AWS-Mainframe-Modernisierung; Amazon QuickSight; Amazon S3		

Übersicht

Wenn Ihr Unternehmen geschäftskritische Daten in einer Mainframe-Umgebung hostet, ist es entscheidend, Erkenntnisse aus diesen Daten zu gewinnen, um Wachstum und Innovation voranzutreiben. Durch die Erschließung von Mainframe-Daten können Sie schnellere, sichere und skalierbare Business Intelligence aufbauen, um datengestützte Entscheidungen, Wachstum und Innovation in der Amazon Web Services ()AWS Cloud zu beschleunigen.

Dieses Muster bietet eine Lösung für die Generierung von Geschäftseinblicken und die Erstellung gemeinsam nutzbarer Geschichten aus Mainframe-Daten mithilfe von AWS Mainframe Modernization File Transfer mit BMC und Amazon Q in. QuickSight Mainframe-Datensätze werden mithilfe von AWS Mainframe Modernization File Transfer mit BMC an Amazon Simple Storage Service (Amazon S3) übertragen. Eine AWS Lambda Funktion formatiert die Mainframe-Datendatei und bereitet sie für das Laden in Amazon QuickSight vor.

Sobald die Daten in Amazon verfügbar sind QuickSight, können Sie natürliche Sprachaufforderungen mit Amazon Q verwenden, QuickSight um Zusammenfassungen der Daten zu erstellen, Fragen zu stellen und Datenstorys zu generieren. Sie müssen keine SQL-Abfragen schreiben oder ein Business Intelligence (BI) -Tool erlernen.

Geschäftlicher Kontext

Dieses Muster stellt eine Lösung für Anwendungsfälle von Mainframe-Datenanalysen und Datenerkenntnissen dar. Mithilfe des Musters erstellen Sie ein visuelles Dashboard für die Daten Ihres Unternehmens. Um die Lösung zu demonstrieren, verwendet dieses Muster ein Gesundheitsunternehmen, das seinen Mitgliedern in den USA medizinische, zahnärztliche und augenärztliche Pläne anbietet. In diesem Beispiel werden demografische Daten und Versicherungsinformationen der Mitglieder in den Mainframe-Datensätzen gespeichert. Das visuelle Dashboard zeigt Folgendes:

- Verteilung der Mitglieder nach Regionen
- Verteilung der Mitglieder nach Geschlecht
- Verteilung der Mitglieder nach Alter
- Verteilung der Mitglieder nach Tariftyp
- Mitglieder, die die Schutzimpfung noch nicht abgeschlossen haben

Nachdem Sie das Dashboard erstellt haben, generieren Sie eine Datenstory, die die Erkenntnisse aus der vorherigen Analyse erklärt. Die Datenstory enthält Empfehlungen zur Erhöhung der Zahl der Mitglieder, die präventive Impfungen abgeschlossen haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Mainframe-Datensätze mit Geschäftsdaten
- Zugriff auf die Installation eines File Transfer Agents auf dem Mainframe

Einschränkungen

- Ihre Mainframe-Datendatei sollte in einem der von Amazon QuickSight unterstützten Dateiformate vorliegen. Eine Liste der unterstützten Dateiformate finden Sie in der QuickSight Amazon-Dokumentation.

  Dieses Muster verwendet eine Lambda-Funktion, um die Mainframe-Datei in ein von Amazon unterstütztes Format zu konvertieren. QuickSight

Architektur

Das folgende Diagramm zeigt eine Architektur zur Generierung von Geschäftseinblicken aus Mainframe-Daten mithilfe von AWS Mainframe Modernization File Transfer mit BMC und Amazon Q in. QuickSight

Das Diagramm zeigt den folgenden Workflow:

1. Ein Mainframe-Datensatz mit Geschäftsdaten wird mithilfe von AWS Mainframe Modernization File Transfer with BMC an Amazon S3 übertragen.
2. Die Lambda-Funktion konvertiert die Datei, die sich im S3-Bucket des Ziels für die Dateiübertragung befindet, in das CSV-Format (Comma-Separated Values).
3. Die Lambda-Funktion sendet die konvertierte Datei an den S3-Bucket des Quelldatensatzes.
4. Die Daten in der Datei werden von Amazon QuickSight aufgenommen.
5. Benutzer greifen auf die Daten in Amazon zu QuickSight. Sie können Amazon Q in verwenden, um mit den Daten QuickSight zu interagieren, indem Sie Eingabeaufforderungen in natürlicher Sprache verwenden.

Tools

AWS-Services

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Mainframe Modernization File Transfer with BMC konvertiert Mainframe-Datensätze und überträgt sie an Amazon S3 für Anwendungsfälle zur Mainframe-Modernisierung, -Migration und Erweiterung.
- Amazon QuickSight ist ein BI-Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können. Dieses Muster verwendet die generativen BI-Funktionen von Amazon Q in QuickSight.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

- Wenn Sie die AWS Identity and Access Management (IAM-) Rollen für AWS Mainframe Modernization File Transfer mit BMC und der Lambda-Funktion erstellen, folgen Sie dem Prinzip der geringsten Rechte.
- Stellen Sie sicher, dass Ihr Quelldatensatz Datentypen für Amazon unterstützt QuickSight. Wenn Ihr Quelldatensatz Datentypen enthält, die nicht unterstützt werden, konvertieren Sie diese in unterstützte Datentypen. Informationen zu nicht unterstützten Mainframe-Datentypen und deren Konvertierung in von Amazon Q unterstützte Datentypen finden Sie im QuickSight Abschnitt Verwandte Ressourcen.

Epen

Richten Sie die AWS Mainframe Modernization Dateiübertragung mit BMC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den File Transfer Agent.	Folgen Sie den Anweisungen in der AWS Dokumentation, um AWS Mainframe Modernization File Transfer Agent auf Ihrem Mainframe zu installieren.	Mainframe-Systemadministrator
Erstellen Sie einen S3-Bucket für die Mainframe-Dateiübertragung.	Erstellen Sie einen S3-Bucket, um die Ausgabedatei von AWS Mainframe Modernization File Transfer with BMC zu speichern. Im Architekturdiagramm ist dies der Ziel-Bucket für die Dateiübertragung.	Ingenieur für Migration
Erstellen Sie den Endpunkt für die Datenübertragung.	1. Erstellen Sie einen S3-Bucket, um die Mainframe-Eingabedatei für die AWS Mainframe Modernization	Spezialist AWS AWS-Mainframe-Modernisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dateiübertragung mit BMC bereitzustellen. 2. Folgen Sie den Anweisungen in der Dokumentation, um den Mainframe-Datenübertragungsendpunkt zu erstellen.AWS	

Konvertiert die Mainframe-Dateinamenerweiterung für die Amazon-Integration QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für die Lambda-Funktion, um die konvertierte Mainframe-Datei von der Quelle in den endgültigen Ziel-Bucket zu kopieren.	Ingenieur für Migration
Erstellen Sie eine Lambda-Funktion.	Gehen Sie wie folgt vor, um eine Lambda-Funktion zu erstellen, die die Dateierweiterung ändert und die Mainframe-Datei in den Ziel-Bucket kopiert: 1. Melden Sie sich bei der AWS Management Console an und navigieren Sie zur AWS Lambda Konsole. 2. Wählen Sie „Funktion erstellen“ und anschließend „Von Grund auf neu erstellen“.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Geben Sie unter Funktionsname einen Namen für Ihre Funktion ein. 4. Wählen Sie in der Runtime-Dropdown-Liste Python.3.X aus. 5. Erweitern Sie Standardausführungsrolle ändern und wählen Sie dann Neue Rolle mit grundlegenden Lambda-Berechtigungen erstellen aus. 6. Wählen Sie Funktion erstellen. 7. Wählen Sie die Registerkarte Code und fügen Sie dann den `S3CopyLambda.py` Python-Code ein, der im Abschnitt Zusätzliche Informationen bereitgestellt wird. Der Python-Code wurde mithilfe von Amazon Q Developer in der integrierten Entwicklungsumgebung (IDE) von Microsoft Visual Studio generiert. 8. Bearbeiten Sie den `destination_bucket_name` auf den Namen des S3-Buckets, den Sie zuvor erstellt haben, und `change destination_file_key` auf den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen der Mainframe-Datei. 9. Stellen Sie die Lambda-Funktion bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon S3 S3-Trigger, um die Lambda-Funktion aufzurufen.	Gehen Sie wie folgt vor, um einen Trigger zu konfiguri eren, der die Lambda-Funktion aufruft: 1. Öffnen Sie in der Lambda-Konsole die Seite Funktione n. 2. Wählen Sie die Lambda-Fu nktion. 3. Wählen Sie in der Funktions übersicht die Option Trigger hinzufügen aus. 4. Wählen Sie in der Dropdownliste Trigger-K onfiguration die Option S3 aus. 5. Geben Sie im Feld Bucket den Namen Ihres Quell-Buc kets ein. 6. Wählen Sie in der Dropdownliste Ereignistyp die Option Alle Ereignisse zur Objekterstellung aus. 7. Aktivieren Sie das Kontrollk ästchen Ich bestätige, dass die Verwendung desselben S3-Buckets für Eingabe und Ausgabe nicht empfohlen wird, und wählen Sie dann Hinzufügen aus.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Tutorial: Verwenden eines Amazon S3-Auslösers zum Aufrufen einer Lambda-Funktion.	
Stellen Sie IAM-Berechtigungen für die Lambda-Funktion bereit.	Für den Zugriff der Lambda-Funktion auf die S3-Buckets des Dateiübertragungsziels und des Quelldatensatzes sind IAM-Berechtigungen erforderlich. Aktualisieren Sie die Richtlinie, die mit der Lambda-Funktionsausführungsrolle verknüpft ist, indem Sie den Ziel-S3-Bucket für die Dateiübertragung `s3:GetObject` und `s3:DeleteObject` den `s3:PutObject` Zugriff auf den S3-Bucket des Quelldatensatzes zulassen und gewähren. Weitere Informationen finden Sie im Abschnitt Erstellen einer Berechtigungsrichtlinie in Tutorial: Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion.	Leiter der Migration

Definieren Sie eine Mainframe-Datenübertragungsaufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Übertragungsaufgabe, um die Mainframe-Datei in den S3-Bucket zu kopieren.	Folgen Sie den Anweisungen in der Dokumentation, um eine Mainframe-Dateiübertragungsaufgabe zu erstellen.AWS Mainframe Modernization Hinweis: Geben Sie die Quellcodepage-Kodierung als IBM1047 und die Ziel-Codepage-Kodierung als UTF-8 an.	Ingenieur für Migration
Überprüfen Sie die Übertragungsaufgabe.	Folgen Sie den Anweisungen in der AWS Mainframe Modernization Dokumentation, um zu überprüfen, ob die Datenübertragung erfolgreich war. Vergewissern Sie sich, dass sich die Mainframe-Datei im Ziel-S3-Bucket für die Dateiübertragung befindet.	Leiter der Migration
Überprüfen Sie die Lambda-Kopierfunktion.	Stellen Sie sicher, dass die Lambda-Funktion initiiert wurde und dass die Datei mit der Erweiterung.csv in den S3-Bucket des Quelldatensatzes kopiert wurde. Die mit der Lambda-Funktion erstellte .csv-Datei ist die Eingabedatendatei für Amazon. QuickSight Beispieldaten finden Sie in der `Sample-data-member-`	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`healthcare-APG` Datei im Abschnitt Anlagen.	

Amazon mit QuickSight den Mainframe-Daten verbinden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon ein QuickSight.	Folgen Sie den Anweisungen in der AWS Dokumentation QuickSight, um Amazon einzurichten.	Leiter der Migration
Erstellen Sie einen Datensatz für Amazon QuickSight.	Folgen Sie den Anweisungen in der AWS Dokumentation QuickSight, um einen Datensatz für Amazon zu erstellen. Die Eingabedatendatei ist die konvertierte Mainframe-Datei, die bei der Definition der Mainframe-Datenübertragungsaufgabe erstellt wurde.	Leiter der Migration

Gewinnen Sie Geschäftseinblicke aus den Mainframe-Daten mithilfe von Amazon Q in QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon Q in ein QuickSight.	Für diese Funktion ist die Enterprise Edition erforderlich. Gehen Sie wie folgt vor QuickSight, um Amazon Q in einzurichten:	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Um das Amazon Q-Add-on zu erhalten, folgen Sie den Anweisungen Schritt 1: Holen Sie sich das Q-Add-on in der AWS Dokumentation. 2. Um die generativen BI-Funktionen in Amazon Q zu nutzen, aktualisieren Sie die Konten Ihrer Benutzer. Folgen Sie den Anweisungen in der AWS Dokumentation. 3. Erstellen Sie ein Amazon Q-Thema, indem Sie den Datensatz verwenden, den Sie zuvor erstellt haben. Folgen Sie den Anweisungen in der AWS Dokumentation. 4. Folgen Sie den Anweisungen in der Dokumentation, um die Metadaten des Themas so zu konfigurieren, dass sie für natürliche Sprachen geeignet sind.AWS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Mainframe-Daten und erstellen Sie ein visuelles Dashboard.	Gehen Sie wie folgt vor QuickSight, um Ihre Daten in Amazon zu analysieren und zu visualisieren: 1. Folgen Sie den Anweisungen in der AWS Dokumentation, um die Mainframe-Datenanalyse zu erstellen. Wählen Sie für den Datensatz den Datensatz aus, der im vorherigen Schritt erstellt wurde. 2. Wählen Sie auf der Analyseseite Visual erstellen aus. 3. Wählen Sie im Fenster „Thema für Analyse erstellen“ die Option Bestehendes Thema aktualisieren aus. 4. Wählen Sie in der Dropdownliste Thema auswählen das Thema aus, das Sie zuvor erstellt haben. 5. Wählen Sie Themenverknüpfung aus. 6. Nachdem Sie das Thema verknüpft haben, wählen Sie Visual erstellen, um das Amazon Q-Fenster Build a Visual zu öffnen.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Schreiben Sie in der Eingabeaufforderungsleiste Ihre Analysefragen. Die für dieses Muster verwendeten Beispielfragen sind die folgenden: • Verteilung der Mitglieder nach Regionen anzeigen • Verteilung der Mitglieder nach Alter anzeigen • Zeigt die Verteilung der Mitglieder nach Geschlecht • Verteilung der Mitglieder nach Tariftyp anzeigen • Zeigt das Mitglied an, das die präventive Impfung nicht abgeschlossen hat Nachdem Sie Ihre Fragen eingegeben haben, wählen Sie Build. Amazon Q in QuickSight erstellt das Bildmaterial. 8. Um die Grafiken zu Ihrem visuellen Dashboard hinzuzufügen, wählen Sie ZUR ANALYSE HINZUFÜGEN. Wenn Sie fertig sind, können Sie Ihr Dashboard veröffentlichen, um es mit anderen in Ihrer Organisation zu teilen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispiele finden Sie unter Visuelles Mainframe-Dashboard im Abschnitt Zusätzliche Informationen.	

Erstellen Sie eine Datenstory mit Amazon Q in QuickSight aus den Mainframe-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenstory.	Erstellen Sie eine Datenstory, um die Erkenntnisse aus der vorherigen Analyse zu erläutern, und geben Sie eine Empfehlung zur Erhöhung der präventiven Impfungen für Mitglieder ab: 1. Folgen Sie den Anweisungen in der AWS Dokumentation, um die Data Story zu erstellen. 2. Verwenden Sie für den Data Story-Prompt Folgendes: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`complete immunization. Include 4 points of supporting data for this pattern.` Sie können auch Ihre eigene Aufforderung erstellen, um Datenstorys für andere Geschäftseinblicke zu generieren. 3. Wählen Sie Visuals hinzufügen aus und fügen Sie die Grafiken hinzu, die für die Data Story relevant sind. Verwenden Sie für dieses Muster die Grafiken, die Sie zuvor erstellt haben. 4. Wählen Sie Build aus. 5. Ein Beispiel für die Ausgabe von Data Storys finden Sie unter Data Story-Ausgabe im Abschnitt Zusätzliche Informationen.	
Sehen Sie sich die generierte Datenstory an.	Folgen Sie den Anweisungen in der AWS Dokumentation, um die generierte Datenstory anzusehen.	Leitung der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie eine generierte Datenstory.	Folgen Sie den Anweisungen in der AWS Dokumentation, um die Formatierung, das Layout oder die visuelle Darstellung in einer Data Story zu ändern.	Leiter der Migration
Teilen Sie eine Datenstory.	Folgen Sie den Anweisungen in der AWS Dokumentation, um eine Data Story mit anderen zu teilen.	Ingenieur für Migration

Fehlerbehebung

Problem	Lösung
Die Mainframe-Dateien oder Datensätze, die in die Suchkriterien für Datensätze für die Aufgabe Übertragung erstellen in AWS Mainframe Modernization File Transfer with BMC eingegeben wurden, konnten nicht gefunden werden.	1. Überprüfen Sie zunächst die Verbindung, indem Sie in der Konsole „Übertragung mit BMC“ die Option AWS Mainframe Modernization Datenübertragungsendpunkte auswählen. Wenn die letzte Heartbeat-Zeit länger als zwei Minuten ist, wurde die Verbindung für die Dateiübertragung nicht hergestellt. Wenn die letzte Heartbeat-Zeit für den auf dem Mainframe ausgeführten Agenten weniger als 2 Minuten beträgt, ist die Verbindung zum Agenten erfolgreich. Fahren Sie mit Schritt 2 fort. 2. Überprüfen Sie das AWS Secrets Manager Setup. Ein geheimer Schlüssel muss in Secrets Manager mit einem Schlüssel von `userId` (Großbuchstabe I) mit dem Wert der Benutzer-ID des Mainframes und einem Schlüssel `password` mit dem Wert

Problem	Lösung
	des Mainframe-Kennworts konfiguriert werden. Bei den `userId` und `password` geheimen Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen unverändert eingegeben werden.

Zugehörige Ressourcen

Um Mainframe-Datentypen wie PACKED-DECIMAL (COMP-3) oder BINARY (COMP oder COMP-4) in einen von Amazon QuickSight unterstützten Datentyp zu konvertieren, sehen Sie sich die folgenden Muster an:

- EBCDIC-Daten mithilfe von Python in ASCII umwandeln und entpacken AWS
- Konvertieren Sie Mainframe-Dateien vom EBCDIC-Format in das durch Zeichen getrennte ASCII-Format in Amazon S3 mit AWS Lambda

Zusätzliche Informationen

S3 .py CopyLambda

Der folgende Python-Code wurde mithilfe einer Aufforderung mit Amazon Q Developer in einer IDE generiert:

```
#Create a lambda function triggered by S3. display the S3 bucket name and key
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
print(bucket, key)
#If key starts with object_created, skip copy, print "copy skipped". Return lambda with
 key value.
if key.startswith('object_created'):
print("copy skipped")
return {
'statusCode': 200,
```

```
'body': key
}
# Copy the file from the source bucket to the destination bucket.
 Destination_bucket_name = 'm2-filetransfer-final-opt-bkt'. Destination_file_key =
 'healthdata.csv'
copy_source = {'Bucket': bucket, 'Key': key}
s3.copy_object(Bucket='m2-filetransfer-final-opt-bkt', Key='healthdata.csv',
 CopySource=copy_source)
print("file copied")
#Delete the file from the source bucket.
s3.delete_object(Bucket=bucket, Key=key)
return {
'statusCode': 200,
'body': 'Copy Successful'
}
```

Visuelles Mainframe-Dashboard

Das folgende Datenbild wurde von Amazon Q QuickSight für die Analysefrage erstellt `show member distribution by region`.

Das folgende Datenbild wurde von Amazon Q QuickSight für die Frage erstellt`show member distribution by Region who have not completed preventive immunization, in pie chart`.

Ausgabe von Data Story

Die folgenden Screenshots zeigen Abschnitte der Datenstory, die von Amazon Q QuickSight für die Aufforderung erstellt wurden. `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data.`

In der Einleitung wird in der Datenstory empfohlen, die Region mit den meisten Mitgliedern auszuwählen, um die größtmögliche Wirkung der Impfmaßnahmen zu erzielen.

Die Datenstory enthält eine Analyse der Mitgliederzahlen für die drei wichtigsten Regionen und nennt den Südwesten als die Region, in der der Schwerpunkt auf Impfmaßnahmen liegt.

Hinweis: Die Regionen Südwesten und Nordosten haben jeweils acht Mitglieder. Im Südwesten gibt es jedoch mehr Mitglieder, die nicht vollständig geimpft sind, sodass er mehr Potenzial hat, von Initiativen zur Erhöhung der Impfraten zu profitieren.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Integrieren Sie Stonebranch Universal Controller in AWS Mainframe Modernization

Quellcode-Repository: aws-mainframe-modernization-stonebranch-integration	Umgebung: PoC oder Pilotprojekt	Technologien: Mainframe ; Modernisierung DevOps; Betrieb; SaaS
Arbeitslast: Open Source; Microsoft	AWS-Services: AWS-Mainframe-Modernisierung; Amazon RDS; Amazon S3	

Übersicht

Dieses Muster erklärt, wie die Workload-Orchestrierung des Stonebranch Universal Automation Center (UAC) in den Mainframe-Modernisierungsservice von Amazon Web Services (AWS) integriert wird. Der AWS Mainframe Modernization Service migriert und modernisiert Mainframe-Anwendungen in die AWS-Cloud. Es bietet zwei Muster: AWS Mainframe Modernization Replatform mit Micro Focus Enterprise Technology und AWS Mainframe Modernization Automated Refactor mit AWS Blu Age.

Stonebranch UAC ist eine Echtzeit-IT-Automatisierungs- und Orchestrierungsplattform. UAC wurde entwickelt, um Jobs, Aktivitäten und Workflows in hybriden IT-Systemen zu automatisieren und zu orchestrieren, von On-Premise bis hin zu AWS. Unternehmenskunden, die Mainframe-Systeme verwenden, stellen auf Cloud-zentrierte, modernisierte Infrastrukturen und Anwendungen um. Die Tools und professionellen Services von Stonebranch erleichtern die Migration vorhandener Scheduler und Automatisierungsfunktionen in die AWS-Cloud.

Wenn Sie Ihre Mainframe-Programme mithilfe des AWS Mainframe Modernization Service in die AWS-Cloud migrieren oder modernisieren, können Sie diese Integration nutzen, um die Batch-Planung zu automatisieren, die Agilität zu erhöhen, die Wartung zu verbessern und die Kosten zu senken.

Dieses Muster enthält Anweisungen für die Integration von Stonebranch Scheduler in Mainframe-Anwendungen, die zur Laufzeit des AWS Mainframe Modernization Service Micro Focus Enterprise migriert wurden. Dieses Muster richtet sich an Lösungsarchitekten, Entwickler, Berater, Migrationsspezialisten und andere Personen, die in den Bereichen Migrationen, Modernisierungen, Betrieb oder tätig sind. DevOps

Angestrebtes Ergebnis

Dieses Muster konzentriert sich auf die Erzielung der folgenden Zielergebnisse:

- Die Möglichkeit, Mainframe-Batch-Jobs, die im AWS Mainframe Modernization Service (Microfocus Runtime) ausgeführt werden, von Stonebranch Universal Controller aus zu planen, zu automatisieren und auszuführen.
- Überwachen Sie die Batch-Prozesse der Anwendung vom Stonebranch Universal Controller aus.
- Batch-Prozesse automatisch oder manuell vom Stonebranch Universal Controller aus starten/neustarten/erneut ausführen/stoppen.
- Rufen Sie die Ergebnisse der Batch-Prozesse für die AWS Mainframe-Modernisierung ab.
- Erfassen Sie die CloudWatchAWS-Protokolle der Batch-Jobs in Stonebranch Universal Controller.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Micro Focus Bank-Demo-Anwendung mit Job Control Language (JCL) -Dateien und einem Batch-Prozess, der in einer AWS Mainframe Modernization Service-Umgebung (Micro Focus Runtime) bereitgestellt wird
- Grundkenntnisse zum Erstellen und Bereitstellen einer Mainframe-Anwendung, die auf Micro Focus Enterprise Server läuft
- Grundkenntnisse über Stonebranch Universal Controller
- Stonebranch-Testlizenz (wenden Sie sich an Stonebranch)
- Windows- oder Linux-Instances von Amazon Elastic Compute Cloud (Amazon EC2) (z. B. xlarge) mit mindestens vier Kernen, 8 GB Arbeitsspeicher und 2 GB Festplattenspeicher
- Apache Tomcat Version 8.5.x oder 9.0.x
- Oracle Java Runtime Environment (JRE) oder OpenJDK Version 8 oder 11
- Amazon Aurora MySQL-kompatible Edition
- Amazon Simple Storage Service (Amazon S3) -Bucket für das Export-Repository
- Amazon Elastic File System (Amazon EFS) für Agenten Stonebranch Universal Message Service (OMS) -Verbindungen für Hochverfügbarkeit (HA)

- Installationsdateien für Stonebranch Universal Controller 7.2 Universal Agent 7.2
- Vorlage für die Aufgabenplanung von AWS Mainframe Modernization (neueste veröffentlichte Version der ZIP-Datei)

Einschränkungen

- Das Produkt und die Lösung wurden nur mit OpenJDK 8 und 11 getestet und ihre Kompatibilität validiert.
- Die Aufgabenplanungsvorlage aws-mainframe-modernization-stonebranch-integration funktioniert nur mit dem AWS Mainframe Modernization Service.
- Diese Vorlage zur Aufgabenplanung funktioniert nur auf einer Unix-, Linux- oder Windows-Edition von Stonebranch-Agenten.

Architektur

Architektur des Zielzustands

Das folgende Diagramm zeigt die AWS-Beispielumgebung, die für dieses Pilotprojekt erforderlich ist.

1. Das Stonebranch Universal Automation Center (UAC) umfasst zwei Hauptkomponenten: Universal Controller und Universal Agents. Stonebranch OMS wird als Nachrichtenbus zwischen dem Controller und einzelnen Agenten verwendet.
2. Die Stonebranch UAC-Datenbank wird von Universal Controller verwendet. Die Datenbank kann mit MySQL, Microsoft SQL Server, Oracle oder Aurora MySQL kompatibel sein.
3. AWS Mainframe Modernization Service — Micro Focus-Laufzeitumgebung mit der bereitgestellten BankDemo Anwendung. Die BankDemo Anwendungsdateien werden in einem S3-Bucket gespeichert. Dieser Bucket enthält auch die Mainframe-JCL-Dateien.
4. Stonebranch UAC kann die folgenden Funktionen für den Batchlauf ausführen:
    a. Starten Sie einen Batch-Job mit dem JCL-Dateinamen, der im S3-Bucket vorhanden ist, der mit dem AWS-Mainframe-Modernisierungsservice verknüpft ist.
    b. Rufen Sie den Status des ausgeführten Batch-Jobs ab.
    c. Warten Sie, bis der Batch-Job abgeschlossen ist.
    d. Ruft die Protokolle der Batch-Job-Ausführung ab.

e. Führen Sie die fehlgeschlagenen Batch-Jobs erneut aus.

f. Brechen Sie den Batch-Job ab, während der Job ausgeführt wird.

5. Stonebranch UAC kann die folgenden Funktionen für die Anwendung ausführen:

   a. Anwendung starten

   b. Status der Bewerbung abrufen

   c. Warten Sie, bis die Anwendung gestartet oder gestoppt ist

   d. Anwendung beenden

   e. Protokolle des Anwendungsbetriebs abrufen

Konvertierung von Stonebranch-Jobs

Das folgende Diagramm zeigt den Prozess der Umstellung von Arbeitsplätzen bei Stonebranch während der Modernisierung. Es wird beschrieben, wie die Jobpläne und Aufgabendefinitionen in ein kompatibles Format konvertiert werden, mit dem Batch-Aufgaben von AWS Mainframe Modernization ausgeführt werden können.

1. Für den Konvertierungsprozess werden die Jobdefinitionen aus dem vorhandenen Mainframe-System exportiert.
2. JCL-Dateien können in den S3-Bucket für die Mainframe-Modernisierungsanwendung hochgeladen werden, sodass diese JCL-Dateien vom AWS Mainframe Modernization Service bereitgestellt werden können.
3. Das Konvertierungstool konvertiert die exportierten Auftragsdefinitionen in UAC-Aufgaben.
4. Nachdem alle Aufgabendefinitionen und Jobpläne erstellt wurden, werden diese Objekte in den Universal Controller importiert. Die konvertierten Aufgaben führen dann die Prozesse im AWS Mainframe Modernization Service aus, anstatt sie auf dem Mainframe auszuführen.

Stonebranch UAC-Architektur

Das folgende Architekturdiagramm stellt ein active-active-passive Modell eines Universal Controllers mit hoher Verfügbarkeit (HA) dar. Stonebranch UAC wird in mehreren Availability Zones eingesetzt, um hohe Verfügbarkeit zu gewährleisten und Disaster Recovery (DR) zu unterstützen.

Universeller Controller

Zwei Linux-Server werden als Universal Controller bereitgestellt. Beide stellen eine Verbindung zum selben Datenbankendpunkt her. Jeder Server beherbergt eine Universal Controller-Anwendung und OMS. Zum Zeitpunkt der Bereitstellung wird die neueste Version von Universal Controller verwendet.

Die Universal Controller werden in der Tomcat-Webapp als Dokument ROOT bereitgestellt und auf Port 80 bereitgestellt. Diese Bereitstellung erleichtert die Konfiguration des Frontend-Load Balancers.

HTTP über TLS oder HTTPS wird mithilfe des Stonebranch-Platzhalterzertifikats aktiviert (z. B.). `https://customer.stonebranch.cloud` Dadurch wird die Kommunikation zwischen dem Browser und der Anwendung gesichert.

OMS

Ein Universal Agent und OMS (Opswise Message Service) befinden sich auf jedem Universal Controller-Server. Alle vom Kunden bereitgestellten Universal Agents sind so eingerichtet, dass sie eine Verbindung zu beiden OMS-Diensten herstellen. OMS fungiert als gemeinsamer Messaging-Dienst zwischen den Universal Agents und dem Universal Controller.

Amazon EFS mountet auf jedem Server ein Spool-Verzeichnis. OMS verwendet dieses gemeinsam genutzte Spool-Verzeichnis, um die Verbindungs- und Aufgabeninformationen von Controllern und Agenten zu speichern. OMS arbeitet in einem Hochverfügbarkeitsmodus. Wenn das aktive OMS ausfällt, hat das passive OMS Zugriff auf alle Daten und nimmt den aktiven Betrieb automatisch wieder auf. Universal Agents erkennen diese Änderung und stellen automatisch eine Verbindung zum neuen aktiven OMS her.

Datenbank

Amazon Relational Database Service (Amazon RDS) beherbergt die UAC-Datenbank, deren Engine mit Amazon Aurora MySQL kompatibel ist. Amazon RDS hilft bei der Verwaltung und Bereitstellung von geplanten Backups in regelmäßigen Abständen. Beide Universal Controller-Instances stellen eine Verbindung mit demselben Datenbank-Endpunkt her.

Load Balancer

Für jede Instanz wird ein Application Load Balancer eingerichtet. Der Load Balancer leitet den Datenverkehr zu einem bestimmten Zeitpunkt an den aktiven Controller weiter. Ihre Instance-Domainnamen verweisen auf die jeweiligen Load Balancer-Endpunkte.

URLs

Jede Ihrer Instanzen hat eine URL, wie im folgenden Beispiel gezeigt.

Umgebung	Instance
Produktion	customer.stonebranch.cloud
Entwicklung (außerhalb der Produktion)	customerdev.stonebranch.cloud
Testen (außerhalb der Produktion)	customertest.stonebranch.cloud

Hinweis: Instanznamen, die nicht zur Produktion verwendet werden, können Ihren Anforderungen entsprechend festgelegt werden.

Hohe Verfügbarkeit

Hochverfügbarkeit (HA) ist die Fähigkeit eines Systems, über einen bestimmten Zeitraum kontinuierlich ohne Ausfall zu arbeiten. Zu diesen Ausfällen gehören unter anderem Speicher, Reaktionsverzögerungen bei der Serverkommunikation aufgrund von CPU- oder Speicherproblemen und Netzwerkkonnektivität.

Um die HA-Anforderungen zu erfüllen:

- Alle EC2-Instances, Datenbanken und anderen Konfigurationen werden in zwei separaten Availability Zones innerhalb derselben AWS-Region gespiegelt.
- Der Controller wird über ein Amazon Machine Image (AMI) auf zwei Linux-Servern in den beiden Availability Zones bereitgestellt. Wenn Sie beispielsweise in der Region Europa eu-west-1 bereitgestellt werden, haben Sie einen Universal Controller in der Availability Zone eu-west-1a und der Availability Zone eu-west-1c.
- Jobs dürfen nicht direkt auf den Anwendungsservern ausgeführt werden und es dürfen keine Daten auf diesen Servern gespeichert werden.
- Der Application Load Balancer führt Integritätsprüfungen auf jedem Universal Controller durch, um den aktiven Controller zu identifizieren und den Datenverkehr an ihn weiterzuleiten. Falls bei einem Server Probleme auftreten, versetzt der Load Balancer den passiven Universal Controller automatisch in einen aktiven Status. Der Load Balancer identifiziert dann die neue aktive Universal Controller-Instanz anhand der Integritätsprüfungen und leitet den Datenverkehr weiter. Der Failover erfolgt innerhalb von vier Minuten ohne Jobverlust, und die Frontend-URL bleibt unverändert.

- Der Aurora MySQL-kompatible Datenbankdienst speichert Universal Controller-Daten. Für Produktionsumgebungen wird ein Datenbankcluster mit zwei Datenbank-Instances in zwei verschiedenen Availability Zones innerhalb einer einzigen AWS-Region erstellt. Beide Universal Controller verwenden eine Java Database Connectivity (JDBC) -Schnittstelle, die auf einen einzelnen Datenbankcluster-Endpunkt verweist. Falls bei einer Datenbankinstanz Probleme auftreten, verweist der Datenbankcluster-Endpunkt dynamisch auf die fehlerfreie Instanz. Es ist kein manueller Eingriff erforderlich.

Backup und Löschen

Stonebranch Universal Controller ist so eingestellt, dass alte Daten nach dem in der Tabelle angegebenen Zeitplan gesichert und gelöscht werden.

Typ	Plan
Aktivität	7 Tage
Prüfung	90 Tage
Verlauf	60 Tage

Backup-Daten, die älter als die angegebenen Daten sind, werden in das XML-Format exportiert und im Dateisystem gespeichert. Nach Abschluss des Sicherungsvorgangs werden ältere Daten aus der Datenbank gelöscht und für Produktionsinstanzen bis zu einem Jahr in einem S3-Bucket archiviert.

Sie können diesen Zeitplan in Ihrer Universal Controller-Oberfläche anpassen. Eine Verlängerung dieser Zeitrahmen kann jedoch zu längeren Ausfallzeiten während der Wartung führen.

Tools

AWS-Services

- AWS Mainframe Modernization ist eine Cloud-native AWS-Plattform, mit der Sie Ihre Mainframe-Anwendungen auf von AWS verwaltete Laufzeitumgebungen modernisieren können. Er bietet Tools und Ressourcen, die Sie bei der Planung und Implementierung von Migration und Modernisierung unterstützen.
- Amazon Elastic Block Store (Amazon EBS) bietet Volumes für die Speicherung auf Blockebene, die in Verbindung mit Amazon-EC2-Instances verwendet werden.

- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud. Dieses Muster verwendet Amazon Aurora MySQL-Compatible Edition.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon EC2 EC2-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Application Load Balancer.

Stonebranch

- Das Universal Automation Center (UAC) ist ein System von Produkten zur Workload-Automatisierung für Unternehmen. Dieses Muster verwendet die folgenden UAC-Komponenten:
  - Universal Controller, eine Java-Webanwendung, die in einem Tomcat-Webcontainer ausgeführt wird, ist die Lösung für Enterprise Job Scheduler und Workload Automation Broker von Universal Automation Center. Der Controller bietet eine Benutzeroberfläche zum Erstellen, Überwachen und Konfigurieren von Controller-Informationen, verwaltet die Planungslogik, verarbeitet alle Nachrichten an und von Universal Agents und synchronisiert einen Großteil des Hochverfügbarkeitsbetriebs von Universal Automation Center.
  - Universal Agent ist ein herstellerunabhängiger Planungsagent, der mit dem vorhandenen Job Scheduler auf allen wichtigen Computerplattformen zusammenarbeitet, sowohl auf älteren als auch auf verteilten Computerplattformen. Alle Scheduler, die auf z/Series, I/Series, Unix, Linux oder Windows laufen, werden unterstützt.
- Universal Agent ist ein herstellerunabhängiger Scheduling-Agent, der mit bestehenden Job-Schedulern auf allen wichtigen Computerplattformen, sowohl älteren als auch verteilten, zusammenarbeitet. Alle Scheduler, die auf z/Series, I/Series, Unix, Linux oder Windows laufen, werden unterstützt.
- Stonebranch aws-mainframe-modernization-stonebranch -integration AWS Mainframe Modernization Universal Extension ist die Integrationsvorlage zum Ausführen, Überwachen und erneuten Ausführen von Batch-Jobs auf der AWS Mainframe Modernization Platform.

Code

Der Code für dieses Muster ist im Repository aws-mainframe-modernization-stonebranch-integration verfügbar. GitHub

Epen

Installieren Sie Universal Controller und Universal Agent auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Installat ionsdateien herunter.	Laden Sie die Installation von den Stonebranch-Servern herunter. Wenden Sie sich an Stonebranch, um die Installat ionsdateien zu erhalten.	Cloud-Architekt
Starten Sie die EC2-Instanz.	Sie benötigen etwa 3 GB zusätzlichen Speicherplatz für die Universal Controller- und Universal Agent-Installationen. Stellen Sie also mindestens 30 GB Festplattenspeicher für die Instanz bereit. Fügen Sie der Sicherhei tsgruppe Port 8080 hinzu, damit darauf zugegriffen werden kann.	Cloud-Architekt
Überprüfen Sie die Vorausset zungen.	Gehen Sie vor der Installation wie folgt vor: 1. Installieren Sie Java wie unter Java Runtime Environment herunterladen beschrieben. `$ sudo yum -y update`	Cloud-Administrator, Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	$ sudo yum install
	 java-11-amazon-cor
	retto
	``
	Stellen Sie sicher, dass Sie eine der unterstützten JAVA-Versionen verwenden . Der vorherige Befehl sollte Java-11 installieren. Überprüfen Sie die Java-Version und stellen Sie sicher, dass Sie Version 11 verwenden, bevor Sie fortfahren.
	2. Führen Sie, wie im Dokument Installation von Apache Tomcat beschrieben, die folgenden Befehle aus.
	``
	$ sudo yum install
	 tomcat tomcat-admin-
	webapps
	$ sudo systemctl
	 enable tomcat
	$ sudo systemctl start
	 tomcat
	``
	3. Erstellen Sie eine Amazon Aurora Aurora-Datenbank, wie unter Einen Aurora MySQL-DB-Cluster erstellen und eine Verbindung zu diesem herstellen beschrieben. Verwenden Sie die Amazon	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aurora MySQL-kompatible Edition. Wählen Sie einen Master-Benutzernamen und ein Master-Passwort. Behalten Sie die Standardwerte für die restlichen Einstellungen bei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Universal Controller.	1. Laden Sie die `universal-controller-7.2.0.0.tar` Installationsdatei auf die EC2-Instanz hoch.
	2. Entarchivieren Sie die Installationsdateien in einem `temp` Ordner.
	`$ tar -xvf universal-controller-7.2.0.0.tar`
	3. Erteilen Sie dem Installationsskript die Ausführungsberechtigung.
	`$ chmod a+x install-controller.sh`
	4. Installieren Sie den Controller. In diesem Beispiel wird der folgende Befehl verwendet, um Universal Controller unter `/usr/share/tomcat` zu installieren. Verwenden Sie die Amazon Aurora Aurora-Datenbank, die Sie in den vorherigen Schritten erstellt haben.
	`$ sudo ./install-controller.sh --tomcat-dir /usr/share/tomcat/ --controller-file universal-controller-7.2.0.`
		Cloud-Architekt, Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	0-build.145.war --dbuser admin --dbpass “****” --dbname uc --rdbms mysql --dburl jdbc:mysql://database-2-instance-1.cih63miincgy.us-east-1.rds.amazonaws.com:3306/ Die letzte Zeile der Skriptausgabe sollte „Installation abgeschlossen“ lauten. 5. Navigieren Sie in der EC2-Instanz zur folgenden URL. http://<public_ip>:8080/uc 6. Geben Sie auf dem Anmeldebildschirm im Bereich Nutzername ops.admin ein und lassen Sie das Feld Passwort leer. 7. Legen Sie ein neues Passwort für den `ops.admin` Benutzer fest.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Universal Agent.	1. Laden Sie die `sb-7.2.0.1-linux-3.10-x86_64.tar.Z` Installationsdatei auf die EC2-Instanz hoch.
	2. Melden Sie sich bei der EC2-Instance an.
	3. Entarchivieren Sie das Universal Agent-Installationspaket.
	`$ zcat sb-7.2.0.1-linux-3.10-x86_64.tar.Z | tar xvf -`
	4. Führen Sie den folgenden Befehl aus.
	`$ sudo ./unvinst --oms_servers 7878@localhost --oms_autostart yes --python yes`
	5. Erstellen Sie eine PAM-Datei.
	`$ cp /etc/pam.d/login /etc/pam.d/ucmd`
	6. Aktivieren Sie Autostart für Universal Agent.
	`$ /sbin/restorecon -v /etc/rc.d/init.d/ubrokerd`
		Cloud-Administrator, Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie OMS zu Universal Controller hinzu.	1. Melden Sie sich mit dem `ops.admin` Benutzer bei Universal Controller an. 2. Wählen Sie in der oberen linken Ecke des Bildschirms das Menü Dienste und anschließend im System das Menü OMS-Server 3. Geben Sie im Feld OMS-Serveradresse localhost ein, und speichern Sie dann. 4. Der Status des OMS-Servers wird als Verbunden und der Sitzungsstatus als Betriebsbereit angezeigt.	Universeller Controller-Administrator

Importieren Sie AWS Mainframe Modernization Universal Extension und erstellen Sie eine Aufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Integrationsvorlage importieren.	Für diesen Schritt benötigen Sie die AWS Mainframe Modernization Universal Extension. Stellen Sie sicher, dass die neueste veröffentlichte Version der ZIP-Datei heruntergeladen wurde. 1. Melden Sie sich mit dem `ops.admin` Benutzer am Universal Controller an.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Navigieren Sie zu Dienste, Integrationsvorlage importieren. 3. Wählen Sie die ZIP-Datei (`aws_mainframe_modernization_stonebranch_extension.zip`) der Integrationsvorlage aus und klicken Sie auf Importieren. Nachdem die Integrationsvorlage importiert wurde, werden unter Verfügbare Services AWS Mainframe Modernization Tasks angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie auflösbare Anmeldeinformationen.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus: • Name: Neue Aufgabe zur Mainframe-Modernisierung • Agent: Wählen Sie den einzigen Agenten aus (AGNT0001). Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Umgebungen auflisten • AWS-Anmeldeinformationen: Wenn Sie der EC2-Instance eine AWS Identity and Access Management (IAM) -Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie das Symbol () neben dem Feld. Geben Sie in dem sich öffnenden Fenster mit den	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anmeldeinformationen die folgenden Informationen ein und speichern Sie dann. • Name: Anmeldeinformationen für die AWS-Mainframe-Modernisierung • Runtime-Benutzer: Schreiben Sie die AWS-Zugriffsschlüssel-ID in dieses Feld. • Runtime-Passwort: Schreiben Sie den geheimen AWS-Schlüssel in dieses Feld. • Endpunkt: Stellen Sie sicher, dass der Endpunkt die richtige AWS-Region hat. Die Standardeinstellung ist https://m2.us-east-1.amazonaws.com. • Region: Geben Sie die Region des AWS Mainframe Modernization Service ein. Der Standardwert ist `us-east-1` . 3. Behalten Sie die Standardwerte in den übrigen Feldern bei und speichern Sie die Aufgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe.	1. Wählen Sie oben im rechten Bereich die Option „Aufgabe starten“. 2. Wählen Sie im Bestätigungsfenster die Option Starten aus. Danach zeigt die Universal Controller Console eine Meldung an, die der folgenden Meldung ähnelt. 24.08.2022 10:11:49 Uhr Die Universalaufgabe „New Mainframe Modernization Task“ mit der Task-Instanz sys_id 1661291493634146313NC8E38DB8OZJY wurde erfolgreich gestartet. 3. Navigieren Sie zu Instances Wenn Sie den Tab Instances nicht sehen, klicken Sie auf den Rechtspfeil, um nach rechts zu blättern. 4. Öffnen Sie das Kontextmenü (mit der rechten Maustaste) für die Task-Instanz in der Liste, wählen Sie „Ausgabe abrufen“ und dann unter „Ausgabe abrufen“ die Option „Senden“	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Im Fenster „Ausgabe abrufen“ sehen Sie die Liste der Umgebungen in STDOUT.	

Testen Sie das Starten eines Batch-Jobs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabe für den Batch-Job.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus: • Name: Neue Aufgabe zur Mainframe-Modernisierung • Agent: Wählen Sie den einzigen Agenten aus (AGNT0001). Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Batch starten (oder Batch starten und warten, bis der Batch-Job ausgeführt wird und bis die Aufgabe in AWS abgeschlossen ist) • AWS-Anmeldeinformationen: Wenn Sie der EC2-Instance eine IAM-Rolle hinzugefü	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten `AWSSecretKey`, wählen Sie das Symbol () neben dem Feld. • Endpunkt: Stellen Sie sicher, dass der Endpunkt die richtige AWS-Region hat. Die Standardeinstellung ist https://m2.us-east-1.amazonaws.com. • Region: Geben Sie die Region des AWS Mainframe Modernization Service ein. Der Standardwert ist `us-east-1`. • Anwendung: Wählen Sie das Symbol neben dem Feld () und wählen Sie unter „Refresh Application Choices“ die Option „Senden“ aus. Dadurch wird eine Verbindung zum AWS Mainframe Modernization Service hergestellt und die Liste der Anwendungen zurückgegeben. Jetzt können Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Anwendung aus der Drop-down-Liste auswählen. Wählen Sie die Anwendung aus, mit der Sie den Batch-Job ausführen möchten. • JCL-Dateiname: `RUNHELLO.jcl` • Auf Erfolg oder Fehler warten: Wenn diese Option ausgewählt ist, wartet die Aufgabe, bis der Batch-Job den Status „Erfolg“ oder „Fehlschlag“ hat. • Abfrageintervall: Dies ist der Zeitraum zwischen den einzelnen Abfragen. • Ausführungsprotokolle abrufen: Wenn diese Option ausgewählt ist, werden Protokolle automatisch abgerufen , wenn der Batch-Job abgeschlossen ist. • Protokollformat: Dies ist das Format der Protokoll e, die ausgedruckt werden sollen. Es kann im Text- oder JSON-Form at sein. 3. Behalten Sie die Standardw erte in den übrigen Feldern	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bei und speichern Sie die Aufgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe.	1. Wählen Sie oben im rechten Bereich die Option „Aufgabe starten“. 2. Wählen Sie im Bestätigungsfenster die Option Starten aus. Danach zeigt die Universal Controller Console eine Meldung an, die der folgenden Meldung ähnelt. 24.08.2022 11:11:59 Uhr Die Universalaufgabe „Mainframe Modernization Start Batch“ wurde erfolgreich mit der Taskinstanz sys_id gestartet. <sys id> 3. Navigieren Sie zur Registerkarte „Instances“. Wenn Sie den Tab „Instances“ nicht sehen, klicken Sie auf den Rechtspfeil, um nach rechts zu blättern. 4. Öffnen Sie das Kontextmenü (mit der rechten Maustaste) für die Task-Instanz in der Liste, wählen Sie „Ausgabe abrufen“ und dann unter „Ausgabe abrufen“ die Option „Senden“	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Im Fenster „Ausgabe abrufen“ sehen Sie die Liste der Umgebungen in STDOUT.	

Erstellen Sie einen Workflow für mehrere Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Aufgaben.	1. Öffnen Sie das Kontextmenü (Rechtsklick) für die Aufgabe, von der Sie Kopien erstellen möchten, und wählen Sie Kopieren. 2. Geben Sie im Fenster Copy AWS Mainframe Modernization Task den folgenden neuen Namen für die neue Aufgabe ein: Mainframe Modernization Start Batch — RUNAWS2. 3. Kopieren Sie die Aufgabe erneut und verwenden Sie dabei den folgenden Namen: Mainframe Modernization Start Batch - RUNAWS3. 4. Kopieren Sie erneut mit der Aufgabe und verwenden Sie dabei den folgenden Namen: Mainframe Modernization Start Batch - RUNAWS4.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Kopieren Sie die Aufgabe ein letztes Mal und verwenden Sie dabei den folgenden Namen: Mainframe Modernization Start Batch - FOOBAR.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aufgaben aktualisieren.	1. Öffnen (doppelklicken) Sie die Aufgabe Mainframe Modernization Start Batch — RUNAWS2, ändern Sie das Feld JCL-Datei name in und speichern Sie`RUNAWS2.jcl` . 2. Öffnen (doppelklicken) Sie die Aufgabe Mainframe Modernization Start Batch — RUNAWS3, ändern Sie das Feld JCL-Datei name in und speichern Sie*`RUNAWS3.jcl`* . 3. Öffnen (doppelklicken) Sie die Aufgabe Mainframe Modernization Start Batch — RUNAWS4, ändern Sie das Feld JCL-Datei name in und speichern Sie. *`RUNAWS4.jcl`* 4. Öffnen (doppelklicken) Sie die Aufgabe Mainframe Modernization Start Batch — FOOBAR, ändern Sie das Feld JCL-Datei name in und speichern Sie*`MISSING.jcl`* . Diese Aufgabe schlägt fehl, weil der Wert für den JCL-Datei namen falsch ist.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Workflow.	1. Navigieren Sie zu Dienste, Workflows. 2. Geben Sie im rechten Bereich Mainframe Modernization Workflow in das Feld Name ein und speichern Sie. 3. Wählen Sie im rechten Bereich die Option Workflow bearbeiten aus. 4. Klicken Sie auf der Registerkarte Workflow-Editor auf die Schaltfläche „Aufgabe hinzufügen“ (+). 5. Wählen Sie im Fenster „Aufgaben suchen“ die Option „Suchen“, um alle Aufgaben im Universal Controller anzuzeigen. 6. Klicken Sie auf das Symbol neben Mainframe Modernization Start Batch Task und ziehen Sie das Symbol an eine leere Stelle im Workflow-Editor. 7. Wiederholen Sie dieselbe Aktion für die anderen Mainframe-Modernis ierungsaufgaben und platzieren Sie sie wie im Abschnitt Zusätzliche Informationen gezeigt.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie die Schaltfläche Connect () und verbinden Sie die Aufgaben miteinander. Um eine Aufgabe mit einer anderen zu verbinden, klicken Sie in die Mitte einer Aufgabe und ziehen Sie sie auf die Zielaufgabe. 9. Connect die Aufgaben wie im Abschnitt Zusätzliche Informationen gezeigt, und speichern Sie den Workflow. 10. Klicken Sie mit der rechten Maustaste auf eine leere Stelle im Workflow-Editor, wählen Sie Workflow starten und dann OK.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status des Workflows.	1. Wählen Sie im linken Menü die Aktivität 2. Wählen Sie in der Mitte des Fensters Start. Sie sehen die Liste der Task-Instanzen in der Liste. 3. Öffnen Sie den Mainframe Modernization Workflow in der Liste (doppelklicken Sie darauf) oder öffnen Sie das Kontextmenü (mit der rechten Maustaste) und wählen Sie Workflow-Aufgabenbefehle, Workflow anzeigen aus. Sie sehen die Aufgaben so, wie sie im Abschnitt Zusätzliche Informati onen dargestellt sind. Es wurde erwartet, dass die zweite Aufgabe fehlschla gen würde, weil Sie eine fehlende JCL-Datei verwendet haben.	Universeller Controller-Administrator

Beheben Sie fehlgeschlagene Batch-Jobs und führen Sie sie erneut aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie die fehlgesch lagene Aufgabe und führen Sie sie erneut aus.	1. Öffnen Sie die fehlgesch lagene Aufgabe (doppelkl icken Sie darauf), um den	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Fehler für die Aufgabe zu sehen. 2. Sie haben zwei Möglichkeiten, die fehlgeschlagene Aufgabe zu reparieren. • Korrigieren Sie den JCL-Dateinamen und setzen Sie ihn auf`F00BAR.jcl` . • Fügen Sie dem JCL-Dateinamen (Temp) den richtigen JCL-Dateinamen hinzu. Dieses Feld überschreibt das Feld JCL-Dateiname. Wählen Sie für dieses Pilotprojekt die zweite Option und speichern Sie die Task-Instanz. 3. Öffnen Sie im Workflow-Monitor das Kontextmenü (Rechtsklick) für die fehlgeschlagene Aufgabe und wählen Sie Befehle, Erneut ausführen. 4. Danach werden alle Aufgaben erfolgreich abgeschlossen.	

Aufgaben „Anwendung starten“ und „Anwendung beenden“ erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Aktion „Anwendung starten“.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus. • Name: Anwendung zur Mainframe-Modernisierung starten • Agent: Wählen Sie den einzigen Agenten (AGNT0001) Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Anwendung starten • AWS-Anmeldeinformationen: Wenn Sie der EC2-Instance eine IAM-Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie die Anmeldeinformationen aus, die Sie zuvor erstellt haben. • Endpunkt: Stellen Sie sicher, dass der	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Endpunkt die richtige Region hat. Die Standardeinstellung ist https://m2.us-east-1.amazonaws.com. • Region: Geben Sie die Region des AWS Mainframe Modernization Service ein. Der Standardwert ist `us-east-1` . • Anwendung: Wählen Sie das Symbol neben dem Feld () und wählen Sie unter „Refresh Application Choices“ die Option „Senden“ aus. Dadurch wird eine Verbindung zum AWS Mainframe Modernization Service hergestellt und die Liste der Anwendungen zurückgegeben. Jetzt können Sie die Anwendung aus der Drop-down-Liste auswählen. Wählen Sie die Anwendung aus, mit der Sie den Batch-Job ausführen möchten. • Auf Erfolg oder Fehler warten: Wenn diese Option ausgewählt ist, wartet die Aufgabe, bis	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Status des Batch-Jobs erfolgreich oder fehlgeschlagen ist. • Abfrageintervall: Dies ist der Zeitraum zwischen den einzelnen Abfragen. • Ausführungsprotokolle abrufen: Wenn diese Option ausgewählt ist, werden Protokolle automatisch abgerufen , wenn der Batch-Job abgeschlossen ist. • Protokollformat: Dies ist das Format der Protokoll e, die ausgedruckt werden sollen. Es kann im Text- oder JSON-Form at sein. 3. Behalten Sie die Standardw erte in den übrigen Feldern bei und speichern Sie die Aufgabe. 4. Kopieren Sie nun diese Aufgabe und erstellen Sie eine Aufgabe für „Anwendung beenden“. Ändern Sie den Namen in Mainframe Moderniz ation Stop Application und ändern Sie die Aktion in Stop Application.	

Eine Aufgabe zum Abbrechen der Batch-Ausführung erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Aktion Batch stornieren.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus. • Name: Mainframe-Modernisierung Batch-Ausführung abbrechen • Agent: Wählen Sie den einzigen Agenten (AGNT0001) Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Batch-Ausführung abbrechen • AWS-Anmeldeinformationen: Wenn Sie der EC2-Instance eine IAM-Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie die Anmeldeinformationen aus, die Sie zuvor erstellt haben. • Endpunkt: Stellen Sie sicher, dass der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Endpunkt die richtige Region hat. Die Standardeinstellung ist https://m2.us-east-1.amazonaws.com. • Region: Geben Sie die Region des AWS Mainframe Modernization Service ein. Der Standardwert ist `us-east-1` . • Anwendung: Wählen Sie das Symbol neben dem Feld () und wählen Sie unter „Refresh Application Choices“ die Option „Senden“ aus. Dadurch wird eine Verbindung zum AWS Mainframe Modernization Service hergestellt und die Liste der Anwendungen zurückgegeben. Jetzt können Sie die Anwendung aus der Drop-down-Liste auswählen. Wählen Sie die Anwendung aus, mit der Sie den Batch-Job ausführen möchten. • Auf Erfolg oder Fehler warten: Wenn diese Option ausgewählt ist, wartet die Aufgabe, bis	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Status des Batch-Jobs erfolgreich oder fehlgeschlagen ist. • Abfrageintervall: Dies ist der Zeitraum zwischen den einzelnen Abfragen. • Ausführungsprotokolle abrufen: Wenn diese Option ausgewählt ist, werden Protokolle automatisch abgerufen , wenn der Batch-Job abgeschlossen ist. • Protokollformat: Dies ist das Format der Protokoll e, die ausgedruckt werden sollen. Es kann im Text- oder JSON-Form at sein. 3. Behalten Sie die Standardw erte in den übrigen Feldern bei und speichern Sie die Aufgabe.	

Zugehörige Ressourcen

- Universeller Controller
- Universeller Agent
- LDAP-Einstellungen
- Einstellungen für Single Sign-On
- Hochverfügbarkeit
- Xpress-Konvertierungstool

Zusätzliche Informationen

Symbole im Workflow-Editor

Alle Aufgaben sind miteinander verbunden

Status des Workflows

Migrieren und replizieren Sie VSAM-Dateien zu Amazon RDS oder Amazon MSK mithilfe von Connect from Precisely

Erstellt von Prachi Khanna (AWS) und Bo microSD GOPALSAMY (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: VSAM	Ziel: Datenbank
R-Typ: Neuarchitektur	Workload: IBM	Technologien: Mainframe; Modernisierung
AWS-Services: Amazon MSK; Amazon RDS; AWS Mainframe Modernization		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Dateien der Virtual Storage Access Method (VSAM) von einem Mainframe in eine Zielumgebung in der AWS Cloud migrieren und replizieren, indem Sie Connect from Precisely verwenden. Zu den Zielumgebungen, die in diesem Muster behandelt werden, gehören Amazon Relational Database Service (Amazon RDS) und Amazon Managed Streaming für Apache Kafka (Amazon MSK). Connect verwendet Change Data Capture (CDC), um kontinuierlich Updates für Ihre Quell-VSAM-Dateien zu überwachen und diese Updates dann in eine oder mehrere Ihrer AWS-Zielumgebungen zu übertragen. Sie können dieses Muster verwenden, um Ihre Ziele in Bezug auf die Modernisierung Ihrer Anwendung oder Datenanalyse zu erreichen. Sie können beispielsweise Connect verwenden, um Ihre VSAM-Anwendungsdateien mit niedriger Latenz in die AWS Cloud zu migrieren, oder Ihre VSAM-Daten zu einem AWS Data Warehouse oder Data Lake für Analysen migrieren, die Synchronisationslatenzen tolerieren können, die höher sind als für die Anwendungsmoderation erforderlich.

Voraussetzungen und Einschränkungen

Voraussetzungen

- IBM z/OS V2R1 oder höher
- CICS Transaction Server für z/OS (CICS TS) V5.1 oder höher (CICS/VSAM-Datenerfassung)

- IBM MQ 8.0 oder höher
- Einhaltung der z/OS-Sicherheitsanforderungen (z. B. APF-Autorisierung für SQData-Ladebibliotheken)
- VSAM-Wiederherstellungsprotokolle aktiviert
- (Optional) CICS VSAM Recovery Version (CICS VR) zur automatischen Erfassung von CDC-Protokollen
- Ein aktives AWS-Konto
- Eine Amazon Virtual Private Cloud (VPC) mit einem Subnetz, das von Ihrer Legacy-Plattform erreichbar ist
- Eine VSAM Connect-Lizenz von Precisely

Einschränkungen

- Connect unterstützt keine automatische Erstellung von Zieltabellen auf der Grundlage von Quell-VSAM-Schemas oder -Kopierbooks. Sie müssen die Struktur der Zieltabelle zum ersten Mal definieren.
- Für Nicht-Streaming-Ziele wie Amazon RDS müssen Sie die Konvertierungsquelle zur Zielzuordnung im Konfigurationsskript Apply Engine angeben.
- Protokollierungs-, Überwachungs- und Warnfunktionen werden über APIs implementiert und erfordern, dass externe Komponenten (wie Amazon CloudWatch) voll funktionsfähig sind.

Produktversionen

- SQData 40134 für z/OS
- SQData 4.0.43 für das Amazon Linux Amazon Machine Image (AMI) auf Amazon Elastic Compute Cloud (Amazon EC2)

Architektur

Quelltechnologie-Stack

- Job Control Language (JCL)
- z/OS Unix-Shell und Interactive System microSD Facility (ISPF)
- VSAM-Dienstprogramme (IDCAMS)

Zieltechnologie-Stack

- Amazon EC2
- Amazon MSK
- Amazon RDS
- Amazon VPC

Zielarchitektur

Migrieren von VSAM-Dateien zu Amazon RDS

Das folgende Diagramm zeigt, wie VSAM-Dateien in Echtzeit oder nahezu in Echtzeit in eine relationale Datenbank wie Amazon RDS migriert werden, indem der CDC-Agent/Publisher in der Quellumgebung (On-Premises-Mainframe) und die Apply Engine in der Zielumgebung (AWS Cloud) verwendet werden.

Das Diagramm zeigt den folgenden Batch-Workflow:

1. Connect erfasst Änderungen an einer Datei, indem VSAM-Dateien aus Sicherungsdateien verglichen werden, um Änderungen zu identifizieren, und sendet die Änderungen dann an den Protokollstream.
2. Der Herausgeber verbraucht Daten aus dem Systemprotokollstream.
3. Der Publisher teilt einer Ziel-Engine erfasste Datenänderungen über TCP/IP mit. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Apply Engine in der Zielumgebung empfängt die Änderungen vom Publisher-Agenten und wendet sie auf eine relationale oder nicht relationale Datenbank an.

Das Diagramm zeigt den folgenden Online-Workflow:

1. Connect erfasst Änderungen in der Online-Datei mithilfe einer Protokollreplikation und streamt dann erfasste Änderungen an einen Protokollstream.
2. Der Herausgeber verbraucht Daten aus dem Systemprotokollstream.
3. Der Herausgeber teilt der Ziel-Engine erfasste Datenänderungen über TCP/IP mit. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.

4. Die Apply Engine in der Zielumgebung empfängt die Änderungen vom Publisher-Agenten und wendet sie dann auf eine relationale oder nicht relationale Datenbank an.

Migrieren von VSAM-Dateien zu Amazon MSK

Das folgende Diagramm zeigt, wie VSAM-Datenstrukturen im Hochleistungsmodus von einem Mainframe zu Amazon MSK gestreamt und JSON- oder AVRO-Schemakonvertierungen automatisch generiert werden, die in Amazon MSK integriert werden können.

Das Diagramm zeigt den folgenden Batch-Workflow:

1. Connect erfasst Änderungen an einer Datei mithilfe von CICS VR oder durch Vergleichen von VSAM-Dateien aus Sicherungsdateien, um Änderungen zu identifizieren. Erfasste Änderungen werden an den Protokollstream gesendet.
2. Der Herausgeber verbraucht Daten aus dem Systemprotokollstream.
3. Der Herausgeber teilt der Ziel-Engine erfasste Datenänderungen über TCP/IP mit. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Replikator-Engine, die im Parallelverarbeitungsmodus arbeitet, teilt die Daten in einen Arbeits-Cache auf.
5. Worker-Threads erfassen die Daten aus dem Cache.
6. Daten werden in Amazon-MSK-Themen aus den Worker-Threads veröffentlicht.
7. Benutzer wenden Änderungen von Amazon MSK auf Ziele wie Amazon DynamoDB, Amazon Simple Storage Service (Amazon S3) oder Amazon OpenSearch Service mithilfe von Connectors an.

Das Diagramm zeigt den folgenden Online-Workflow:

1. Änderungen in der Online-Datei werden mithilfe einer Protokollreplikation erfasst. Erfasste Änderungen werden an den Protokollstream gestreamt.
2. Der Herausgeber verbraucht Daten aus dem Systemprotokollstream.
3. Der Herausgeber teilt der Ziel-Engine erfasste Datenänderungen über TCP/IP mit. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Replikator-Engine, die im Parallelverarbeitungsmodus arbeitet, teilt die Daten in einen Arbeits-Cache auf.

5. Worker-Threads erfassen die Daten aus dem Cache.
6. Daten werden in Amazon-MSK-Themen aus den Worker-Threads veröffentlicht.
7. Benutzer wenden Änderungen von Amazon MSK auf Ziele wie DynamoDB ,Amazon S3 oder OpenSearch Service mithilfe von Connectors an.

Tools

- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.

Polen

Vorbereiten der Quellumgebung (Hauptrahmen)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Connect CDC 4.1.	1. Wenden Sie sich an das Precisely Support-Team, um eine Lizenz und Installationspakete zu erhalten. 2. Verwenden Sie Beispiel-JCLs, um Connect CDC 4.1 zu installieren. Anweisungen finden Sie unter Installieren von Connect CDC (SQData) mit JCL in der Präzise Dokumentation. 3. Führen Sie den `SETPROG APF` Befehl aus, um die Connect-Ladebibliotheken SQDATA.V4nnn.LOADLIB zu autorisieren.	IBM Mainframe Developer/ Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das zFS-Verze ichnis ein.	Um ein zFS-Verzeichnis einzurichten, folgen Sie den Anweisungen aus den zFS-Variablenverzeichnissen in der Präzise Dokumentation. Hinweis: Controller-Daemon- und Capture/Publisher-Agent-Konfigurationen werden im Dateisystem z/OS UNIX Systems Services gespeiche rt (bezeichnet als zFS). Die Controller-Daemon-, Capture-, Storage- und Publisher-Agenten benötigen eine vordefinierte zFS-Verze ichnisstruktur zum Speichern einer kleinen Anzahl von Dateien.	IBM Mainframe Developer/ Admin
Konfigurieren Sie TCP/IP-Po rts.	Um TCP/IP-Ports zu konfigurieren, folgen Sie den Anweisungen unter TCP/IP-Ports in der Dokumentation Präzise. Hinweis: Der Controller-Daemon benötigt TCP/IP-Po rts auf Quellsystemen. Die Ports werden von den Engines auf den Zielsystemen referenzi ert (wo erfasste Änderungs daten verarbeitet werden).	IBM Mainframe Developer/ Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen z/OS-Protokollstream.	Um einen z/OS-Protokollstream zu erstellen, folgen Sie den Anweisungen unter Create z/OS system logStreams in der Präzise Dokumentation. Hinweis: Connect verwendet den Logstream, um während der Migration Daten zwischen Ihrer Quellumgebung und der Zielumgebung zu erfassen und zu streamen. Ein Beispiel für eine JCL, die eine z/OS- erstellt LogStream, finden Sie unter Erstellen von z/OS-System-logStreams in der Dokumentation Präzise.	IBM Mainframe-Entwickler
Identifizieren und autorisieren Sie IDs für zFS-Benutzer und gestartete Aufgaben.	Verwenden Sie RACF, um Zugriff auf das OMVS-zFS-Dateisystem zu gewähren. Eine Beispiel-JCL finden Sie unter Identifizieren und Autorisieren von zFS-Benutzer- und gestarteten Aufgaben-IDs in der Präzise Dokumentation.	IBM Mainframe-Entwickler/ Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie öffentliche/private z/OS-Schlüssel und die autorisierte Schlüsseldatei.	Führen Sie die JCL aus, um das Schlüsselpaar zu generieren. Ein Beispiel finden Sie unter Beispiel für Schlüsselpaare im Abschnitt Zusätzliche Informationen dieses Musters. Anweisungen finden Sie unter Generieren öffentlicher und privater z/OS-Schlüssel und autorisierter Schlüsseldatei in der Präzise Dokumentation.	IBM Mainframe-Entwickler/Admin

Aktivieren Sie das CICS VSAM Log Replicate und fügen Sie es an den Protokoll stream an.	Führen Sie das folgende JCL-Skript aus:
	
	`//STEP1 EXEC PGM=IDCAMS`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSIN DD *`
	`ALTER SQDATA.CICS.FILEA -`
	`LOGSTREAMID(SQDATA.VSAMCDC.LOG1) -`
	`LOGREPLICATE`
		IBM Mainframe-Entwickler/Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie das VSAM File Recovery Log über eine -FCT.	Ändern Sie die Dateisteuerungstabelle (FCT), um die folgenden Parameteränderungen widerzuspiegeln: `Configure FCT Parms CEDA ALT FILE(name) GROUP(groupname) DSNAME(data set name) RECOVERY(NONE|BACKOUTONLY|ALL) FWDRECOVLOG(NO|1-99) BACKUPTYPE(STATIC|DYNAMIC) RECOVERY PARAMETERS RECOVery : None | Backoutonly | All Fwdrecovlog : No | 1-99 BAckuptype : Static | Dynamic`	IBM Mainframe-Entwickler/ Admin
Richten Sie CD CzLog für den Publisher-Agenten ein.	1. Erstellen Sie die CD CzLog Publisher CAB-Datei. 2. Verschlüsseln Sie die veröffentlichten Daten. 3. Bereiten Sie die CD CzLog Publisher Runtime JCL vor.	IBM Mainframe-Entwickler/ Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Controller-Daemon.	1. Öffnen Sie das ISPF-Bedienfeld und führen Sie den folgenden Befehl aus, um das Menü Präzissiv zu öffnen: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Um den Controller-Daemon einzurichten, wählen Sie Option 2 aus dem Menü aus.	IBM Mainframe-Entwickler/Admin
Aktivieren Sie den Herausgeber.	1. Öffnen Sie das ISPF-Bedienfeld und führen Sie den folgenden Befehl aus, um das Menü Präzissiv zu öffnen: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Um den Herausgeber einzurichten, wählen Sie Option 3 aus dem Menü und I zum Einfügen aus.	IBM Mainframe-Entwickler/Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Logstream.	1. Öffnen Sie das ISPF-Bedienfeld und führen Sie den folgenden Befehl aus, um das Menü Präzissiv zu öffnen: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Um den Protokollstream einzurichten, wählen Sie Option 4 aus dem Menü und I für das Einfügen aus. Geben Sie dann den Namen des Protokollstreams ein, der in den vorherigen Schritten erstellt wurde.	IBM Mainframe-Entwickler/Admin

Vorbereiten der Zielumgebung (AWS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Präzise auf einer EC2-Instance.	Um Connect from Precisely auf dem Amazon Linux AMI für Amazon EC2 zu installieren, folgen Sie den Anweisungen unter Install Connect CDC (SQData) on UNIX in der Precisely-Dokumentation.	Allgemeines AWS
Öffnen Sie TCP/IP-Ports.	Um die Sicherheitsgruppe so zu ändern, dass sie die Controller-Daemon-Ports für ein- und ausgehenden	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zugriff enthält, folgen Sie den Anweisungen von TCP/IP in der Dokumentation Präzise.	
Erstellen Sie Dateiverz eichnisse.	Um Dateiverzeichnisse zu erstellen, folgen Sie den Anweisungen unter Zielanwen dungsumgebung vorbereiten in der Dokumentation Präzise.	Allgemeines AWS

Erstellen Sie die Konfigura tionsdatei Apply Engine.	Erstellen Sie die Konfigura tionsdatei Apply Engine im Arbeitsverzeichnis der Apply Engine. Die folgende Beispielkonfigurationsdatei zeigt Apache Kafka als Ziel:
	`builtin.features=S ASL_SCRAM`
	`security.protocol= SASL_SSL`
	`sasl.mechanism=SCR AM-SHA-512`
	`sasl.username=`
	`sasl.password=`
	`metadata.broker.li st=`
	Hinweis: Weitere Informati onen finden Sie unter Sicherheit in der Apache-Ka fka-Dokumentation.
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Skripts für die Apply Engine-Verarbeitung.	Erstellen Sie die Skripts für die Apply Engine, um Quelldaten zu verarbeiten und Quelldaten auf das Ziel zu replizieren. Weitere Informationen finden Sie unter Erstellen eines Anwendungs-Engine-Skripts in der Präzisionsdokumentation.	Allgemeines AWS
Führen Sie die Skripts aus.	Verwenden Sie die `SQDENG` Befehle `SQDPARSE` und , um das Skript auszuführen. Weitere Informationen finden Sie unter Parsen eines Skripts für zOS in der Präzisionsdokumentation.	Allgemeines AWS

Validieren der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Liste der VSAM-Dateien und Zieltabellen für die CDC-Verarbeitung.	1. Validieren Sie VSAM-Dateien, einschließlich Replikationsprotokollen, Wiederherstellungsprotokollen, FCT-Parametern und dem Protokollstream. 2. Validieren Sie Zieldatenbanktabellen, einschließlich der Frage, ob die Tabellen gemäß der erforderlichen Schemadefinition, dem Tabellenzugriff und anderen Kriterien erstellt werden.	Allgemeines AWS, Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass das Connect-CDC-SQData-Produkt verknüpft ist.	Führen Sie einen Testauftrag aus und überprüfen Sie, ob der Rückgabecode für diesen Auftrag 0 (erfolgreich) ist. Hinweis: Connect CDC SQData Apply Engine-Stat usmeldungen sollten aktive Verbindungsmeldungen anzeigen.	Allgemeines AWS, Mainframe

Ausführen und Validieren von Testfällen (Batch)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Batch-Auftrag auf dem Mainframe aus.	Führen Sie den Batch-Anwendungsauftrag mit einer geänderten JCL aus. Fügen Sie die folgenden Schritte in die geänderte JCL ein: 1. Erstellen Sie ein Backup der Datendateien. 2. Vergleichen Sie die Sicherungsdatei mit den geänderten Datendateien, generieren Sie die Deltadatei und notieren Sie sich dann die Delta-Datensatzanzahl aus den Nachrichten. 3. Verschieben Sie die Deltadatei in den z/OS-Prot okollstream.	Allgemeines AWS, Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Führen Sie die JCL aus. Ein Beispiel für eine JCL finden Sie unter Dateivergleich vorbereiten in der Präzise Dokumentation.	
Überprüfen Sie den Logstream .	Überprüfen Sie den Protokoll stream, um zu bestätigen, dass Sie die Änderungsdaten für den abgeschlossenen Mainframe-Batch-Auftrag sehen können.	Allgemeines AWS, Mainframe
Validieren Sie die Anzahl der Änderungen am Quelldelta und der Zieltabelle.	Gehen Sie wie folgt vor, um zu bestätigen, dass die Datensätze beschädigt wurden: 1. Erfassen Sie die Anzahl der Quell-Delta aus den Batch-JCL-Nachrichten. 2. Überwachen Sie die Anzahl der in der VSAM-Datei eingefügten, aktualisierten oder gelöschten Datensätze auf Datensatzebene. 3. Fragen Sie die Zieltabelle nach der Anzahl der Datensätze ab. 4. Vergleichen und listen Sie alle verschiedenen Datensatzanzahlen auf.	Allgemeines AWS, Mainframe

Ausführen und Validieren von Testfällen (Online)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Online-Tr ansaktion in einer CICS-Regi on aus.	1. Führen Sie die Online-Tr ansaktion aus, um den Testfall zu validieren. 2. Validieren Sie den Transakti onsausführungscode (RC=0 – Erfolg).	IBM Mainframe-Entwickler
Überprüfen Sie den Logstream .	Vergewissern Sie sich, dass der Protokollstream mit bestimmten Änderungen auf Datensatzebene gefüllt ist.	AWS Mainframe-Entwickler
Validieren Sie die Anzahl in der Zieldatenbank.	Überwachen Sie die Apply Engine auf die Anzahl der Datensätze.	Präzises Linux
Validieren Sie die Anzahl der Datensätze und Datensätze in der Zieldatenbank.	Fragen Sie die Zieldaten bank ab, um die Anzahl der Datensätze und Datensätze zu überprüfen.	Allgemeines AWS

Zugehörige Ressourcen

- VSAM z/OS (Genauige Dokumentation)
- Engine anwenden (präzise Dokumentation)
- Replikator-Engine (genaue Dokumentation)
- Der Protokollstream (IBM-Dokumentation)

Zusätzliche Informationen

Beispiel für eine Konfigurationsdatei

Dies ist ein Beispiel für eine Konfigurationsdatei für einen Protokollstream, bei dem die Quellumgebung ein Mainframe und die Zielumgebung Amazon MSK ist:

```
 -- JOBNAME -- PASS THE SUBSCRIBER NAME
 -- REPORT  progress report will be produced after "n" (number) of Source records
processed.

 JOBNAME VSMTOKFK;
 --REPORT EVERY 100;
 -- Change Op has been ‘I’ for insert, ‘D’ for delete , and ‘R’ for Replace. For RDS
it is 'U' for update
 -- Character Encoding on z/OS is Code Page 1047, on Linux and UNIX it is Code Page
819 and on Windows, Code Page 1252
 OPTIONS
 CDCOP('I', 'U', 'D'),
 PSEUDO NULL = NO,
 USE AVRO COMPATIBLE NAMES,
 APPLICATION ENCODING SCHEME = 1208;

 --       SOURCE DESCRIPTIONS

 BEGIN GROUP VSAM_SRC;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       TARGET DESCRIPTIONS

 BEGIN GROUP VSAM_TGT;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       SOURCE DATASTORE (IP & Publisher name)

 DATASTORE cdc://10.81.148.4:2626/vsmcdct/VSMTOKFK
 OF VSAMCDC
 AS CDCIN
 DESCRIBED BY GROUP VSAM_SRC ACCEPT ALL;

 --       TARGET DATASTORE(s) - Kafka and topic name

 DATASTORE 'kafka:///MSKTutorialTopic/key'
 OF JSON
```

```
  AS CDCOUT
  DESCRIBED BY GROUP VSAM_TGT FOR INSERT;

  --       MAIN SECTION

  PROCESS INTO
  CDCOUT
  SELECT
  {
  SETURL(CDCOUT, 'kafka:///MSKTutorialTopic/key')
  REMAP(CDCIN, account_file, GET_RAW_RECORD(CDCIN, AFTER), GET_RAW_RECORD(CDCIN,
 BEFORE))
  REPLICATE(CDCOUT, account_file)
  }
  FROM CDCIN;
```

Beispiel für Schlüsselpaar

Dieses Beispiel zeigt, wie Sie die JCL ausführen, um das Schlüsselpaar zu generieren:

```
//SQDUTIL EXEC PGM=SQDUTIL //SQDPUBL DD DSN=&USER..NACL.PUBLIC, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPKEY DD DSN=&USER..NACL.PRIVATE, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPARMS DD  keygen //SYSPRINT DD SYSOUT= //SYSOUT DD SYSOUT=* //
SQDLOG DD SYSOUT=* //*SQDLOG8 DD DUMMY
```

Modernisieren Sie die Mainframe-Ausgabeverwaltung in AWS mithilfe von OpenText Micro Focus Enterprise Server und LRS PageCenterX

Erstellt von Shubham Roy (AWS), Abraham Rondon (Micro Focus) und Guy Tucker (Levi, Ray und Shoup Inc)

Umgebung: PoC oder Pilotprojekt	Quelle: IBM Mainframe	Ziel: AWS
R-Typ: Plattformwechsel	Workload: IBM	Technologien: Mainframe; Migration; Modernisierung
AWS-Services: AWS Managed Microsoft AD; Amazon EC2; Amazon FSx für Windows File Server; Amazon RDS; AWS Mainframe Modernization		

Übersicht

Durch die Modernisierung Ihres Mainframe-Ausgabemanagements können Sie Kosteneinsparungen erzielen, die technische Belastung durch die Wartung älterer Systeme verringern und die Ausfallsicherheit und Agilität durch DevOps und cloudnative Technologien von Amazon Web Services (AWS) verbessern. Dieses Muster zeigt Ihnen, wie Sie Ihre geschäftskritischen Mainframe-Ausgabeverwaltungs-Workloads in der AWS Cloud modernisieren. Das Muster verwendet OpenText Micro Focus Enterprise Server als Laufzeit für eine modernisierte Mainframe-Anwendung mit Bol, Ray & Shoup, Inc. (LRS) VPSX/MFI (Micro Focus Interface) als Druckserver und LRS PageCenterX als Archivserver. LRS PageCenterX bietet Lösungen zur Ausgabeverwaltung zum Anzeigen, Indizieren, Suchen, Archivieren und Sichern des Zugriffs auf Geschäftsausgaben.

Das Muster basiert auf dem Ansatz der Mainframe-Modernisierung des Plattformwechsels. Mainframe-Anwendungen werden von AWS Mainframe Modernization auf Amazon Elastic Compute Cloud (Amazon EC2) migriert. Mainframe-Ausgabeverwaltungs-Workloads werden zu Amazon

EC2 migriert, und eine Mainframe-Datenbank, wie IBM Db2 für z/OS, wird zu Amazon Relational Database Service (Amazon RDS) migriert. Der LRS Directory Integration Server (LRS/DIS) arbeitet mit AWS Directory Service for Microsoft Active Directory für die Authentifizierung und Autorisierung von Ausgabemanagement-Workflows.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Mainframe-Ausgabeverwaltungs-Workload.
- Grundlegendes Wissen über die Neuerstellung und Bereitstellung einer Mainframe-Anwendung, die auf OpenText Micro Focus Enterprise Server ausgeführt wird. Weitere Informationen finden Sie im Datenblatt zu Enterprise Server in der OpenText Micro-Focus-Dokumentation.
- Grundlegendes Wissen zu Lösungen und Konzepten für den LRS-Clouddruck. Weitere Informationen finden Sie unter Output Modernization in der LRS-Dokumentation.
- Micro Focus Enterprise Server-Software und -Lizenz. Weitere Informationen erhalten Sie von OpenText Micro Focus sales .
- Software und Lizenzen für LRS VPSX/MFI, LRS PageCenterX, LRS/Queue und LRS/DIS. Weitere Informationen erhalten Sie von LRS . Sie müssen die Hostnamen der EC2-Instances angeben, auf denen die LRS-Produkte installiert werden.

Hinweis: Weitere Informationen zu Konfigurationsüberlegungen für Mainframe-Ausgabeverwaltung s-Workloads finden Sie unter Überlegungen im Abschnitt Zusätzliche Informationen dieses Musters.

Produktversionen

- OpenText Micro Focus Enterprise Server 8.0 oder höher
- LRS VPSX/MFI
- LRS PageCenterX V1R3 oder höher

Architektur

Quelltechnologie-Stack

- Betriebssystem – IBM z/OS
- Programmiersprache – Allgemeine Geschäftssprache (COBOL), Job Control Language (JCL) und Customer Information Control System (CICS)
- Datenbank – IBM Db2 für z/OS, IBM Information Management System (IMS)-Datenbank und Virtual Storage Access Method (VSAM)
- Sicherheit – Ressourcenzugriffskontrolleinrichtung (RACF), CA Top Secret für z/OS und Access Control Einrichtung 2 (ACF2)
- Druck- und Archivlösungen – IBM Mainframe z/OS-Ausgabe und Druckprodukte (IBM Infoprint Server für z/OS, LRS und CA Deliver) und Archivierungslösungen (CA Deliver, ASG Mobius oder CA Bundle)

Quellarchitektur

Das folgende Diagramm zeigt eine typische aktuelle Zustandsarchitektur für eine Mainframe-Ausgabeverwaltungs-Workload.

Das Diagramm zeigt den folgenden Workflow:

1. Benutzer führen Geschäftstransaktionen auf einem System des Engagements (SoE) durch, das auf einer in COBOL geschriebenen IBM CICS-Anwendung basiert.
2. Die SoE ruft den Mainframe-Service auf, der die Geschäftstransaktionsdaten in einer system-of-records (SoR)-Datenbank wie IBM Db2 für z/OS aufzeichnet.
3. Die SoR behält die Geschäftsdaten aus der SoE bei.
4. Der Batch-Auftrag-Scheduler initiiert einen Batch-Auftrag, um die Druckausgabe zu generieren.
5. Der Batch-Auftrag extrahiert Daten aus der Datenbank. Es formatiert die Daten entsprechend den Geschäftsanforderungen und generiert dann Geschäftsausgaben wie Abrechnungen, Ausweise oder Kreditauszüge. Schließlich leitet der Batch-Auftrag die Ausgabe an die Ausgabeverwaltung weiter, um die Ausgabe basierend auf den Geschäftsanforderungen zu formatieren, zu veröffentlichen und zu speichern.
6. Die Ausgabeverwaltung erhält die Ausgabe vom Batch-Auftrag. Die Ausgabeverwaltung indiziert, ordnet und veröffentlicht die Ausgabe an einem bestimmten Ziel im Ausgabeverwaltungssystem, z. B. LRS PageCenter-X-Lösungen (wie in diesem Muster gezeigt) oder CA View.
7. Benutzer können die Ausgabe anzeigen, suchen und abrufen.

Zieltechnologie-Stack

- Betriebssystem – Windows Server läuft auf Amazon EC2
- Datenverarbeitung – Amazon EC2
- Speicher – Amazon Elastic Block Store (Amazon EBS) und Amazon FSx für Windows File Server
- Programmiersprache – COBOL, JCL und CICS
- Datenbank – Amazon RDS
- Sicherheit – AWS Managed Microsoft AD
- Drucken und Archivieren – Lösung für LRS Printing (VPSX) und Archive (PageCenterX) in AWS
- Mainframe-Laufzeitumgebung – OpenText Micro Focus Enterprise Server

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für eine Mainframe-Ausgabeverwaltungs-Workload, die in der AWS Cloud bereitgestellt wird.

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Job-Scheduler initiiert einen Batch-Job, um Ausgaben wie Abrechnungen, Ausweise oder Kreditanweisungen zu erstellen.
2. Der Mainframe-Batch-Auftrag (auf Amazon EC2 umgestellt) verwendet die OpenText Micro Focus Enterprise Server-Laufzeit, um Daten aus der Anwendungsdatenbank zu extrahieren, Geschäftslogik auf die Daten anzuwenden und die Daten zu formatieren. Anschließend werden die Daten mithilfe des OpenText Micro Focus Drucker-Ausgangsmoduls an ein Ausgabeziel gesendet (OpenText Micro Focus-Dokumentation).
3. Die Anwendungsdatenbank (eine SoR, die auf Amazon RDS ausgeführt wird) behält Daten für die Druckausgabe bei.
4. Die LRS-VPSX/MFI-Ausgabelösung wird auf Amazon EC2 bereitgestellt und ihre Betriebsdaten werden in Amazon EBS gespeichert. LRS VPSX/MFI verwendet den TCP/IP-basierten LRS/Queue-Übertragungsagenten, um Ausgabedaten über die OpenText Micro Focus JES Print Exit API zu sammeln.

   LRS VPSX/MFI führt eine Datenvorverarbeitung durch, z. B. EBCDIC-ASCII-Übersetzung. Es erledigt auch komplexere Aufgaben, einschließlich der Konvertierung von Mainframe-exklusiven

Datenströmen wie IBM Advanced Function microSD (AFP) und Xerox Line Conditioned Data Stream (S) in häufigere Anzeige- und Druckdatenströme wie Druckerbefehlssprache (PCL) und PDF.

Während des Wartungsfensters von LRS PageCenterX behält LRS VPSX/MFI die Ausgabewarteschlange bei und dient als Backup für die Ausgabewarteschlange. LRS VPSX/MFI verbindet und sendet Ausgaben an LRS PageCenterX unter Verwendung des LRS/Queue-Protokolls. LRS/Queue führt einen Austausch sowohl der Bereitschaft als auch des Abschlusses für die Aufträge durch, um sicherzustellen, dass die Datenübertragung erfolgt.

Hinweise:

Weitere Informationen zu Druckdaten, die von OpenText Micro Focus Print Exit an LRS/Queue- und LRS-VPSX/MFI-unterstützte Mainframe-Batch-Mechanismen übergeben werden, finden Sie unter Druckdatenerfassung im Abschnitt Zusätzliche Informationen.

LRS VPSX/MFI kann Zustandsprüfungen auf Druckerflottenebene durchführen. Weitere Informationen finden Sie unter Zustandsprüfungen für Druckerflotten im Abschnitt Zusätzliche Informationen dieses Musters.

5. Die LRS PageCenter-X-Ausgabeverwaltungslösung wird auf Amazon EC2 bereitgestellt und ihre Betriebsdaten werden in Amazon FSx für Windows File Server gespeichert. LRS PageCenterX bietet ein zentrales Berichtsverwaltungssystem aller in LRS PageCenterX importierten Dateien zusammen mit allen Benutzern, die auf die Dateien zugreifen können. Benutzer können bestimmte Dateiinhalte anzeigen oder Suchen über mehrere Dateien hinweg nach Übereinstimmungskriterien durchführen.

   Die LRS/NetX-Komponente ist ein Multi-Thread-Webanwendungsserver, der eine gemeinsame Laufzeitumgebung für die LRS PageCenter-X-Anwendung und andere LRS-Anwendungen bereitstellt. Die LRS/Web Connect-Komponente ist auf Ihrem Webserver installiert und stellt einen Konnektor vom Webserver zum LRS/NetX-Webanwendungsserver bereit.
6. LRS PageCenterX bietet Speicher für Dateisystemobjekte. Die Betriebsdaten von LRS PageCenterX werden in Amazon FSx für Windows File Server gespeichert.
7. Authentifizierung und Autorisierung der Ausgabeverwaltung werden von AWS Managed Microsoft AD mit LRS/DIS durchgeführt.

Hinweis: Die Ziellösung erfordert in der Regel keine Anwendungsänderungen, um Mainframe-Formatierungssprachen wie IBM AFP oder XeroxS zu berücksichtigen.

AWS-Infrastrukturarchitektur

Das folgende Diagramm zeigt eine hochverfügbare und sichere AWS-Infrastrukturarchitektur für eine Mainframe-Ausgabeverwaltungs-Workload.

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Scheduler initiiert den Batch-Prozess und wird auf Amazon EC2 über mehrere Availability Zones für hohe Verfügbarkeit (HA) bereitgestellt.

   Hinweis: Dieses Muster deckt die Implementierung des Batch-Schedulers nicht ab. Weitere Informationen zur Implementierung finden Sie in der Dokumentation zum Softwareanbieter für Ihren Scheduler.

2. Der Mainframe-Batch-Auftrag (in einer Programmiersprache wie JCL oder COBOL geschrieben) verwendet die Kerngeschäftslogik, um Druckausgaben wie Abrechnungen, Ausweise und Kreditanweisungen zu verarbeiten und zu generieren. Der Batch-Auftrag wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt. Es verwendet die OpenText Micro Focus Print Exit API, um die Druckausgabe zur Datenvorverarbeitung an LRS VPSX/MFI weiterzuleiten.
3. Der LRS-VPSX/MFI- Druckserver wird auf Amazon EC2 über zwei Availability Zones für HA bereitgestellt (redundantes Paar aus aktivem Standby). Es verwendet Amazon EBS als Betriebsdatenspeicher. Der Network Load Balancer führt eine Zustandsprüfung für die LRS-VPSX/MFI-EC2-Instances durch. Wenn sich eine aktive Instance in einem fehlerhaften Zustand befindet, leitet der Load Balancer den Datenverkehr an Hot Standby-Instances in der anderen Availability Zone weiter. Die Druckanforderungen werden in der LRS-Auftragswarteschlange lokal in jeder der EC2-Instances gespeichert. Im Falle eines Fehlers muss eine ausgefallene Instance neu gestartet werden, bevor die LRS-Services die Verarbeitung der Druckanforderung fortsetzen können.

   Hinweis: LRS VPSX/MFI kann auch Zustandsprüfungen auf Druckerflottenebene durchführ en. Weitere Informationen finden Sie unter Zustandsprüfungen für Druckerflotten im Abschnitt Zusätzliche Informationen dieses Musters.

4. Die LRS PageCenter-X-Ausgabeverwaltung wird auf Amazon EC2 über zwei Availability Zones für HA bereitgestellt (redundantes Paar aus aktivem Standby). Es verwendet Amazon FSx for Windows File Server als Betriebsdatenspeicher. Wenn sich eine aktive Instance in einem fehlerhaften Zustand befindet, führt der Load Balancer eine Zustandsprüfung der LRS PageCenter-X-EC2-Instances durch und leitet den Datenverkehr an Standby-Instances in der anderen Availability Zone weiter.
5. Ein Network Load Balancer stellt einen DNS-Namen bereit, um den LRS-VPSX/MFI-Server in LRS PageCenterX zu integrieren.

   Hinweis: LRS PageCenterX unterstützt einen Layer 4 Load Balancer.

6. LRS PageCenterX verwendet Amazon FSx für Windows File Server als Betriebsdatenspeicher, der in zwei Availability Zones für HA bereitgestellt wird. LRS PageCenterX versteht nur Dateien, die sich in der Dateifreigabe befinden, nicht in einer externen Datenbank.
7. AWS Managed Microsoft AD wird mit LRS/DIS verwendet, um die Authentifizierung und Autorisierung von Ausgabemanagement-Workflows durchzuführen. Weitere Informationen finden Sie unter Ausgabeauthentifizierung und -autorisierung drucken im Abschnitt Zusätzliche Informationen.

Tools

AWS-Services

- AWS Directory Service for Microsoft Active Directory ermöglicht es Ihren verzeichnisfähigen Workloads und AWS-Ressourcen, Microsoft Active Directory in der AWS Cloud zu verwenden.
- Amazon Elastic Block Store (Amazon EBS) stellt Volumes für die Speicherung auf Blockebene für die Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2)-Instances bereit.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon EC2-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Network Load Balancer .

- Amazon FSx bietet Dateisysteme, die branchenübliche Konnektivitätsprotokolle unterstützen und eine hohe Verfügbarkeit und Replikation über AWS-Regionen hinweg bieten. Dieses Muster verwendet Amazon FSx für Windows File Server.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.

Andere Tools

- Die LRS PageCenter-X-Software bietet eine skalierbare Lösung für die Verwaltung von Dokumenten- und Berichten, mit der Benutzer durch automatisierte Indizierung, Verschlüsselung und erweiterte Suchfunktionen den maximalen Nutzen aus Informationen ziehen können.
- LRS VPSX/MFI (Micro Focus Interface), das von LRS und OpenText Micro Focus entwickelt wurde, erfasst die Ausgabe aus einem JES-Spool von OpenText Micro Focus Enterprise Server und liefert sie zuverlässig an ein bestimmtes Druckziel.
- LRS/Queue ist ein Übertragungsagent, der TCP/IP-basiert ist. LRS VPSX/MFI verwendet LRS/Queue, um Druckdaten über die OpenText Micro-Focus-JES-Programmierschnittstelle zum Beenden zu sammeln oder zu erfassen.
- LRS Directory Integration Server (LRS/DIS) wird für die Authentifizierung und Autorisierung während des Druck-Workflows verwendet.
- OpenText Micro Focus Enterprise Server ist eine Anwendungsbereitstellungsumgebung für Mainframe-Anwendungen. Es bietet die Laufzeitumgebung für Mainframe-Anwendungen, die mithilfe einer beliebigen Version von OpenText Micro Focus Enterprise Developer migriert oder erstellt werden.

Polen

Einrichten der OpenText Micro-Focus-Laufzeit und Bereitstellen einer Mainframe-Batchanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Laufzeit ein und stellen Sie eine Demoanwendung bereit.	Um OpenText Micro Focus Enterprise Server auf Amazon EC2 einzurichten und die OpenText Micro Focus- BankDemo	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Demonstrationsanwendung bereitzustellen, folgen Sie den Anweisungen im AWS Mainframe Modernization-Benutzerhandbuch. Die BankDemo Anwendung ist eine Mainframe-Batch-Anwendung, die die Druckausgabe erstellt und dann initiiert.	

Einrichten eines LRS- Druckservers auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon EC2-Windows-Instance.	Um eine Amazon EC2-Windows-Instance zu starten, folgen Sie den Anweisungen in Schritt 1: Starten einer Instance in der Amazon EC2Dokumentation. Verwenden Sie denselben Hostnamen, den Sie für Ihre LRS-Produktlizenz verwendet haben. Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS VPSX/MFI erfüllen: • CPU – Dual Core • RAM – 16 GB • Laufwerk – 500 GB	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Minimale EC2-Instance – `m5.xlarge` • Betriebssystem – Windows • Software – Internet Information Services (IIS) oder Apache Hinweis: Die oben genannten Hardware- und Softwarea nforderungen sind für eine kleine Druckerflotte (etwa 500-1000) vorgesehen. Um alle Anforderungen zu erfüllen, wenden Sie sich an Ihre LRS- und AWS-Kontakte. 1. Vergewissern Sie sich beim Erstellen Ihrer Windows-Instance, dass der EC2-Hostname mit dem Hostnamen übereinst immt, der für die LRS-Produ ktlizenz verwendet wird. 2. Stellen Sie eine Verbindung zu Ihrer EC2-Instance her, indem Sie den Anweisung en unter Schritt 2: Herstelle n einer Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation folgen. 3. Suchen und öffnen Sie im Windows-Startmenü Server Manager .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie in Server Manager Dashboard , Schnellstart , Rollen und Features hinzufügen und dann Serverrollen aus. 5. Wählen Sie unter Serverrollen WebServer (IIS) und dann Anwendungsentwicklung aus. 6. Aktivieren Sie in Application Development das Kontrollkästchen CGI. 7. Um CGI zu installieren, folgen Sie den Anweisungen im Windows Server Manger Assistenten zum Hinzufügen von Rollen und Funktionen. 8. Öffnen Sie Port 5500 in der Windows-Firewall der EC2-Instance für die LRS/Queue-Kommunikation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS VPSX/MFI auf der EC2-Instance.	1. Stellen Sie eine Verbindung zu Ihrer EC2- Instance her. 2. Öffnen Sie den Link zur Produkt-Downloadseite in der LRS-E-Mail-Nachricht, die Sie erhalten haben sollten. Hinweis: LRS-Produkte werden durch elektronische Dateiübertragung (EFT) verteilt. 3. Laden Sie LRS VPSX/MFI herunter und entpacken Sie die Datei (Standardordner: `c:\LRS`). 4. Um LRS VPSX/MFI zu installieren, starten Sie den LRS Product Installer aus dem entpackten Ordner. 5. Wählen Sie im Menü Features auswählen die Option VPSX Server und dann Weiter aus, um den Installationsprozess zu starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/Queue.	1. Stellen Sie eine Verbindung zu Ihrer OpenText Micro Focus Enterprise Server-EC2-Instance her. 2. Öffnen Sie den Link zur LRS-Produkt-Downloadseite in der LRS-E-Mail-Nachricht, die Sie erhalten sollten, laden Sie LRS/Queue herunter und entpacken Sie dann die Datei. 3. Navigieren Sie zu dem Speicherort, an den Sie die Dateien heruntergeladen haben, und starten Sie dann den LRS-Produktinstallationsprogramm, um LRS/Queue zu installieren. 4. Folgen Sie den Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsprozess abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	Das LRS/DIS-Produkt ist häufig in der LRS-VPSX-Installation enthalten. Wenn LRS/DIS jedoch nicht zusammen mit LRS VPSX installiert wurde, führen Sie die folgenden Schritte aus, um es zu installieren: 1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her. 2. Öffnen Sie den Link zur LRS-Produkt-Downloadseite in der LRS-E-Mail-Nachricht, die Sie erhalten hätten sollten, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Navigieren Sie zu dem Speicherort, an den Sie die Dateien heruntergeladen haben, und starten Sie dann den LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer LRS Misc Tools , wählen Sie LRS DIS und dann Next aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationspro	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gramm, um den Installat ionsprozess abzuschließen.	
Erstellen Sie eine Zielgruppe.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen einer Zielgrupp e für Ihren Network Load Balancer folgen. Wenn Sie die Zielgruppe erstellen, registrie ren Sie die LRS-VPSX/MFI-EC2-Instance als Ziel: 1. Wählen Sie auf der Seite Gruppendetails angeben für Zieltyp auswählen die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port 5500 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instances die LRS-VPSX/ MFI-EC2-Instance aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer .	Um den Network Load Balancer zu erstellen, folgen Sie den Anweisungen in der Elastic Load Balancing-Dokumentation. Ihr Network Load Balancer leitet den Datenverkehr von OpenText Micro Focus Enterprise Server an die LRS-VPSX/MFI-EC2-Instance weiter. Wenn Sie den Network Load Balancer erstellen, wählen Sie die folgenden Werte auf der Seite Listener und Routing aus: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port 5500 aus. 3. Wählen Sie für Standardaktion die Option Weiterleiten an für die Zielgruppe aus, die Sie zuvor erstellt haben.	Cloud-Architekt

Micro OpenText Focus Enterprise Server mit LRS/Queue und LRS VPSX/MFI integrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Micro Focus Enterprise Server für die LRS/Queue-Integration.	1. Stellen Sie eine Verbindung zu Ihrer OpenText Micro Focus Enterprise Server EC2-Instance her, indem	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Anweisungen in der Amazon EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Start menüdie Micro OpenText Focus Enterprise Server Administration-Benutzeroberfläche. 3. Wählen Sie in der Menüleiste NATIV aus. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO für Ihre Enterprise-Server-Region aus. 5. Scrollen Sie im linken Navigationsbereich von Allgemein nach unten zum Abschnitt Zusätzliche, um die Umgebungsvariablen (`LRSQ_ADDRESS` , `LRSQ_PORT` , `LRSQ_COMMAND`) so zu konfigurieren, dass sie auf LRSQ zeigen. • Geben Sie für LRSQ_ADDRESS die IP-Adresse oder den DNS-Namen des Network Load Balancer sein, den Sie zuvor erstellt haben. • Geben Sie für LRSQ_PORT VPSX	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	LRSQ Listener Port (5500) ein. • Geben Sie für LRSQ_COMMAND den Pfadspeicherort der ausführbaren LRSQ-Datei ein. Hinweis: LRS unterstützt derzeit ein maximales Zeichenlimit von 50 für DNS-Namen. Wenn Ihr DNS-Name länger als 50 Zeichen ist, können Sie die IP-Adresse des Network Load Balancer sals Alternative verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie OpenText Micro Focus Enterprise Server für die LRS-VPSX/MFI-Integration.	1. Kopieren Sie den `VPSX_MFI_R2` Ordner aus dem LRS-VPSX/MFI-Installationsprogramm in den Micro-Focus-Enterprise-Server-Speicherort unter `C:\BANKDEMO\print` . 2. Stellen Sie eine Verbindung zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen in der Amazon EC2-Dokumentation folgen. 3. Öffnen Sie im Windows-Start menüdie Micro Focus Enterprise Server Administration-Benutzeroberfläche. 4. Wählen Sie in der Menüleiste NATIV aus. 5. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 6. Wählen Sie unter BANKDEMO die Option JES aus. 7. Fügen Sie unter JES-Programmpfad den `DLL(VPSX_MFI_R2)` Pfad aus hinzu`C:\BANKDEMO\print` .	Cloud-Architekt

Einrichten der Druckwarteschlange und der Druckbenutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie das OpenText Micro Focus Print Exit-Modul dem Micro Focus Enterprise Server-Stapeldruck Serverausführungsprozess zu.	1. Stellen Sie eine Verbindung zu Ihrer OpenText Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen in der Amazon EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Start menüdie Micro OpenText Focus Enterprise Server Administration-Benutzeroberfläche. 3. Wählen Sie in der Menüleiste NATIV aus. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 5. Wählen Sie unter BANKDEMO die Option JES aus und scrollen Sie nach unten zu Drucker. 6. Ordnen Sie unter Drucker das OpenText Micro Focus Print Exit-Modul (LRSPRTE6 für Batch) dem OpenText Micro Focus Enterprise Server-Batch-Computer Server Execution Process (SEP) zu. Dies ermöglicht das Ausgabe-Routing an LRS VPSX/MFI.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zur Konfiguration finden Sie unter Verwenden des - Ausgangs in der OpenText Micro-Focus-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ausgabewarteschlange in LRS VPSX/MFI und integrieren Sie sie in LRS PageCenterX.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her. 2. Öffnen Sie im Windows-Start menüdie VPSX-Webschnittstelle . 3. Wählen Sie im Navigationsbereich Drucker aus. 4. Wählen Sie Hinzufügen und dann Drucker hinzufügen aus. 5. Geben Sie auf der Seite Druckerkonfiguration für Druckername Lokal ein. 6. Geben Sie für VPSX-ID VPS1 ein. 7. CommTypeWählen Sie für TCPIP/LRSQ aus. 8. Geben Sie für Host/IP-Adresse die IP-Adresse des Network Load Balancer sein, der den LRS PageCenter-X-EC2-Instances zugrunde liegt. 9. Geben Sie für Remote-Port 5800 ein. 10. Geben Sie für Remote-Warteschlange den Namen des LRS PageCenter-X-Dokumentordners ein, in dem die Ausgabe gespeichert wird.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie Hinzufügen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Druckbenutzer in LRS VPSX/MFI.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her. 2. Öffnen Sie im Windows-Start menüdie VPSX-Webschnittstelle . 3. Wählen Sie im Navigationsbereich Sicherheit und dann Benutzer aus. 4. Wählen Sie in der Spalte Benutzername die Option admin und dann Kopieren aus. 5. Geben Sie im Fenster Benutzerprofilverwaltung für Benutzername einen Benutzernamen ein (z. B. PrintUser). 6. Geben Sie unter Beschreibung eine kurze Beschreibung ein (z. B. Benutzer für Testdruck). 7. Wählen Sie Aktualisieren. Dadurch wird ein Druckbenutzer erstellt (z. B. PrintUser). 8. Wählen Sie im Navigationsbereich unter Benutzer den neuen Benutzer aus, den Sie erstellt haben. 9. Wählen Sie im Menü Befehl die Option Sicherheit aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Wählen Sie auf der Seite Sicherheitsregeln alle entsprechenden Optionen für Druckersicherheit und Auftragssicherheit aus und wählen Sie dann Speichern aus. 11. Um Ihren neuen Druckbenutzer zur Administrator gruppehinzuzufügen, wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 12. Fügen Sie im Fenster Sicherheitskonfiguration Ihren neuen Druckbenutzer zur Spalte Administrator hinzu.	

Einrichten eines LRS PageCenter-X-Servers auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon EC2-Windows-Instance.	Starten Sie eine Amazon EC2-Windows-Instance, indem Sie den Anweisungen unter Schritt 1: Starten einer Instance in der Amazon EC2Dokumentation folgen. Verwenden Sie denselben Hostnamen, den Sie für Ihre LRS-Produktlizenz verwendet haben.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS PageCenterX erfüllen: • CPU – Dual Core • RAM – 16 GB • Laufwerk – 500 GB • Minimale EC2-Instance – `m5.xlarge` • Betriebssystem – Windows • Software – IIS oder Apache Hinweis: Die oben genannten Hardware- und Softwarea nforderungen sind für eine kleine Druckerflotte (etwa 500–1000) vorgesehen. Um alle Anforderungen zu erfüllen, wenden Sie sich an Ihre LRS- und AWS-Kontakte. 1. Vergewissern Sie sich beim Erstellen Ihrer Windows-Instance, dass der EC2-Hostname mit dem Hostnamen übereinst immt, der für die LRS-Produ ktlizenz verwendet wird. 2. Stellen Sie eine Verbindung zu Ihrer EC2-Instance her, indem Sie den Anweisung en in der Amazon EC2-Dokumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Suchen und öffnen Sie im Windows-Startmenü Server Manager . 4. Wählen Sie im Server Manager Dashboard , Schnellstart , Rollen und Features hinzufügen und dann Serverrollen aus. 5. Wählen Sie unter Serverrol len WebServer (IIS) und dann Anwendungsentwickl ung aus. 6. Aktivieren Sie unter Anwendungsentwicklung das Kontrollkästchen CGI. 7. Um CGI zu installieren, folgen Sie den Anweisung en im Windows Server Manger Assistenten zum Hinzufügen von Rollen und Funktionen. 8. Öffnen Sie Port 5800 für eingehenden TCP/IP-Da tenverkehr in der Windows-Firewall der EC2-Instance. LRS VPSX verwendet das TCPIP/LRSQ-Protokoll auf dem 5800-Port, um mit LRS PageCenterX zu kommunizi eren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS PageCenterX auf der EC2-Instance.	1. Stellen Sie eine Verbindung zu Ihrer EC2- Instance her. 2. Öffnen Sie den Link zur Produkt-Downloadseite in der LRS-E-Mail-Nachricht, die Sie erhalten haben sollten. Hinweis: LRS-Produkte werden durch elektronische Dateiübertragung (EFT) verteilt. 3. Laden Sie LRS PageCenterX herunter und entpacken Sie die Datei (Standard ordner: `c:\LRS`). 4. Um LRS PageCenterX zu installieren, starten Sie den LRS Product Installer aus dem entpackten Ordner. 5. Wählen Sie im Menü Features auswählen die Option PageCenterX und dann Weiter aus, um den Installationsprozess zu starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	Das LRS/DIS-Produkt ist häufig in der LRS-VPSX-Installation enthalten. Wenn LRS/DIS jedoch nicht zusammen mit LRS VPSX installiert wurde, führen Sie die folgenden Schritte aus, um es zu installieren: 1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenterX-EC2-Instance her. 2. Öffnen Sie den Link zur LRS-Produkt-Downloadseite in der LRS-E-Mail, die Sie erhalten hätten sollten, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Navigieren Sie zu dem Speicherort, an den Sie die Dateien heruntergeladen haben, und starten Sie dann den LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer LRS Misc Tools , wählen Sie LRS DIS und dann Next aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsprozess abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen einer Zielgruppe für Ihren Network Load Balancer folgen. Wenn Sie die Zielgruppe erstellen, registrieren Sie die LRS PageCenter-X-EC2-Instance als Ziel: 1. Wählen Sie auf der Seite Gruppendetails angeben für Zieltyp auswählen die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port 5800 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instances die LRS PageCenter-X-EC2-Instance aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer .	Um den Network Load Balancer zu erstellen, folgen Sie den Anweisungen in der Elastic Load Balancing-Dokumentation. Ihr Network Load Balancer leitet den Datenverkehr von LRS VPSX/MFI an die LRS PageCenter-X-EC2-Instance weiter. Wenn Sie den Network Load Balancer erstellen, wählen Sie auf der Seite Listeners und Routing die folgenden Werte aus: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port 5800 aus. 3. Wählen Sie für Standarda ktion die Option Weiterleiten an für die Zielgruppe aus, die Sie zuvor erstellt haben.	Cloud-Architekt

Einrichten von Ausgabeverwaltungsfunktionen in LRS PageCenterX

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Importfun ktion in LRS PageCenterX.	Sie können die Funktion LRS PageCenterX Import verwenden, um die Ausgaben, die auf LRS PageCenterX landen, anhand von Kriterien	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wie Auftragsname oder Formular-ID zu erkennen. Anschließend können Sie die Ausgaben an bestimmte Ordner in LRS PageCenterX weiterleiten. Gehen Sie wie folgt vor, um die Importfunktion zu aktiviere n: 1. Stellen Sie eine Verbindun g zu Ihrer LRS PageCenter-X-EC2-Instance her, indem Sie den Anweisungen in der Amazon EC2Dokume ntation folgen. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Ex plorer die Option Admin aus. 4. Wählen Sie auf der Seite Konfiguration die Option Erweitert, Parameter importieren aus. 5. Aktivieren Sie im Abschnitt Importparameter das Kontrollkästchen Erweiterter Import. 6. Um die Änderungen zu bestätigen, wählen Sie Aktualisieren aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Richtlinie zur Aufbewahrung von Dokumenten.	LRS PageCenterX verwendet eine Richtlinie zur Aufbewahrung von Dokumenten, um zu entscheiden, wie lange ein Dokument in LRS PageCenterX aufbewahrt werden soll. Gehen Sie wie folgt vor, um die Richtlinie zur Aufbewahrung von Dokumenten zu konfigurieren: 1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenter-X-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Explorer die Option Admin aus. 4. Wählen Sie auf der Seite Admin die Option Archivgruppenliste/Allgemeiner Administrator und dann Aufbewahrungsrichtlinie aus. 5. Wählen Sie im Abschnitt Aufbewahrungsrichtlinie die Option Hinzufügen aus, um eine Aufbewahrungsrichtlinie zu erstellen. 6. Geben Sie auf der Seite Informationen zur	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufbewahrungsrichtlinie einen Namen für die Aufbewahrungsrichtlinie , eine Beschreibung und einen Aufbewahrungszeitraum für Dokumente ein. 7. Um Ihre Änderungen zu speichern und die Richtlinie zu erstellen, wählen Sie OK aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Regel, um das Ausgabedokument an einen bestimmten Ordner in LRS PageCenterX weiterzul eiten.	In LRS PageCenterX bestimmt Destination den Ordnerpfad, an den die Ausgabe gesendet wird, wenn dieses Ziel durch die Berichtsdefinition aufgerufen wird. Erstellen Sie für dieses Beispiel einen Ordner basierend auf dem Ordner Formular-ID in der Berichtsdefinition und speichern Sie die Ausgabe in diesem Ordner. 1. Stellen Sie eine Verbindun g zu Ihrer LRS PageCenter-X-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Websc hnittstelle . 3. Wählen Sie im Ordner-Ex plorer Admin , Advance Import , Ziel aus. 4. Wählen Sie im Abschnitt Ziel die Option Hinzufüge n aus, um das Formular Zielwartung zu öffnen. 5. Geben Sie im Formular Zielwartung die folgenden Werte ein: • Zielname – Formular • Beschreibung – Beschreibung des Ziels, z. B. Formbasierte Ordnerstruktur	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Zieltyp – Ordner • Ordnerparameter – Ordnerpfad importieren (der Ordnerpfad, der in PageCenterX erstellt wird, wenn das Dokument eintrifft; der Pfad `/Test/&FORM/&IMPORTDATE/&IMPORTTIME` erstellt beispielsweise einen `Test` Basisordner, einen Unterordner basierend auf der Formular-ID `STD`, einen Unterordner basierend auf dem Importdatum und dann einen Unterordner basierend auf der Importzeit) • Dokumentname – Dynamischer Name, der einem Dokument zugewiesen wird, wenn es im Ordner gespeichert wird. 6. Wählen Sie in der Dropdown-Liste eine Aufbewahrungsrichtlinie aus. Wählen Sie beispielsweise Year1 aus, um das Dokument 1 Jahr lang aufzubewahren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Um die Änderungen zu speichern, wählen Sie OK aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Berichtsdefinition.	1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenterX-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Explorer Admin , Advance Import , Berichtsdefinition und dann Hinzufügen aus. 4. Geben Sie auf der Wartungsseite Berichtsdefinition auf der Registerkarte Allgemein den Namen der Berichtsdefinition ein. 5. Auf der Registerkarte Allgemein können Sie unter Felder Auswahlkriterien wie Auftragsname, Formular , Klasse und Autor angeben. Sie könnten beispielsweise den Jobnamen MFIDEMO eingeben. Der Wert Auftragsname ist der Name des Batch-Auftrags, der die Druckausgabe generiert. 6. Wählen Sie auf der Registerkarte Ziel unter Verfügbares Ziel das zuvor erstellte Ziel aus (Formular).	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie Hinzufüge n, um das Form ularziela ls Zugewiesenes Ziel hinzuzufügen. Hinweis: Dieses Beispiel enthält eine Berichtsd efinition, in der eine vom MFIDEMO generierte und an LRS PageCenterX weitergeleitete Ausgabe in der in der Zieldefinition definierten Ordnerstruktur gespeichert wird.	

Einrichten der Authentifizierung und Autorisierung für die Ausgabeverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Managed Microsoft AD-Domain mit Benutzern und Gruppen.	1. Um ein Verzeichnis in AWS Managed Microsoft AD zu erstellen, folgen Sie den Anweisungen unter Erstellen Ihres AWS Managed Microsoft AD-Verzeichnisses. 2. Um eine EC2-Instance (Active Directory Manager) bereitzustellen und Active Directory-Tools zur Verwaltung Ihres AWS Managed Microsoft AD zu installieren, folgen Sie den Anweisungen in Schritt 3:	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellen einer EC2-Instance zur Verwaltung Ihres AWS Managed Microsoft AD. 3. Um eine Verbindung zu Ihrer EC2-Instance herzustellen, folgen Sie den Anweisungen in der Amazon EC2-Dokumentation. Hinweis: Wenn Sie eine Verbindung mit der EC2-Instance herstellen, geben Sie im Fenster Windows-Sicherheit die Administratoranmeldeinformationen für das Verzeichnis ein, das Sie in Schritt 1 erstellt haben. 4. Wählen Sie im Windows-Start menüunter Windows Administrative Tools die Option Active Directory-Benutzer und -Computer aus. 5. Um einen Druckbenutzer in der Active-Directory-Domain zu erstellen, folgen Sie den Anweisungen unter Erstellen eines Benutzers.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbinden Sie die EC2-Instances mit einer AWS Managed Microsoft AD-Domain.	Fügen Sie die Instances LRS VPSX/MFI und LRS PageCenterX EC2 automatisch (Dokumentation zum AWS Knowledge Center) oder manuell (Dokumentation zum AWS Directory Service) zu Ihrer AWS Managed Microsoft AD-Domain hinzu.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und integrieren Sie LRS/DIS mit AWS Managed Microsoft AD für die LRS PageCenterX EC2-Instance.	1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenter-X-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Explorer die Option Admin aus. 4. Wählen Sie auf der Seite Konfiguration im Abschnitt Sicherheitsparameter für Sicherheitstyp LRS/DIS aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie im Windows-Start menüden Ordner PageCenterX, wählen Sie Server Start und dann Server Stop aus. 7. Melden Sie sich bei LRS PageCenterX mit Ihrem Active-Directory-Benutzernamen und -Passwort an.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine Importgruppe, um die Ausgabe von LRS VPSX nach LRS PageCenterX zu importieren.	1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenter-X-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Explorer die Optionen Admin ,Sicherheitsadministrator, Gruppen aus. 4. Wählen Sie im Abschnitt Gruppen die Option Hinzufügen aus, um das Formular Gruppenpräferenz zu öffnen. 5. Geben Sie im Formular Gruppenpräferenz Werte für Gruppenname und Beschreibung ein. 6. Erweitern Sie Allgemeine Optionen und aktivieren Sie dann das Kontrollkästchen Importieren. 7. Um die Änderungen zu speichern, wählen Sie OK aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Importgruppe eine Sicherheitsregel hinzu.	1. Öffnen Sie das Kontextmenü (rechte Maustaste) für die Importgruppe . 2. Wählen Sie Advance und dann Security aus. 3. Wählen Sie im Abschnitt Sicherheit die Option Importieren und aktivieren Sie das Kontrollkästchen Unterordner. 4. Um die Änderungen zu speichern, wählen Sie Anwenden aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzer in LRS PageCenterX, um den Ausgabeimport aus LRS VPSX/MFI durchzuführen.	Wenn Sie einen Benutzer in LRS PageCenterX erstellen , um den Ausgabeimport durchzuführen, sollte der Benutzername mit der VPSX-ID der Druckausgabewartes chlange in LRS VPSX/MFI übereinstimmen. In diesem Beispiel ist die VPSX-ID VPS1. 1. Stellen Sie eine Verbindun g zu Ihrer LRS PageCenter-X-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Ex plorer die Optionen Admin ,Sicherheitsadministrator, Benutzer aus. 4. Wählen Sie Hinzufügen, um das Wartungsformular für Benutzerprofile zu öffnen. 5. Geben Sie unter Benutzerp rofilverwaltung für Benutzername VPS1 ein.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den Benutzer LRS PageCenterX Import der Gruppe Nur importieren hinzu.	Gehen Sie wie folgt vor, um die erforderliche Berechtigung für den Dokumentenimport von LRS VPSX nach LRS PageCenterX bereitzustellen: 1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenter-X-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Explorer die Optionen Admin ,Sicherheitsadministrator, Gruppen aus. 4. Öffnen Sie im Abschnitt Gruppen das Kontextmenü (rechte Maustaste) für die Gruppe Nur importieren und wählen Sie dann Weiter, Sicherheit aus. 5. Wählen Sie auf der Seite Ordnersicherheitsdatensätze (ImportOnly) die Registerkarte Benutzer aus. 6. Wählen Sie auf der Registerkarte Benutzer unter Name die Option Benutzer VPS1 aus der Dropdown-Liste aus und wählen Sie Anwenden aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie LRS/DIS mit AWS Managed Microsoft AD für die LRS-VPSX/MFI-EC2-Instance.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her. 2. Öffnen Sie im Windows-Startmenü die VPSX-Webschnittstelle . 3. Wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 4. Wählen Sie auf der Seite Sicherheitskonfiguration im Abschnitt Sicherheitsparameter für Sicherheitstyp LRS/DIS (External) aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie im Windows-Start menüden Ordner LRS Output Management, wählen Sie Server Start und dann Server Stop aus. 7. Melden Sie sich bei LRS VPSX/MFI mit Ihrem Active-Directory-Benutzernamen und -Passwort an.	Cloud-Architekt

Konfigurieren von Amazon FSx für Windows File Server als Betriebsdatenspeicher für LRS PageCenterX

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Dateisystem für LRS PageCenterX.	Um Amazon FSx for Windows File Server als Betriebsdatenspeicher für LRS PageCenterX in einer Multi-AZ-Umgebung zu verwenden, folgen Sie den Anweisungen in Schritt 1: Erstellen Ihres Dateisystems.	Cloud-Architekt
Ordnen Sie die Dateifreigabe der LRS PageCenter-X-EC2-Instance zu.	Um die im vorherigen Schritt erstellte Dateifreigabe der LRS PageCenter-X-EC2-Instance zuzuordnen, folgen Sie den Anweisungen in Schritt 2: Zuordnen Ihrer Dateifreigabe zu einer EC2-Instance, auf der Windows Server ausgeführt wird.	Cloud-Architekt
Ordnen Sie dem Amazon-FSx-Netzwerkfreigabelaufwerk das LRS PageCenter-X-Kontrollverzeichnis und das Hauptordnerverzeichnis zu.	1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenter-X-EC2-Instance her, indem Sie den Anweisungen in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die PCX-Webschnittstelle . 3. Wählen Sie im Ordner-Explorer die Option Admin ,Konfiguration aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie auf der Seite Konfiguration die Option Verzeichnisse und dann Kontrollverzeichnis aus. 5. Geben Sie unter Kontrollverzeichnisse ein `\\FSx file share DNS name \share\cntl` . 6. Geben Sie unter Master-Ordnerverzeichnis ein `\\FSx file share DNS name \share\mstr` .	

Testen eines Ausgabeverwaltungs-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie eine Batch-Press-Anforderung von der OpenText Micro Focus BankDemo -App aus.	1. Öffnen Sie den 3270-Terminal-Emulator in Ihrer OpenText Micro Focus Enterprise Server EC2-Instance. 2. Stellen Sie eine Verbindung mit der BankDemo App her, indem Sie den Befehl ausführen `connect 127.0.0.1:9278` . 3. Geben Sie in der BankDemo Befehlszeilenschnittstelle für Benutzer-ID B0001 ein. Geben Sie für Passwort	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen nicht leeren Schlüssel ein. 4. Geben Sie für die Option Gedruckte Anweisung(en) anfordern X in die leere Zeile ein. 5. Geben Sie im Abschnitt Anweisung senden nach für Mail Y ein und drücken Sie dann F10.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Druckausgabe in LRS PageCenterX.	1. Stellen Sie eine Verbindung zu Ihrer LRS PageCenter-X-EC2-Instance her, indem Sie den Anweisungen in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie im Windows-Start menüdie PCX-Webschnittstelle . 3. Öffnen Sie im Navigationsbereich den Ordner Test, öffnen Sie den Ordner STD und öffnen Sie dann den Ordner mit dem Ausführungsdatum des Auftrags, z. B. `08-03-2023` (MM-TT-JJJJ). Hinweis: Dies ist dieselbe Ordnerstruktur wie in der Anleitung Erstellen einer Regel, um das Ausgabedokument an einen bestimmten Ordner in LRS PageCenterX weiterzuleiten. 4. Öffnen Sie die `formtest-STD.txt` Datei. Sie können jetzt die Druckausgabe eines Kontoauszugs mit Spalten für Konto-ID, Beschreibung , Datum , Betrag und Saldo sehen. Ein Beispiel	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie im `batch_print_output` Anhang für dieses Muster.	

Zugehörige Ressourcen

- LRS
- Erweiterter Funktionsbereitstellungsdatenstrom (IBM-Dokumentation)
- Line Conditioned Data Stream (S) (Compart-Dokumentation)
- Micro Focus Enterprise Server auf AWS (AWS-Schnellstarts)
- Unterstützung von Enterprise Mainframe Workloads in AWS mit Micro Focus (Blogbeitrag)
- Modernisieren Sie Ihre Mainframe-Workloads für den Onlinedruck auf AWS (AWS Prescriptive Guidance)
- Modernisieren Sie Ihre Mainframe-Stapeldruck-Workloads in AWS (AWS Prescriptive Guidance)

Zusätzliche Informationen

Überlegungen

Während Ihrer Modernisierung können Sie eine Vielzahl von Konfigurationen für Mainframe-Batch- und Online-Prozesse sowie die von ihnen generierte Ausgabe in Betracht ziehen. Die Mainframe-Plattform wurde von jedem Kunden und Anbieter angepasst, der sie mit bestimmten Anforderungen verwendet, die sich direkt auf den Druck auswirken. Beispielsweise könnte Ihre aktuelle Plattform den IBM AFP-Datenstrom oder XeroxS in den aktuellen Workflow integrieren. Darüber hinaus können Mainframe-Wagensteuerzeichen und Kanalbefehlswörter das Aussehen der gedruckten Seite beeinflussen und erfordern möglicherweise eine besondere Handhabung. Im Rahmen des Modernisierungsplanungsprozesses empfehlen wir Ihnen, die Konfigurationen in Ihrer spezifischen Druckumgebung zu bewerten und zu verstehen.

Drucken der Datenerfassung

OpenText Micro Focus Print Exit übergibt die erforderlichen Informationen, damit LRS VPSX/MFI die Spool-Datei effektiv verarbeiten kann. Die Informationen bestehen aus Feldern, die in den relevanten Kontrollblöcken übergeben werden, z. B. den folgenden:

- JOBNAME
- OWNER (USERID)
- DESTINATION
- FORM
- DATENAME
- WRITER

LRS VPSX/MFI unterstützt die folgenden Mainframe-Batch-Mechanismen zur Erfassung von Daten von OpenText Micro Focus Enterprise Server:

- BATCH COBOL- Druck-/Spool-Verarbeitung mit Standard-z/OS-JCL-Anweisungen SYSOUT DD/ OUTPUT.
- BATCH COBOL- Druck-/Spool-Verarbeitung mit Standard-z/OS-JCL-CA-SPOOL-SUBSYS-DD-Anweisungen.
- IMS/COBOL- Druck-/Spool-Verarbeitung über die CBLTDLI-Schnittstelle. Eine vollständige Liste der unterstützten Methoden und Programmierbeispiele finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Zustandsprüfungen für Druckerflotten

LRS VPSX/MFI (LRS LoadX) kann detaillierte Zustandsprüfungen durchführen, einschließlich Geräteverwaltung und Betriebsoptimierung. Die Geräteverwaltung kann Fehler in einem Druckergerät erkennen und die Druckanforderung an einen fehlerfreien Drucker weiterleiten. Weitere Informationen zu detaillierten Zustandsprüfungen für Druckerflotten finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Authentifizierung und Autorisierung drucken

LRS/DIS ermöglicht es LRS-Anwendungen, Benutzer-IDs und Passwörter mithilfe von Microsoft Active Directory oder einem LDAP-Server (Lightweight Directory Access Protocol) zu authentifizieren. Zusätzlich zur grundlegenden Druckautorisierung kann LRS/DIS in den folgenden Anwendungsfällen auch detaillierte Drucksicherheitskontrollen anwenden:

- Verwalten Sie, wer den Druckerauftrag durchsuchen kann.
- Verwalten Sie die Browsing-Ebene der Aufträge anderer Benutzer.

- Verwalten Sie operative Aufgaben, z. B. Sicherheit auf Befehlsebene wie Anhalten oder Freigeben, Bereinigen, Ändern, Kopieren und Umleiten. Die Sicherheit kann entweder durch die Benutzer-ID oder die Gruppe eingerichtet werden, ähnlich wie bei einer Active-Directory-Sicherheitsgruppe oder einer LDAP-Gruppe.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Modernisieren Sie Mainframe-Batchdruck-Workloads in AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI

Erstellt von Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray und Shoup Inc) und Kevin Yung (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: IBM Mainframe	Ziel: AWS
R-Typ: Plattformwechsel	Workload: IBM	Technologien: Mainframe; Modernisierung
AWS-Services: AWS Managed Microsoft AD; Amazon EC2; Amazon S3; Amazon EBS		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Ihre geschäftskritischen Mainframe-Batchdruck-Workloads in der Amazon Web Services (AWS) Cloud modernisieren können, indem Sie Micro Focus Enterprise Server als Laufzeit für eine modernisierte Mainframe-Anwendung und LRS VPSX/MFI (Micro Focus Interface) als Druckserver verwenden. Das Muster basiert auf dem Ansatz der Mainframe-Modernisierung des Plattformwechsels. Bei diesem Ansatz migrieren Sie Ihre Mainframe-Batch-Aufträge zu Amazon Elastic Compute Cloud (Amazon EC2) und Ihre Mainframe-Datenbank, z. B. IBM DB2 für z/OS, zu Amazon Relational Database Service (Amazon RDS). Die Authentifizierung und Autorisierung für den modernisierten Druck-Workflow wird von AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD, durchgeführt. Der LRS Directory Information Server (LRS/DIS) ist in AWS Managed Microsoft AD integriert. Durch die Modernisierung Ihrer Stapeldruck-Workloads können Sie die IT-Infrastrukturkosten senken, die technische Belastung durch die Wartung älterer Systeme verringern, Datensilos entfernen, die Agilität und Effizienz mit einem DevOps Modell erhöhen und On-Demand-Ressourcen und Automatisierung in der AWS Cloud nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Workload für Mainframe-Ausdruck oder Ausgabemanagement
- Grundlegendes Wissen über die Neuerstellung und Bereitstellung einer Mainframe-Anwendung, die auf Micro Focus Enterprise Server ausgeführt wird (weitere Informationen finden Sie im Enterprise Server-Datenblatt in der Micro Focus-Dokumentation.)
- Grundlegendes Wissen zu Lösungen und Konzepten für den LRS-Cloud-druck (weitere Informationen finden Sie unter Output Modernization in der LRS-Dokumentation.)
- Software und Lizenz von Micro Focus Enterprise Server (weitere Informationen erhalten Sie von Micro Focus Sales.)
- LRS-VPSX/MFI-, LRS/Queue- und LRS/DIS-Software und Lizenzen (Weitere Informationen erhalten Sie beim LRS-Vertrieb.)

Hinweis : Weitere Informationen zu Konfigurationsüberlegungen für Mainframe-Stapeldruck-Workloads finden Sie unter Überlegungen im Abschnitt Zusätzliche Informationen dieses Musters.

Produktversionen

- Micro Focus Enterprise Server 6.0 (Produkt-Update 7)
- LRS VPSX/MFI V1R3 oder höher

Architektur

Quelltechnologie-Stack

- Betriebssystem – IBM z/OS
- Programmiersprache – Common Business-Oriented Language (COBOL), Job Control Language (JCL) und Customer Information Control System (CICS)
- Datenbank – IBM DB2 für z/OS und Virtual Storage Access Method (VSAM)
- Sicherheit – Ressourcenzugriffskontrolleinrichtung (RACF), CA Top Secret für z/OS und Access Control Einrichtung 2 (ACF2)
- Druck- und Ausgabeverwaltung – IBM Mainframe z/OS Druckprodukte (IBM Tivoli Output Manager für z/OS, LRS und CA View)

Zieltechnologie-Stack

- Betriebssystem – Microsoft Windows Server läuft auf Amazon EC2
- Datenverarbeitung – Amazon EC2
- Programmiersprache – COBOL, JCL und CICS
- Datenbank – Amazon RDS
- Sicherheit – AWS Managed Microsoft AD
- Druck- und Ausgabeverwaltung – LRS-Ausgabelösung in AWS
- Mainframe-Laufzeitumgebung – Micro Focus Enterprise Server

Quellarchitektur

Das folgende Diagramm zeigt eine typische aktuelle Zustandsarchitektur für einen Mainframe-Batchdruck-Workload:

Das Diagramm zeigt den folgenden Workflow:

1. Benutzer führen Geschäftstransaktionen auf einem System des Engagements (SoE) durch, das auf einer in COBOL geschriebenen IBM CICS-Anwendung basiert.
2. Die SoE ruft den Mainframe-Service auf, der die Geschäftstransaktionsdaten in einer system-of-records (SoR)-Datenbank wie IBM DB2 für z/OS aufzeichnet.
3. Die SoR behält die Geschäftsdaten aus der SoE bei.
4. Der Batch-Auftrag-Scheduler initiiert einen Batch-Auftrag, um die Druckausgabe zu generieren.
5. Der Batch-Auftrag extrahiert Daten aus der Datenbank, formatiert die Daten gemäß den Geschäftsanforderungen und generiert dann Geschäftsausgaben wie Abrechnungen, Ausweise oder Kreditanweisungen. Schließlich leitet der Batch-Auftrag die Ausgabe an das Drucken der Ausgabeverwaltung für die Verarbeitung und Ausgabebereitstellung weiter, basierend auf den Geschäftsanforderungen.
6. Beim Drucken der Ausgabeverwaltung wird eine Druckausgabe vom Stapelauftrag empfangen und diese Ausgabe dann an ein bestimmtes Ziel übermittelt, z. B. per E-Mail, eine Dateifreigabe, die sichere FTP verwendet, einen physischen Drucker, der LRS-Ausgabelösungen verwendet (wie in diesem Muster gezeigt), oder IBM Tivoli.

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für einen Mainframe-Batchdruck-Workload, der in der AWS Cloud bereitgestellt wird:

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Job-Scheduler initiiert einen Batch-Job, um eine Druckausgabe zu erstellen, z. B. Abrechnungen, Ausweise oder Kreditanweisungen.
2. Der Mainframe-Batch-Auftrag (ersetzt auf Amazon EC2) verwendet die Micro Focus Enterprise Server-Laufzeit, um Daten aus der Anwendungsdatenbank zu extrahieren, Geschäftslogik auf die Daten anzuwenden, die Daten zu formatieren und die Daten dann mithilfe von Micro Focus Print Exit an ein Druckziel zu senden (Micro Focus-Dokumentation).
3. Die Anwendungsdatenbank (eine SoR, die auf Amazon RDS ausgeführt wird) behält Daten für die Druckausgabe bei.
4. Die LRS-VPSX/MFI-Ausgabelösung wird auf Amazon EC2 bereitgestellt und ihre Betriebsdaten werden im Amazon Elastic Block Store (Amazon EBS) gespeichert. LRS VPSX/MFI verwendet den TCP/IP-basierten LRS/Queue-Übertragungsagenten, um Druckdaten über die Micro Focus JES Print Exit API zu sammeln und die Daten an ein bestimmtes Druckerziel zu übermitteln.

Hinweis: Die Ziellösung erfordert in der Regel keine Anwendungsänderungen, um Mainframe-Formatierungssprachen wie IBM Advanced Function microSD (AFP) oder Xerox Line Condition Data Stream (S) zu berücksichtigen. Weitere Informationen zur Verwendung von Micro Focus für die Migration und Modernisierung von Mainframe-Anwendungen in AWS finden Sie unter Unterstützung von Enterprise Mainframe Workloads in AWS mit Micro Focus in der AWS-Dokumentation.

AWS-Infrastrukturarchitektur

Das folgende Diagramm zeigt eine hochverfügbare und sichere AWS-Infrastrukturarchitektur für einen Mainframe-Batch-Pressing-Workload:

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Scheduler initiiert den Batch-Prozess und wird auf Amazon EC2 über mehrere Availability Zones hinweg für hohe Verfügbarkeit (HA) bereitgestellt. Hinweis: Dieses Muster deckt die Implementierung des Batch-Schedulers nicht ab. Weitere Informationen zur Implementierung finden Sie in der Dokumentation zum Softwareanbieter für Ihren Scheduler.

2. Der Mainframe-Batch-Auftrag (geschrieben in einer Programmiersprache wie JCL oder COBOL) verwendet die Kerngeschäftslogik, um Druckausgaben wie Abrechnungen, Ausweise und Kreditanweisungen zu verarbeiten und zu generieren. Der Auftrag wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt und verwendet Micro Focus Print Exit, um die Druckausgabe zum Drucken durch Endbenutzer an LRS VPSX/MFI weiterzuleiten.
3. LRS VPSX/MFI verwendet einen TCP/IP-basierten LRS/Queue-Übertragungsagenten, um Druckdaten von der Micro Focus JES Print Exit-Programmierschnittstelle zu erfassen oder zu erfassen. Druck-Beendigung übergibt die erforderlichen Informationen, damit LRS VPSX/MFI die Spool-Datei effektiv verarbeiten und LRS/Queue-Befehle dynamisch erstellen kann. Die Befehle werden dann mit einer integrierten Standardfunktion von Micro Focus ausgeführt. Hinweis: Weitere Informationen zu Druckdaten, die von Micro Focus Print Exit an LRS/Queue- und LRS-VPSX/MFI-unterstützte Mainframe-Batch-Mechanismen übergeben werden, finden Sie unter Druckdatenerfassung im Abschnitt Zusätzliche Informationen dieses Musters.
4. Ein Network Load Balancer bietet einen DNS-Namen zur Integration von Micro Focus Enterprise Server mit LRS VPSX/MFI. Hinweis: LRS VPSX/MFI unterstützt einen Layer 4 Load Balancer. Der Network Load Balancer führt auch eine grundlegende Zustandsprüfung für LRS VPSX/MFI durch und leitet den Datenverkehr an die registrierten Ziele weiter, die fehlerfrei sind.
5. Der LRS-VPSX/MFI- Druckserver wird auf Amazon EC2 über zwei Availability Zones für HA bereitgestellt und verwendet Amazon EBS als Betriebsdatenspeicher. LRS VPSX/MFI unterstützt sowohl den Aktiv-Aktiv- als auch den Aktiv-Passiv-Servicemodus. Diese Architektur verwendet mehrere AZs in einem Aktiv-Passiv-Paar als Aktiv- und Hot-Standby. Der Network Load Balancer führt eine Zustandsprüfung für LRS-VPSX/MFI-EC2-Instances durch und leitet Datenverkehr an Hot-Standby-Instances in der anderen AZ weiter, wenn sich eine aktive Instance in einem fehlerhaften Zustand befindet. Die Druckanforderungen werden in der LRS-Auftragswarteschlange lokal in jeder der EC2-Instances gespeichert. Im Falle einer Wiederherstellung muss eine ausgefallene Instance neu gestartet werden, damit die LRS-Services die Verarbeitung der Druckanforderung fortsetzen können. Hinweis: LRS VPSX/MFI kann auch Zustandsprüfungen auf Druckerflottenebene durchführen. Weitere Informationen finden Sie unter Zustandsprüfungen von Druckerflotten im Abschnitt Zusätzliche Informationen dieses Musters.
6. AWS Managed Microsoft AD lässt sich in LRS/DIS integrieren, um die Authentifizierung und Autorisierung von Druck-Workflows durchzuführen. Weitere Informationen finden Sie unter Drucken von Authentifizierung und Autorisierung im Abschnitt Zusätzliche Informationen dieses Musters.
7. LRS VPSX/MFI verwendet Amazon EBS für die Blockspeicherung. Sie können Amazon-EBS-Daten von aktiven EC2-Instances in Amazon S3 als point-in-time Snapshots sichern und auf Hot-

Standby-EBS-Volumes wiederherstellen. Um die Erstellung, Aufbewahrung und Löschung von Amazon-EBS-Volume-Snapshots zu automatisieren, können Sie Amazon Data Lifecycle Manager verwenden, um die Häufigkeit automatisierter Snapshots festzulegen und sie auf der Grundlage Ihrer RTO/RPO-Anforderungen wiederherzustellen.

Tools

AWS-Services

- Amazon EBS – Amazon Elastic Block Store (Amazon EBS) stellt Volumes für die Speicherung auf Blockebene für die Verwendung mit EC2-Instances bereit. EBS-Volumes verhalten sich wie unformatierte Blockgeräte. Sie können diese Volumes als Geräte auf Ihren Instances mounten.
- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können Amazon EC2 verwenden, um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können auf- oder abskalieren.
- Amazon RDS – Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud vereinfacht. Es bietet kostengünstige, anpassbare Kapazität für eine relationale Datenbank und verwaltet allgemeine Datenbankverwaltungsaufgaben.
- AWS Managed Microsoft AD – AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft Active Directory, ermöglicht es Ihren verzeichnisfähigen Workloads und AWS-Ressourcen, verwaltetes Active Directory in AWS zu verwenden.

Andere Tools

- LRS VPSX/MFI (Micro Focus Interface) – VPSX/MFI, gemeinsam entwickelt von LRS und Micro Focus, erfasst die Ausgabe aus einem Micro Focus Enterprise Server-JES-Spool und liefert sie zuverlässig an ein bestimmtes Druckziel.
- LRS Directory Information Server (LRS/DIS) – LRS/DIS wird für die Authentifizierung und Autorisierung während des Druck-Workflows verwendet.
- LRS/Queue – LRS VPSX/MFI verwendet einen TCP/IP-basierten LRS/Queue-Übertragungsagenten, um Druckdaten über die Programmierschnittstelle Micro Focus JES Print Exit zu erfassen oder zu erfassen.
- Micro Focus Enterprise Server – Micro Focus Enterprise Server ist eine Anwendungsbereitstellungsumgebung für Mainframe-Anwendungen. Es bietet die

Ausführungsumgebung für Mainframe-Anwendungen, die mithilfe einer beliebigen Version von Micro Focus Enterprise Developer migriert oder erstellt werden.

Polen

Micro Focus Enterprise Server auf Amazon EC2 einrichten und eine Mainframe-Batchanwendung bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Micro Focus Enterprise Server ein und stellen Sie eine Demoanwendung bereit.	Richten Sie Micro Focus Enterprise Server auf Amazon EC2 ein und stellen Sie dann die Micro Focus- BankDemo Demonstrationsanwendung auf Amazon EC2 bereit, indem Sie den Anweisungen im Micro Focus Enterprise Server auf AWS Quick Start-Bereitstellungshandbuch folgen. Die BankDemo Anwendung ist eine Mainframe-Batch-Anwendung, die die Druckausgabe erstellt und dann initiiert.	Cloud-Architekt

Einrichten eines LRS- Druckservers auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich eine LRS-Produktlizenz zum Drucken.	Um eine LRS-Produktlizenz für LRS VPSX/MFI, LRS/Queue und LRS/DIS zu erhalten, wenden Sie sich an das LRS-Output-Management-Team. Sie müssen die	Leiter erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hostnamen der EC2-Instances angeben, auf denen die LRS-Produkte installiert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon EC2-Windows-Instance, um LRS VPSX/MFI zu installieren.	Starten Sie eine Amazon EC2-Windows-Instance, indem Sie den Anweisungen unter Schritt 1: Starten einer Instance in der Amazon EC2Dokumentation folgen. Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS VPSX/MFI erfüllen: • CPU – Dual Core • RAM – 16 GB • Laufwerk – 500 GB • Minimale EC2-Instance – m5.xlarge • Betriebssystem – Windows/ Linux • Software – Internet Informati on Service (IIS) oder Apache Hinweis: Die oben genannten Hardware- und Softwarea nforderungen sind für eine kleine Druckerflotte (etwa 500–1000) vorgesehen. Um alle Anforderungen zu erfüllen, wenden Sie sich an Ihre LRS- und AWS-Kontakte. Gehen Sie beim Erstellen Ihrer Windows-Instance wie folgt vor:	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Vergewissern Sie sich, dass der EC2-Hostname derselbe Hostname ist, der für die LRS-Produktlizenz verwendet wird. 2. Aktivieren Sie CGI in Amazon EC2, indem Sie Folgendes ausführen: a. Stellen Sie eine Verbindung zu Ihrer EC2-Instance her, indem Sie die Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation befolgen. b. Suchen und öffnen Sie im Windows-Startmenü Server Manager. c. Wählen Sie in Server Manager Dashboard , Schnellstart , Rollen und Features hinzufügen aus. Wählen Sie dann Serverrollen aus. d. Wählen Sie unter Serverrollen WebServer (IIS) und dann Anwendungsentwicklung aus. e. Aktivieren Sie unter Anwendungsentwickl	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ung das Kontrollkästchen CGI. f. Folgen Sie den Anweisungen im Windows Server Manger Assistenten zum Hinzufügen von Rollen und Funktionen, um CGI zu installieren. g. Öffnen Sie Port 5500 in der Windows-Firewall der EC2-Instance für die LRS/Queue-Kommunik ation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS VPSX/MFI auf der EC2-Instance.	1. Stellen Sie eine Verbindung zu Ihrer EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation folgen. 2. Öffnen Sie den Link zur Produkt-Downloadseite in der LRS-E-Mail, die Sie erhalten sollten. Hinweis: LRS-Produkte werden durch elektronische Dateiübertragung (EFT) verteilt. 3. Laden Sie LRS VPSX/MFI herunter und entpacken Sie die Datei (Standardordner: `c:\LRS`). 4. Starten Sie den LRS Product Installer aus dem entpackten Ordner, um LRS VPSX/MFI zu installieren. 5. Wählen Sie im Menü Features auswählen die Option VPSX Server (V1R3.022) und dann Weiter aus, um den Installationsprozess zu starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/Queue.	1. Stellen Sie eine Verbindung zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation folgen. 2. Öffnen Sie den Link zur LRS-Produkt-Downloadseite in der LRS-E-Mail, die Sie erhalten sollten, laden Sie LRS/Queue herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Speicherort, an den Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm, um LRS/Queue zu installieren.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie den Link zur LRS-Produkt-Downloadseite in der LRS-E-Mail, die Sie erhalten sollten, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Speicherort, an den Sie die Dateien heruntergeladen haben, und starten Sie dann den LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer LRS Misc Tools , wählen SieLRS DIS aus und wählen Sie dann Weiter aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsprozess abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe und registrieren Sie LRS VPSX/MFI EC2 als Ziel.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen einer Zielgruppe für Ihren Network Load Balancer in der Elastic Load Balancing-Dokumentation folgen. Gehen Sie beim Erstellen der Zielgruppe wie folgt vor: 1. Wählen Sie auf der Seite Gruppendetails angeben für Zieltyp auswählen die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port 5500 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instances die LRS-VPSX/MFI-EC2-Instances aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer .	Folgen Sie den Anweisungen unter Erstellen eines Network Load Balancer sin der Elastic Load Balancing-Dokument ation. Ihr Network Load Balancer leitet den Datenverk ehr von Micro Focus Enterpris e Server an LRS VPSX/MFI EC2 weiter. Wenn Sie den Network Load Balancer erstellen, gehen Sie auf der Seite Listeners und Routing wie folgt vor: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port 5500 aus. 3. Wählen Sie für Standarda ktion die Option Weiterleiten an für die Zielgruppe aus, die Sie zuvor erstellt haben.	Cloud-Architekt

Micro Focus Enterprise Server mit LRS VPSX/MFI und LRS/Queue integrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Micro Focus Enterprise Server für die LRS/ Queue-Integration.	1. Stellen Sie eine Verbindun g zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Micro Focus Enterprise Server Administration-Benutzeroberfläche. 3. Wählen Sie in der Menüleiste NATIV aus. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 5. Scrollen Sie im linken Navigationsbereich nach unten zum Abschnitt Zusätzliche, um die Umgebungsvariablen (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) so zu konfigurieren, dass sie auf LRSQ zeigen. 6. Geben Sie für LRSQ_ADDRESS die IP-Adresse oder den DNS-Namen des Network Load Balancer sein, den Sie zuvor erstellt haben. 7. Geben Sie für LRSQ_PORT VPSX LRSQ Listener Port (5500) ein. 8. Geben Sie für LRSQ_COMMAND den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pfadspeicherort der ausführbaren LRSQ-Datei ein. Hinweis: LRS unterstützt derzeit ein maximales Zeichenlimit von 50 für DNS-Namen, dies kann sich jedoch in Zukunft ändern. Wenn Ihr DNS-Name größer als 50 ist, können Sie die IP-Adresse des Network Load Balancer als Alternative verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Micro Focus Enterprise Server für die LRS-VPSX/MFI-Integration.	1. Kopieren Sie den `VPSX_MFI_R2` Ordner aus dem LRS-VPSX/MFI-Installationsprogramm in den Micro-Focus-Enterprise-Server-Speicherort unter `C\BANKDEMO\print` . 2. Stellen Sie eine Verbindung zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung zu Ihrer Instance in der Amazon EC2-Dokumentation folgen. 3. Öffnen Sie im Windows-Startmenü die Micro Focus Enterprise Server Administration-Benutzeroberfläche. 4. Wählen Sie in der Menüleiste NATIV aus. 5. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 6. Wählen Sie unter BANKDEMO die Option JES aus. 7. Fügen Sie unter JES-Programmpfad den `DLL(VPSX_MFI_R2)` Pfad vom `C\BANKDEMO\print` Speicherort hinzu.	Cloud-Architekt

Einrichten von Druckern und Drucken von Benutzern in Micro Focus Enterprise Server und LRS VPSX/MFI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie das Micro Focus Print Exit-Modul dem Micro Focus Enterprise Server-Stapeldruck-Serverausführungsprozess zu.	1. Stellen Sie eine Verbindung zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Micro Focus Enterprise Server Administration-Benutzeroberfläche. 3. Wählen Sie in der Menüleiste NATIV aus. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 5. Wählen Sie unter BANKDEMO die Option JES aus und scrollen Sie nach unten zu Drucker. 6. Ordnen Sie in Drucker das Micro Focus Print Exit-Modul (LRSPRTE6 für Batch) dem Micro Focus Enterprise Server-Stapeldruck-Serverausführungsprozess (SEP) zu. Dies ermöglicht das	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausgabe-Routing an LRS VPSX/MFI. 7. Melden Sie sich bei der Enterprise Server-Ve rwaltungsoberfläche an. Weitere Informationen zur Konfiguration finden Sie unterUsing the Exit in der Micro Focus-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Drucker in LRS VPSX/MFI hinzu.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie die VPSX-Webschnittstelle im Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Drucker aus. 4. Wählen Sie Hinzufügen und dann Drucker hinzufügen aus. 5. Geben Sie auf der Seite Druckerkonfiguration für Druckername Lokal ein. 6. Geben Sie für VPSX-ID VPS1 ein. 7. CommTypeWählen Sie für TCPIP/LRSQ aus. 8. Geben Sie für Host/IP-Adresse die IP-Adresse des physischen Druckers ein, den Sie hinzufügen möchten. 9. Geben Sie für Gerät den Namen Ihres Geräts ein. 10. Wählen Sie entweder Windows-Treiber oder Linux/Mac-Treiber aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie Hinzufügen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Druckbenutzer in LRS VPSX/MFI.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie die VPSX-Webschnittstelle im Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Benutzer aus. 4. Wählen Sie in der Spalte Benutzername die Option admin und dann Kopieren aus. 5. Geben Sie im Fenster Benutzerprofilverwaltung für Benutzername einen Benutzernamen ein (z. B. PrintUser). 6. Geben Sie unter Beschreibung eine kurze Beschreibung ein (z. B. Benutzer für Testdruck). 7. Wählen Sie Aktualisieren. Dadurch wird ein Druckbenutzer erstellt (z. B. PrintUser). 8. Wählen Sie im Navigationsbereich unter Benutzer	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den neuen Benutzer aus, den Sie erstellt haben. 9. Wählen Sie im Menü Befehl die Option Sicherheit aus. 10. Wählen Sie auf der Seite Sicherheitsregeln alle entsprechenden Optionen für Druckersicherheit und Auftragssicherheit aus und wählen Sie dann Speichern aus. 11. Um Ihren neuen Druckbenutzer zur Administratorgruppehinzuzufügen, gehen Sie zum Navigationsbereich, wählen Sie Sicherheit und dann Konfigurieren aus. 12. Fügen Sie im Fenster Sicherheitskonfiguration Ihren neuen Druckbenutzer zur Spalte Administrator hinzu.	

Einrichten der Druckauthentifizierung und -autorisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Managed Microsoft AD-Domain mit Benutzern und Gruppen.	1. Erstellen Sie ein Active Directory in AWS Managed Microsoft AD, indem Sie den Anweisungen unter Erstellen Ihres AWS Managed Microsoft AD-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verzeichnisses in der AWS Directory Service-D okumentation folgen. 2. Stellen Sie eine EC2-Instance (Active Directory Manager) bereit und installieren Sie Active Directory-Tools zur Verwaltung Ihres AWS Managed Microsoft AD, indem Sie den Anweisung en unter Schritt 3: Bereitste llen einer EC2-Instance zur Verwaltung Ihres AWS Managed Microsoft AD in der AWS Directory Service-Dokumentation folgen. 3. Stellen Sie eine Verbindung mit Ihrer EC2-Instance her, indem Sie den Anweisung en unter Schritt 2: Herstelle n einer Verbindung mit Ihrer Instance in der Amazon EC2-Dokumentation folgen. Hinweis: Wenn Sie eine Verbindung mit der EC2-Instance herstellen, geben Sie Ihre Administratoranmel deinformationen (für das Verzeichnis, das Sie in Schritt 1 erstellt haben) im Windows-Sicherheitsfenster ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Windows-Startmenü unter Windows Administrative Tools die Option Active Directory-Benutzer und -Computer aus. 5. Erstellen Sie einen Druckbenutzer in der Active Directory-Domain, indem Sie die Schritte unter Erstellen eines Benutzers in der AWS Directory-Serviced okumentation befolgen.	
Verbinden Sie LRS VPSX/MFI EC2 mit einer AWS Managed Microsoft AD-Domain.	Fügen Sie LRS VPSX/MFI EC2 automatisch (Dokumentation zum AWS Knowledge Center) oder manuell (Dokumentation zum AWS Directory Service) zu Ihrer AWS Managed Microsoft AD-Domain hinzu.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und integrieren Sie LRS/DIS mit AWS Managed Microsoft AD.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer Instance in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die VPSX-Webschnittstelle. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 4. Wählen Sie auf der Seite Sicherheitskonfiguration im Abschnitt Sicherheitsparameter für Sicherheitstyp die Option Intern aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie den Ordner LRS Output Management im Microsoft Windows Start-Menü, wählen Sie Server Start und dann Server Stop aus. 7. Melden Sie sich bei LRS VPSX/MFI mit Ihrem Active-Directory-Benutzernamen und -Passwort an.	Cloud-Architekt

Testen eines Druck-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie eine Batchdruckanforderung von der Micro Focus BankDemo -App aus.	1. Öffnen Sie den Terminal-Emulator 3270 in Ihrer Micro Focus Enterprise Server-EC2-Instance. 2. Stellen Sie eine Verbindung mit der BankDemo App her, indem Sie den folgenden Befehl ausführen: `connect 127.0.0.1:9278` 3. Geben Sie in der BankDemo Befehlszeilenschnittstelle für Benutzer-ID B0001 ein. Geben Sie für Passwort einen nicht leeren Schlüssel ein. 4. Geben Sie für die Option Gedruckte Anweisung(en) anfordern X in die leere Zeile ein. 5. Geben Sie im Abschnitt Anweisung senden nach für Mail Y ein und drücken Sie dann F10.	Testingenieur
Überprüfen Sie die Druckausgabe in LRS VPSX/MFI.	1. Stellen Sie eine Verbindung zu Ihrer LRS-VPSX/MFI-EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Herstellen einer Verbindung mit Ihrer	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instance in der Amazon EC2Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die VPSX-Webschnittstelle. 3. Wählen Sie im Navigationsbereich Drucker und dann Ausgabewarteschlange aus. 4. Wählen Sie in der Spalte Spool-ID die Spool-ID für die Anforderung in der Druckerwarteschlange aus. 5. Wählen Sie auf der Registerkarte Aktionen in der Spalte COMMAND die Option Durchsuchen aus. Sie können jetzt die Druckausgabe eines Kontoauszugs mit Spalten für Kontonummer, Beschreibung, Datum , Betrag und Saldo sehen. Ein Beispiel finden Sie im batch_print_output-Anhang für dieses Muster.	

Zugehörige Ressourcen

- LRS Output Modernization (LRS-Dokumentation)
- ANSI- und Maschinenschlittsteuerungen (IBM-Dokumentation)
- Kanalbefehlswörter (IBM-Dokumentation)

- Bereitstellung von Enterprise Mainframe Workloads in AWS mit Micro Focus (AWS Partner Network Blog)
- Erstellen Sie einen Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager (Dokumentation zu AWS Prescriptive Guidance)
- Advanced Function microSD (AFP)-Datenstrom (IBM-Dokumentation)
- Line Conditioned Data Stream (S) (Compart-Dokumentation)
- Micro Focus Enterprise Server auf AWS (AWS-Schnellstarts)

Zusätzliche Informationen

Überlegungen

Während Ihrer Modernisierung können Sie eine Vielzahl von Konfigurationen sowohl für Mainframe-Batch-Prozesse als auch für die von ihnen generierte Ausgabe in Betracht ziehen. Die Mainframe-Plattform wurde von jedem Kunden und Anbieter angepasst, der sie mit bestimmten Anforderungen verwendet, die sich direkt auf den Druck auswirken. Ihre aktuelle Plattform kann beispielsweise das IBM Advanced Function microSD (AFP) oder den Xerox Line Condition Data Stream (S) in den aktuellen Workflow integrieren. Darüber hinaus können Mainframe-Wagensteuerzeichen und Kanalbefehlswörter das Aussehen der gedruckten Seite beeinflussen und erfordern möglicherweise eine besondere Handhabung. Im Rahmen des Modernisierungsplanungsprozesses empfehlen wir Ihnen, die Konfigurationen in Ihrer spezifischen Druckumgebung zu bewerten und zu verstehen.

Drucken der Datenerfassung

Micro Focus Print Exit übergibt die erforderlichen Informationen, damit LRS VPSX/MFI die Spool-Datei effektiv verarbeiten kann. Die Informationen bestehen aus Feldern, die in den entsprechenden Kontrollblöcken übergeben werden, z. B.:

- JOBNAME
- OWNER (USERID)
- DESTINATION
- FORM
- DATENAME
- WRITER

LRS VPSX/MFI unterstützt die folgenden Mainframe-Batch-Mechanismen zur Erfassung von Daten aus Micro Focus Enterprise Server.

- BATCH COBOL- Druck-/Spool-Verarbeitung mit Standard-z/OS-JCL-Anweisungen SYSOUT DD/OUTPUT
- BATCH COBOL Druck-/Spoolverarbeitung mit Standard-z/OS JCL CA-SPOOL SUBSYS DD-Anweisungen
- IMS/COBOL Druck-/Spoolverarbeitung über die CBLTDLI-Schnittstelle (eine vollständige Liste der unterstützten Methoden und Programmierbeispiele finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.)

Zustandsprüfungen von Druckerflotten

LRS VPSX/MFI (LRS LoadX) kann detaillierte Zustandsprüfungen durchführen, einschließlich Geräteverwaltung und Betriebsoptimierung. Die Geräteverwaltung kann Fehler in einem Druckergerät erkennen und die Druckanforderung an einen fehlerfreien Drucker weiterleiten. Weitere Informationen zu detaillierten Zustandsprüfungen für Druckerflotten finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Authentifizierung und Autorisierung drucken

LRS/DIS ermöglicht es LRS-Anwendungen, Benutzer-IDs und Passwörter mithilfe von Microsoft Active Directory oder einem LDAP-Server zu authentifizieren. Zusätzlich zur grundlegenden Druckautorisierung kann LRS/DIS in den folgenden Anwendungsfällen auch detaillierte Drucksicherheitskontrollen anwenden:

- Verwalten Sie, wer den Druckerauftrag durchsuchen kann.
- Verwalten Sie die Browsing-Ebene der Aufträge anderer Benutzer.
- Verwalten Sie operative Aufgaben. Zum Beispiel Sicherheit auf Befehlsebene wie Anhalten/Freigeben, Bereinigen, Ändern, Kopieren und Umleiten. Die Sicherheit kann entweder durch die Benutzer-ID oder die Gruppe eingerichtet werden (ähnlich wie die AD-Gruppe oder die LDAP-Gruppe).

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Modernisieren Sie Mainframe-Online-Druck-Workloads auf AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI

Erstellt von Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) und Kevin Yung (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Mainframe	Ziel: AWS
R-Typ: Replatform	Arbeitslast: IBM	Technologien: Mainframe; Migration; Modernisierung
AWS-Services: Von AWS verwaltetes Microsoft AD; Amazon EC2; Amazon RDS; Amazon EBS		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Ihre geschäftskritischen Mainframe-Online-Druck-Workloads in der Amazon Web Services (AWS) -Cloud modernisieren können, indem Sie Micro Focus Enterprise Server als Laufzeit für eine modernisierte Mainframe-Anwendung und LRS VPSX/MFI (Micro Focus Interface) als Druckserver verwenden. Das Muster basiert auf dem Ansatz der Replatform Mainframe-Modernisierung. Bei diesem Ansatz migrieren Sie Ihre Mainframe-Online-Anwendung zu Amazon Elastic Compute Cloud (Amazon EC2) und Ihre Mainframe-Datenbank, wie IBM DB2 for z/OS, zu Amazon Relational Database Service (Amazon RDS). Die Authentifizierung und Autorisierung für den modernisierten Druck-Workflow erfolgt durch AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD. Der LRS Directory Information Server (LRS/DIS) ist in AWS Managed Microsoft AD für die Authentifizierung und Autorisierung von Druckworkflows integriert. Durch die Modernisierung Ihrer Online-Druck-Workloads können Sie die IT-Infrastrukturkosten senken, den technischen Aufwand für die Wartung älterer Systeme verringern, Datensilos beseitigen, die Agilität und Effizienz mit einem DevOps Modell erhöhen und die Vorteile von On-Demand-Ressourcen und Automatisierung in der AWS-Cloud nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Mainframe-Workload für Online-Druck oder Output-Management
- Grundkenntnisse zur Neuerstellung und Bereitstellung einer Mainframe-Anwendung, die auf Micro Focus Enterprise Server ausgeführt wird (Weitere Informationen finden Sie im Enterprise Server-Datenblatt in der Micro Focus-Dokumentation.)
- Grundkenntnisse der LRS Cloud-Printing-Lösungen und -Konzepte (Weitere Informationen finden Sie in der LRS-Dokumentation unter Output Modernization.)
- Micro Focus Enterprise Server-Software und -Lizenz (Weitere Informationen erhalten Sie vom Micro Focus-Vertrieb.)
- Software und Lizenzen für LRS VPSX/MFI, LRS/Queue und LRS/DIS (Weitere Informationen erhalten Sie vom LRS-Vertrieb.)

Hinweis : Weitere Informationen zu Überlegungen zur Konfiguration von Mainframe-Online-Druck-Workloads finden Sie unter Überlegungen im Abschnitt Zusätzliche Informationen dieses Patterns.

Produktversionen

- Micro Focus Enterprise Server 8.0 oder höher
- LRS VPSX/MFI V1R3 oder höher

Architektur

Quelltechnologie-Stack

- Betriebssystem — IBM z/OS
- Programmiersprache — Common Business-Oriented Language (COBOL) und Customer Information Control System (CICS)
- Datenbank — IBM DB2 für z/OS, IBM Information Management System (IMS) und Virtual Storage Access Method (VSAM)
- Sicherheit — Resource Access Control Facility (RACF), CA Top Secret für z/OS und Access Control Facility 2 (ACF2)

- Druck- und Ausgabemanagement — IBM Mainframe-z/OS-Druckprodukte (IBM Infoprint Server für z/OS, LRS und CA View)

Zieltechnologie-Stack

- Betriebssystem — Microsoft Windows Server läuft auf Amazon EC2
- Datenverarbeitung — Amazon EC2
- Programmiersprache — COBOL und CICS
- Datenbank — Amazon RDS
- Sicherheit — AWS Managed Microsoft AD
- Druck- und Ausgabemanagement — LRS-Drucklösung auf AWS
- Mainframe-Laufzeitumgebung — Micro Focus Enterprise Server

Quellarchitektur

Das folgende Diagramm zeigt eine typische aktuelle Architektur für einen Mainframe-Online-Druck-Workload.

Das Diagramm zeigt den folgenden Workflow:

1. Benutzer führen Geschäftstransaktionen auf einem System of Engagement (SoE) durch, das auf einer in COBOL geschriebenen IBM CICS-Anwendung basiert.
2. Das SoE ruft den Mainframe-Service auf, der die Geschäftstransaktionsdaten in einer system-of-records (SoR) -Datenbank wie IBM DB2 for z/OS aufzeichnet.
3. Das SoR speichert die Geschäftsdaten aus dem SoE.
4. Ein Benutzer initiiert eine Anforderung zur Generierung der Druckausgabe vom CICS-SoE, wodurch eine Drucktransaktionsanwendung zur Verarbeitung der Druckanforderung initiiert wird.
5. Die Anwendung für Drucktransaktionen (z. B. ein CICS- und COBOL-Programm) extrahiert Daten aus der Datenbank, formatiert die Daten gemäß den Geschäftsanforderungen und generiert Geschäftsergebnisse (Druckdaten) wie Abrechnungen, Personalausweise oder Kreditauszüge. Anschließend sendet die Anwendung mithilfe der Virtual Telecommunications Access Method (VTAM) eine Druckanforderung. Ein z/OS-Druckserver (wie IBM Infoprint Server) verwendet NetSpool oder eine ähnliche VTAM-Komponente, um die Druckanforderungen abzufangen, und

erstellt dann Druckausgabedatensätze auf dem JES-Spool mithilfe von JES-Ausgabeparametern. Die JES-Ausgabeparameter geben die Routing-Informationen an, die der Druckserver verwendet, um die Ausgabe an einen bestimmten Netzwerkdrucker zu übertragen. Der Begriff VTAM bezieht sich auf den z/OS Communications Server und das System Network Architecture (SNA) - Serviceelement von z/OS.

6. Die Komponente zur Übertragung der Druckausgabe überträgt die ausgegebenen Druckdatensätze vom JES-Spool an externe Drucker oder Druckserver wie LRS (wie in diesem Muster gezeigt), IBM Infoprint Server oder E-Mail-Ziele.

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für einen Mainframe-Online-Druck-Workload, der in der AWS-Cloud bereitgestellt wird:

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer initiiert über eine Online-Benutzeroberfläche (CICS) eine Druckanfrage, um Druckausgaben wie Rechnungsauszüge, Personalausweise oder Kreditauszüge zu erstellen.
2. Die Mainframe-Online-Anwendung (auf Amazon EC2 umgestellt) verwendet die Micro Focus Enterprise Server-Laufzeit, um Daten aus der Anwendungsdatenbank zu extrahieren, Geschäftslogik auf die Daten anzuwenden, die Daten zu formatieren und die Daten dann mithilfe von Micro Focus CICS Print Exit (DFHUPRNT) an ein Druckziel zu senden.
3. Die Anwendungsdatenbank (ein SoR, der auf Amazon RDS läuft) speichert Daten für die Druckausgabe.
4. Die LRS VPSX/MFI-Drucklösung wird auf Amazon EC2 bereitgestellt, und ihre Betriebsdaten werden im Amazon Elastic Block Store (Amazon EBS) gespeichert. LRS VPSX/MFI verwendet einen TCP/IP-basierten LRS/Queue-Übertragungsagenten, um Druckdaten über die Micro Focus CICS Print Exit API (DFHUPRNT) zu sammeln und die Daten an ein bestimmtes Druckerziel zu senden. Die ursprüngliche TERMID (TERM), die in der modernisierten CICS-Anwendung verwendet wurde, wird als Name der VPSX/MFI-Warteschlange verwendet.

Hinweis: Die Ziellösung erfordert in der Regel keine Anwendungsänderungen, um Mainframe-Formatierungssprachen wie IBM Advanced Function Presentation (AFP) oder Xerox Line Condition Data Stream (LCDS) zu berücksichtigen. Weitere Informationen zur Verwendung von Micro Focus

für die Migration und Modernisierung von Mainframe-Anwendungen auf AWS finden Sie in der AWS-Dokumentation unter Empowering Enterprise Mainframe Workloads on AWS with Micro Focus.

AWS-Infrastrukturarchitektur

Das folgende Diagramm zeigt eine hochverfügbare und sichere AWS-Infrastrukturarchitektur für einen Mainframe-Online-Druck-Workload:

Das Diagramm zeigt den folgenden Workflow:

1. Die Mainframe-Online-Anwendung (geschrieben in einer Programmiersprache wie CICS oder COBOL) verwendet die Kerngeschäftslogik, um Druckausgaben wie Abrechnungen, Personalausweise und Kreditauszüge zu verarbeiten und zu generieren. Die Online-Anwendung wird auf Amazon EC2 in zwei Availability Zones (AZ) für hohe Verfügbarkeit (HA) bereitgestellt und verwendet Micro Focus CICS Print Exit, um die Druckausgabe zum Drucken durch Endbenutzer an LRS VPSX/MFI weiterzuleiten.
2. LRS VPSX/MFI verwendet einen TCP/IP-basierten LRS/Queue-Übertragungsagenten, um Druckdaten über die Micro Focus Online Print Exit-Programmierschnittstelle zu sammeln oder zu erfassen. Online Print Exit leitet die erforderlichen Informationen weiter, damit LRS VPSX/MFI die Druckdatei effektiv verarbeiten und LRS/Queue-Befehle dynamisch erstellen kann.

   Hinweis : Weitere Informationen zu den verschiedenen Methoden der CICS-Anwendungsprogrammierung für den Druck und deren Unterstützung in Micro Focus Enterprise Server und LRS VPSX/MFI finden Sie unter Druckdatenerfassung im Abschnitt Zusätzliche Informationen dieses Musters.
3. Ein Network Load Balancer stellt einen DNS-Namen für die Integration von Micro Focus Enterprise Server mit LRS VPSX/MFI bereit. Hinweis: LRS VPSX/MFI unterstützt einen Layer-4-Load Balancer. Der Network Load Balancer führt außerdem eine grundlegende Integritätsprüfung für LRS VPSX/MFI durch und leitet den Datenverkehr an die registrierten Ziele weiter, die fehlerfrei sind.
4. Der LRS VPSX/MFI-Druckserver wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt und verwendet Amazon EBS als Betriebsdatenspeicher. LRS VPSX/MFI unterstützt sowohl den aktiv-aktiven als auch den aktiv-passiven Servicemodus. Diese Architektur verwendet mehrere Availability Zones in einem Aktiv-Passiv-Paar als aktiven und Hot-Standby. Der Network Load Balancer führt eine Integritätsprüfung für LRS VPSX/MFI EC2-Instances durch und leitet den Datenverkehr an Hot-Standby-Instances in einer anderen Availability Zone weiter, wenn sich eine

aktive Instance in einem fehlerhaften Zustand befindet. Die Druckanforderungen werden lokal in jeder EC2-Instanz in der LRS-Job-Warteschlange gespeichert. Im Falle einer Wiederherstellung muss eine ausgefallene Instanz neu gestartet werden, damit die LRS-Dienste die Verarbeitung der Druckanforderung fortsetzen können.

Hinweis: LRS VPSX/MFI kann auch Zustandsprüfungen auf Ebene der Druckerflotte durchführen. Weitere Informationen finden Sie unter Integritätsprüfungen der Druckerflotte im Abschnitt Zusätzliche Informationen dieses Musters.

5. AWS Managed Microsoft AD lässt sich in LRS/DIS integrieren, um die Authentifizierung und Autorisierung von Druckworkflows durchzuführen. Weitere Informationen finden Sie unter Druckauthentifizierung und Autorisierung im Abschnitt Zusätzliche Informationen dieses Musters.
6. LRS VPSX/MFI verwendet Amazon EBS für Blockspeicher. Sie können Amazon EBS-Daten von aktiven EC2-Instances als point-in-time Snapshots auf Amazon S3 sichern und sie auf Hot-Standby-EBS-Volumes wiederherstellen. Um die Erstellung, Aufbewahrung und Löschung von Amazon EBS-Volume-Snapshots zu automatisieren, können Sie Amazon Data Lifecycle Manager verwenden, um die Häufigkeit automatisierter Snapshots festzulegen und sie auf der Grundlage Ihrer RTO/RPO-Anforderungen wiederherzustellen.

Tools

AWS-Services

- Amazon Elastic Block Store (Amazon EBS) bietet Volumes für die Speicherung auf Blockebene, die in Verbindung mit Amazon-EC2-Instances verwendet werden. EBS-Volumes verhalten sich wie unformatierte Blockgeräte. Sie können diese Volumes als Geräte auf Ihren Instances mounten.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- AWS Directory Service for Microsoft Active Directory (AD), auch bekannt als AWS Managed Microsoft Active Directory, ermöglicht es Ihren verzeichnissensitiven Workloads und AWS-Ressourcen, verwaltetes Active Directory in AWS zu verwenden.

Andere Tools

- LRS VPSX/MFI (Micro Focus Interface), das gemeinsam von LRS und Micro Focus entwickelt wurde, erfasst die Ausgabe von einem Micro Focus Enterprise Server JES-Spool und leitet sie zuverlässig an ein bestimmtes Druckziel weiter.
- Der LRS Directory Information Server (LRS/DIS) wird für die Authentifizierung und Autorisierung während des Druckworkflows verwendet.
- LRS/Queue ist ein TCP/IP-basierter LRS/Queue-Übertragungsagent, der von LRS VPSX/MFI verwendet wird, um Druckdaten über die Micro Focus Online Print Exit-Programmierschnittstelle zu sammeln oder zu erfassen.
- Micro Focus Enterprise Server ist eine Umgebung zur Anwendungsbereitstellung für Mainframe-Anwendungen. Sie bietet die Ausführungsumgebung für Mainframe-Anwendungen, die mithilfe einer beliebigen Version von Micro Focus Enterprise Developer migriert oder erstellt wurden.

Epen

Micro Focus Enterprise Server auf Amazon EC2 einrichten und eine Mainframe-Online-Anwendung bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Micro Focus Enterprise Server ein und stellen Sie eine Demo-Online-Anwendung bereit.	Richten Sie Micro Focus Enterprise Server auf Amazon EC2 ein und stellen Sie dann die Micro Focus Account Demo-Anwendung (ACCT-Demo) auf Amazon EC2 bereit, indem Sie den Anweisungen unter Tutorial: CICS-Support in der Micro Focus-Dokumentation folgen. Die ACCT-Demo-Anwendung ist eine Mainframe-Online-Anwendung (CICS), die die Druckausgabe erstellt und dann initiiert.	Cloud-Architekt

Richten Sie einen LRS-Druckserver auf Amazon EC2 ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich eine LRS-Produktlizenz zum Drucken.	Um eine LRS-Produktlizenz für LRS VPSX/MFI, LRS/Queue und LRS/DIS zu erhalten, wenden Sie sich an das LRS Output Management Team. Sie müssen die Hostnamen der EC2-Instances angeben, auf denen die LRS-Produkte installiert werden.	Bauen Sie einen Vorsprung auf
Erstellen Sie eine Amazon EC2 EC2-Windows-Instance, um LRS VPSX/MFI zu installieren.	Starten Sie eine Amazon EC2 EC2-Windows-Instance, indem Sie den Anweisungen in Schritt 1: Starten einer Instance in der Amazon EC2 EC2-Dokumentation folgen. Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS VPSX/MFI erfüllen: • Zentralprozessor — Doppelkern • RAM — 16 GB • Laufwerk — 500 GB • Minimale EC2-Instanz — m5.xlarge • Betriebssystem — Windows/Linux • Software — Internetinformationsdienst (IIS) oder Apache	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Die oben genannten Hardware- und Softwarea nforderungen sind für eine kleine Druckerflotte (etwa 500—1000) vorgesehen. Um die vollständigen Anforderungen zu erfahren, wenden Sie sich an Ihre Ansprechpartner bei LRS und AWS. Gehen Sie beim Erstellen Ihrer Windows-Instance wie folgt vor: 1. Vergewissern Sie sich, dass der EC2-Hostname derselbe Hostname ist, der für die LRS-Produktlizenz verwendet wurde. 2. Aktivieren Sie CGI in Amazon EC2, indem Sie wie folgt vorgehen: a. Connect zu Ihrer EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. b. Suchen und öffnen Sie im Windows-Startmenü den Server-Manager. c. Wählen Sie im Server-Manager Dashboard, Schnellstart, Rollen und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktionen hinzufügen aus. Wählen Sie dann Serverrollen aus. d. Wählen Sie unter Serverrollen die Option WebServer (IIS) und dann Anwendung sentwicklung aus. e. Aktivieren Sie unter Anwendungsentwickl ung das Kontrollkästchen CGI. f. Folgen Sie den Anweisungen im Windows Server-Ma nager-Assistenten zum Hinzufügen von Rollen und Funktionen, um CGI zu installieren. g. Öffnen Sie Port 5500 in der Windows-Firewall der EC2-Instance für die LRS/Queue-Kommunik ation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS VPSX/MFI auf der EC2-Instanz.	1. Connect zu Ihrer EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokum entation folgen. 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur Produkt-Download-Seite. Hinweis: LRS-Produkte werden per elektronischer Dateiübertragung (EFT) vertrieben. 3. Laden Sie LRS VPSX/MFI herunter und entpacken Sie die Datei (Standardordner:). `c:\LRS` 4. Starten Sie den LRS Product Installer aus dem entpackten Ordner, um LRS VPSX/MFI zu installieren. 5. Wählen Sie im Menü „Funktionen auswählen“ die Option VPSX® Server (V1R3.022) und klicken Sie dann auf Weiter, um den Installationsvorgang zu starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/Queue.	1. Connect zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokum entation folgen. 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/Queue herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Verzeichnis, in das Sie die Dateien herunterg eladen haben, und starten Sie dann das LRS-Produ ktinstallationsprogramm, um LRS/Queue zu installieren.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	1. Connect zu Ihrer LRS VPSX/MFI EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Verzeichnis, in das Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer die Option LRS Misc Tools, wählen Sie LRS DIS und dann Weiter aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsvorgang abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe und registrieren Sie LRS VPSX/MFI EC2 als Ziel.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen Sie eine Zielgruppe für Ihren Network Load Balancer in der Elastic Load Balancing Balancing-Dokumentation folgen. Gehen Sie beim Erstellen der Zielgruppe wie folgt vor: 1. Wählen Sie auf der Seite Gruppendetails angeben für Wählen Sie einen Zieltyp die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port die Option 5500 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instances die LRS VPSX/MFI EC2-Instances aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	Folgen Sie den Anweisungen unter Network Load Balancer erstellen in der Elastic Load Balancing Balancing-Dokumentation. Ihr Network Load Balancer leitet den Datenverkehr vom Micro Focus Enterprise Server an LRS VPSX/MFI EC2 weiter. Wenn Sie den Network Load Balancer erstellen, gehen Sie auf der Seite Listener und Routing wie folgt vor: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port die Option 5500 aus. 3. Wählen Sie für Standarda ktion die Option Weiterleiten an für die Zielgruppe, die Sie zuvor erstellt haben.	Cloud-Architekt

Integrieren Sie Micro Focus Enterprise Server mit LRS VPSX/MFI und LRS/Queue

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Micro Focus Enterprise Server für die LRS/Queue-Integration.	1. Connect zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon EC2 EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Micro Focus Enterprise Server Administration UI. 3. Wählen Sie in der Menüleiste NATIVE. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO oder Ihre Enterprise-Serverregion aus. 5. Scrollen Sie im linken Navigationsbereich von Allgemein nach unten zum Abschnitt Erweitert, um die Umgebungsvariablen (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) so zu konfigurieren, dass sie auf LRSQ verweisen. 6. Geben Sie für LRSQ_ADDRESS die IP-Adresse oder den DNS-Namen des Network Load Balancer ein, den Sie zuvor erstellt haben. 7. Geben Sie für LRSQ_PORT den VPSX LRSQ Listener Port (5500) ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Geben Sie für LRSQ_COMMAND den Pfad der ausführbaren LRSQ-Datei ein. 9. Hinweis: LRS unterstützt derzeit eine maximale Zeichenbeschränkung von 50 für DNS-Namen, dies kann sich jedoch in future ändern. Wenn Ihr DNS-Name größer als 50 ist, können Sie alternativ die IP-Adresse des Network Load Balancer verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie CICS Print Exit (DFHUPRNT) für die Initialisierung von Micro Focus Enterprise Server zur Verfügung.	1. Connect zu Ihrer Micro Focus Enterprise Server EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. 2. Kopieren Sie CICS Print Exit (DFHUPRNT) aus dem ausführbaren LRS VPSX/MFI-Ordner (benanntVPSX_MFI_R2) in den Micro Focus Enterprise Server EC2-Instance-Speicherort. Für 32-Bit-Systeme lautet der Speicherort. `C:\Program Files (x86) \Micro Focus\Enterprise Server\bin` Für 64-Bit-Systeme lautet der Standort`C:\Program Files (x86) \Micro Focus\Enterprise Server\bin64` . Hinweis: Die `DFHUPRNT_64.dll` Datei muss `DFHUPRNT.dll` beim Kopieren umbenannt werden. Stellen Sie sicher, dass Micro Focus Enterprise Server	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CICS Print Exit (DFHUPRNT) erkannt hat 1. Stoppen und starten Sie Micro Focus Enterprise Server. 2. Öffnen Sie im Administrationsbereich von Micro Focus Enterprise Server die Optionen Monitor, Logs, Console logs. 3. Suchen Sie in den Konsolenprotokollen nach der folgenden Meldung: „3270 printer user exit DFHUPRNT successfully installed successfully.“	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Terminal-ID (TermIDs) des CICS-Druckers als Micro Focus Enterprise Server.	Aktivieren Sie den 3270-Druck in Micro Focus Enterprise Server 1. Öffnen Sie im Administrationsbereich von Micro Focus Enterprise Server die Optionen CICS, Resources, By Group. 2. Wählen Sie im linken Navigationsbereich SIT (System Initialization Table) und dann BNKCICV. 3. Scrollen Sie im Bereich Allgemein nach unten zu 3270, und aktivieren Sie dann das Kontrollkästchen 3270 Print. Definieren Sie das Terminal des CICS-Druckers in Micro Focus Enterprise Server 1. Öffnen Sie im Administrationsbereich von Micro Focus Enterprise Server die Optionen CICS, Resources, By Type. 2. Wählen Sie im linken Navigationsbereich Term und anschließend Neu aus. Das Formular „Terminalressource erstellen“ wird geöffnet.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Geben Sie unter Name den Namen der LRS-Druckwarteschlange ein. (Hinweis: Dieses Muster verwendet „P275“ als Terminal-ID und LRS VPSX-Druckwarteschlange des CICS-Druckers.) 4. Geben Sie als Gruppe BANKTERM ein. 5. Geben Sie für Automatische Installation — Modell den Wert NEIN ein. 6. Geben Sie für Terminal Identifiers — Terminal type den Wert DFHPRT32 ein. 7. Geben Sie als Netzname VTAMP275 ein. 8. Aktivieren Sie für Terminal Usage das Kontrollkästchen In Betrieb. 9. Scrollen Sie zum Seitenanfang und wählen Sie dann Speichern. 10. Wählen Sie Installieren aus. In einer Popup-Meldung wird eine Meldung angezeigt, dass die Installation erfolgreich abgeschlossen wurde.	

Richten Sie Drucker und Druckbenutzer in Micro Focus Enterprise Server und LRS VPSX/MFI ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Druckwartschlange im LRS VPSX.	1. Connect zu Ihrer LRS VPSX/MFI EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. 2. Öffnen Sie das VPSX-Webinterface über das Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Drucker aus. 4. Wählen Sie Hinzufügen und dann Drucker hinzufügen. 5. Geben Sie auf der Seite Druckerkonfiguration P275 als Druckername ein. 6. Geben Sie für VPSX ID VPS1 ein. 7. Wählen CommTypeSie für TCPIP/LRSQ aus. 8. Geben Sie für Host/IP-Adresse die IP-Adresse des physischen Druckers ein, den Sie hinzufügen möchten. 9. Geben Sie unter Gerät den Namen Ihres Geräts ein.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Wählen Sie entweder Windows-Treiber oder Linux/Mac-Treiber. 11. Wählen Sie Hinzufügen aus. Hinweis: Die Druckwart eschlange muss den in Micro Focus Enterprise Server erstellten Print TermIDs entsprechen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Druckbenutzer in LRS VPSX/MFI.	1. Connect zu Ihrer LRS VPSX/MFI EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. 2. Öffnen Sie das VPSX-Webinterface über das Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Benutzer aus. 4. Wählen Sie in der Spalte Benutzername die Option admin und dann Kopieren aus. 5. Geben Sie im Fenster Benutzerprofilverwaltung für Benutzername einen Benutzernamen ein (z. B. PrintUser). 6. Geben Sie unter Beschreibung eine kurze Beschreibung ein (z. B. Benutzer für Testdruck). 7. Wählen Sie Aktualisieren. Dadurch wird ein Druckbenutzer erstellt (z. B. PrintUser). 8. Wählen Sie im Navigationsbereich unter Benutzer	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den neuen Benutzer aus, den Sie erstellt haben. 9. Wählen Sie im Befehlsmenü die Option Sicherheit aus. 10. Wählen Sie auf der Seite Sicherheitsregeln alle zutreffenden Optionen für Druckersicherheit und Jobsicherheit aus, und klicken Sie dann auf Speichern. 11. Um Ihren neuen Druckbenutzer zur Administratorgruppe hinzuzufügen, wechseln Sie zum Navigationsbereich, wählen Sie Sicherheit und dann Konfigurieren aus. 12. Fügen Sie im Fenster Sicherheitskonfiguration Ihren neuen Druckbenutzer zur Administratorspalte hinzu.	

Richten Sie die Druckauthentifizierung und -autorisierung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine von AWS verwaltete Microsoft AD-Domain mit Benutzern und Gruppen.	1. Erstellen Sie ein Active Directory auf AWS Managed Microsoft AD, indem Sie den Anweisungen unter Erstellen Sie Ihr	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Managed Microsoft AD-Verzeichnis in der AWS Directory Service Service-Dokumentation folgen. 2. Stellen Sie eine EC2-Instance (Active Directory -Manager) bereit und installieren Sie Active Directory-Tools zur Verwaltung Ihres AWS Managed Microsoft AD. Folgen Sie dazu den Anweisungen in Schritt 3: Bereitstellen einer EC2-Instance zur Verwaltung Ihres AWS Managed Microsoft AD in der AWS Directory Service Service-Dokumentation. 3. Connect zu Ihrer EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. Hinweis: Wenn Sie eine Verbindung mit der EC2-Instance herstellen, geben Sie Ihre Administratoranmeldedaten (für das Verzeichnis, das Sie in Schritt 1 erstellt haben) in das Windows-Sicherheitsfenster ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Windows-Startmenü unter Windows-Verwaltungstools die Option Active Directory-Benutzer und -Computer aus. 5. Erstellen Sie einen Druckbenutzer in der Active Directory-Domäne, indem Sie die Schritte unter Benutzer erstellen in der Dokumentation zum AWS-Verzeichnisdienst befolgen.	
Verbinden Sie LRS VPSX/MFI EC2 mit einer von AWS verwalteten Microsoft AD-Domain.	Verbinden Sie LRS VPSX/MFI EC2 automatisch (AWS Knowledge Center-Dokumentation) oder manuell (AWS Directory Service-Dokumentation) mit Ihrer AWS Managed Microsoft AD-Domain.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und integrieren Sie LRS/DIS mit AWS Managed Microsoft AD.	1. Connect zu Ihrer LRS VPSX/MFI EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 4. Wählen Sie auf der Seite Sicherheitskonfiguration im Abschnitt Sicherheitsparameter für Sicherheitstyp die Option Intern aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie den Ordner LRS Output Management im Microsoft Windows-Startmenü, wählen Sie Serverstart und dann Serverstopp aus. 7. Melden Sie sich mit Ihrem Active Directory-Benutzernamen und -Passwort bei LRS VPSX/MFI an.	Cloud-Architekt

Testen Sie einen Online-Druck-Workflow

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie über die Micro Focus ACCT Demo-App eine Online-Druckanfrage.	1. Öffnen Sie den TN3270-Terminalemulator in Ihrer Micro Focus Enterpris e Server EC2-Instance. (Hinweis: Dieses Muster verwendet 3270-Term inalemulatoren.) 2. Connect zum TN3270-Te rminalemulator (Rumba) her. Verwenden Sie als Hostnamenadresse 127.0.0.1. Verwenden Sie für Telnet-Port 9270. 3. Nachdem Sie eine Verbindung zum 3270-Bild schirm hergestellt haben, drücken Sie CTL+SHIFT +Z, um den Bildschirm zu löschen. 4. Um die ACCT-Demo-Anwendung zu starten, geben Sie im leeren Bildschirm ACCT ein. Dadurch wird der Hauptbild schirm der Anwendung ACCT Demo Online (CICS) geöffnet. Hinweis: Der Hauptbildschirm enthält Menüoptionen wie Kontodatei, Suchen nach Namen, Enter, Anforderu ngstyp, Konto und Drucker.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Um eine Druckanfrage über die ACCT Demo Online (CICS) -Anwendung einzureichen, geben Sie P in das Feld Anforderungstyp, 11111 in das Kontofeld und P275 in das Druckerfeld ein. Achten Sie darauf, den Wert im Druckerfeld auf den Wert der Terminal-ID des CICS-Druckers einzustellen. 6. Drücken Sie die Eingabetaste. Die Meldung „Print Request Scheduled“ wird am unteren Bildschirmrand angezeigt. Dadurch wird bestätigt, dass aus der ACCT-Demo-Anwendung eine Online-Druckanfrage generiert und zur Druckverarbeitung an LRS VPS/MFI gesendet wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Druckausgabe in LRS VPSX/MFI.	1. Connect zu Ihrer LRS VPSX/MFI EC2-Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon EC2 EC2-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Drucker und dann Ausgabewarteschlange aus. Suchen Sie die P275-Druckwarteschlange, die Sie zuvor für den Online-Druck erstellt haben. 4. Wählen Sie für die Druckerwarteschlange (P275) in der Spalte Spool-ID die Spool-ID für den Auftrag in der Druckerwarteschlange aus. 5. Wählen Sie auf der Registerkarte Aktionen in der Spalte COMMAND die Option Durchsuchen aus. Sie können jetzt die Druckausgabe eines Kontoauszugs mit Spalten für Kontonummer, NACHNAME,	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	VORNAME, ADRESSE, TELEFON und Nr. sehen. Ausgestellte Karten, Ausstellungsdatum, Betrag und Saldo. Ein Beispiel für dieses Muster finden Sie im Anhang online_print_output.	

Zugehörige Ressourcen

- Modernisierung der LRS-Leistung (LRS-Dokumentation)
- VTAM-Netzwerkkonzepte (IBM-Dokumentation)
- Zusammenfassung der LU-Typen (Logical Unit) (IBM-Dokumentation)
- ANSI und Maschinenwagensteuerungen (IBM-Dokumentation)
- Unterstützung von Mainframe-Workloads für Unternehmen auf AWS mit Micro Focus (AWS-Partnernetzwerk-Blog)
- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager (Dokumentation zu AWS Prescriptive Guidance)
- AFP-Datenstream (Advanced Function Presentation) (IBM-Dokumentation)
- Line Conditioned Data Stream (LCDS) (Compart-Dokumentation)

Zusätzliche Informationen

Überlegungen

Während Ihrer Modernisierung können Sie eine Vielzahl von Konfigurationen für Mainframe-Online-Prozesse und die damit generierte Leistung in Betracht ziehen. Die Mainframe-Plattform wurde von allen Kunden und Anbietern, die sie verwenden, an spezielle Anforderungen angepasst, die sich direkt auf den Druck auswirken. Beispielsweise kann Ihre aktuelle Plattform IBM Advanced Function Presentation (AFP) oder den Xerox Line Condition Data Stream (LCDS) in den aktuellen Arbeitsablauf integrieren. Darüber hinaus können Mainframe-Wagen-Steuerzeichen und Kanalbefehle das Aussehen der gedruckten Seite beeinflussen und erfordern möglicherweise eine

besondere Behandlung. Im Rahmen der Planung der Modernisierung empfehlen wir Ihnen, die Konfigurationen in Ihrer spezifischen Druckumgebung zu bewerten und zu verstehen.

Erfassung von Druckdaten

In diesem Abschnitt werden die Methoden zur CICS-Anwendungsprogrammierung zusammengefasst, die Sie in einer IBM-Mainframe-Umgebung zum Drucken verwenden können. LRS-VPSX/MFI-Komponenten bieten Techniken, mit denen dieselben Anwendungsprogramme Daten auf dieselbe Weise erstellen können. In der folgenden Tabelle wird beschrieben, wie die einzelnen Methoden der Anwendungsprogrammierung in einer modernisierten CICS-Anwendung unterstützt werden, die in AWS und Micro Focus Enterprise Server mit einem LRS VPSX/MFI-Druckserver ausgeführt wird.

Methode	Beschreibung	Support der Methode in einer modernisierten Umgebung
FÜHRUNGSKRÄFTE SENDEN TEXT... oder EXEC CICS SEND MAP..	Diese CICS- und VTAM-Methoden sind für die Erstellung und Bereitstellung von 3270/SCS-Druckdatenströmen an LUTYPE0-, LUTYPE1- und LUTYPE3-Druckgeräte verantwortlich.	Eine Micro Focus Online Print Exit (DFHUPRNT) - Anwendungsprogrammschnittstelle (API) ermöglicht die Verarbeitung von Druckdaten durch VPSX/MFI, wenn 3270/SCS-Druckdatenströme mit einer dieser Methoden erstellt werden.
FÜHRUNGSKRÄFTE SENDEN TEXT... oder EXEC CICS SEND MAP.. (mit IBM Mainframe-Software von Drittanbietern)	Die CICS- und VTAM-Methoden sind für die Erstellung und Bereitstellung von 3270/SCS-Druckdatenströmen für die Druckgeräte LUTYPE0, LUTYPE1 und LUTYPE3 verantwortlich. Softwareprodukte von Drittanbietern fangen die Druckdaten ab, konvertieren die Daten in Standarddruckformatdaten mit einem ASA/MCH-Steuerzeic	Eine Micro Focus Online Print Exit (DFHUPRNT) - API ermöglicht die Verarbeitung von Druckdaten durch VPSX/MFI, wenn 3270/SCS-Druckdatenströme mit einer dieser Methoden erstellt werden.

	hen und platzieren die Daten auf dem JES-Spool, damit sie von Mainframe-basierte n Drucksystemen verarbeit et werden können, die JES verwenden.	
EXEC CICS SPOOLOPEN	Diese Methode wird von CICS-Anwendungsprogrammen verwendet, um Daten direkt in den JES-Spool zu schreiben . Die Daten stehen dann für die Verarbeitung durch Mainframe-basierte Drucksyst eme zur Verfügung, die JES verwenden.	Micro Focus Enterprise Server spoolt die Daten in den Enterprise Server-Spool, wo sie vom VPSX/MFI Batch Print Exit (LRSPRTE6) verarbeitet werden können, der die Daten auf VPSX spoolt.
DRS/API	Eine von LRS bereitgestellte programmatische Schnittst elle wird zum Schreiben von Druckdaten in JES verwendet.	VPSX/MFI bietet eine Ersatzschnittstelle, die die Druckdaten direkt an VPSX weiterleitet.

Zustandsprüfungen der Druckerflotte

LRS VPSX/MFI (LRS LoadX) kann tiefgreifende Zustandsprüfungen durchführen, einschließlich Geräteverwaltung und Betriebsoptimierung. Die Geräteverwaltung kann Fehler in einem Druckergerät erkennen und die Druckanforderung an einen fehlerfreien Drucker weiterleiten. Weitere Informationen zu umfassenden Integritätsprüfungen für Druckerflotten finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Authentifizierung und Autorisierung drucken

LRS/DIS ermöglicht LRS-Anwendungen die Authentifizierung von Benutzer-IDs und Kennwörtern mithilfe von Microsoft Active Directory oder einem LDAP-Server. Zusätzlich zur grundlegenden Druckautorisierung kann LRS/DIS in den folgenden Anwendungsfällen auch detaillierte Drucksicherheitskontrollen anwenden:

- Legen Sie fest, wer den Druckerauftrag durchsuchen kann.

- Verwaltet die Navigationsebene der Aufträge anderer Benutzer.
- Operative Aufgaben verwalten. Zum Beispiel Sicherheitsfunktionen auf Befehlsebene wie „Sperren/Freigeben“, „Löschen“, „Ändern“, „Kopieren“ und „Umleiten“. Die Sicherheit kann entweder anhand der Benutzer-ID oder der Gruppe (ähnlich der AD-Gruppe oder der LDAP-Gruppe) eingerichtet werden.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verschieben Sie Mainframe-Dateien mit Transfer Family direkt nach Amazon S3

Erstellt von Luis Gustavo Dantas (AWS)

Umgebung: Produktion	Quelle: Mainframe	Ziel: Amazon S3
R-Typ: N/A	Arbeitslast: IBM	Technologien: Mainframe ; Speicher und Backup; Modernisierung
AWS-Services: AWS Transfer-Familie; Amazon S3		

Übersicht

Im Rahmen der Modernisierung können Sie sich der Herausforderung stellen, Dateien zwischen Ihren lokalen Servern und der Amazon Web Services (AWS) Cloud zu übertragen. Die Übertragung von Daten von Mainframes kann eine große Herausforderung sein, da Mainframes in der Regel nicht auf moderne Datenspeicher wie Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) oder Amazon Elastic File System (Amazon EFS) zugreifen können.

Viele Kunden verwenden Intermediate-Staging-Ressourcen wie lokale Linux-, Unix- oder Windows-Server, um Dateien in die AWS-Cloud zu übertragen. Sie können diese indirekte Methode vermeiden, indem Sie AWS Transfer Family mit dem Secure Shell (SSH) File Transfer Protocol (SFTP) verwenden, um Mainframe-Dateien direkt auf Amazon S3 hochzuladen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine virtuelle private Cloud (VPC) mit einem Subnetz, das über Ihre Legacy-Plattform erreichbar ist
- Ein Transfer Family Family-Endpunkt für Ihre VPC
- Mainframe-VSAM-Dateien (Virtual Storage Access Method) wurden in sequentielle Dateien mit fester Länge konvertiert (IBM-Dokumentation)

Einschränkungen

- SFTP überträgt Dateien standardmäßig im Binärmodus, was bedeutet, dass Dateien unter Beibehaltung der EBCDIC-Kodierung auf Amazon S3 hochgeladen werden. Wenn Ihre Datei keine binären oder gepackten Daten enthält, können Sie den Unterbefehl sftp ascii (IBM-Dokumentation) verwenden, um Ihre Dateien während der Übertragung in Text zu konvertieren.
- Sie müssen Mainframe-Dateien (AWS Prescriptive Guidance) entpacken, die gepackte und binäre Inhalte enthalten, um diese Dateien in Ihrer Zielumgebung verwenden zu können.
- Amazon S3 S3-Objekte können eine Größe von mindestens 0 Byte bis zu einem Maximum von 5 TB haben. Weitere Informationen zu den Funktionen von Amazon S3 finden Sie unter Häufig gestellte Fragen zu Amazon S3.

Architektur

Quelltechnologie-Stack

- Sprache zur Jobkontrolle (JCL)
- z/OS Unix-Shell und ISPF
- SFTP
- VSAM und Flatfiles

Zieltechnologie-Stack

- Transfer Family
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)

Zielarchitektur

Das folgende Diagramm zeigt eine Referenzarchitektur für die Verwendung von Transfer Family mit SFTP, um Mainframe-Dateien direkt in einen S3-Bucket hochzuladen.

Das Diagramm zeigt den folgenden Workflow:

1. Sie verwenden einen JCL-Job, um Ihre Mainframe-Dateien über Direct Connect vom Legacy-Mainframe in die AWS-Cloud zu übertragen.
2. Direct Connect ermöglicht es Ihrem Netzwerkverkehr, im globalen AWS-Netzwerk zu bleiben und das öffentliche Internet zu umgehen. Direct Connect verbessert auch die Netzwerkgeschwindigkeit, angefangen bei 50 Mbit/s bis hin zur Skalierung auf bis zu 100 Gbit/s.
3. Der VPC-Endpunkt ermöglicht Verbindungen zwischen Ihren VPC-Ressourcen und den unterstützten Diensten, ohne das öffentliche Internet zu nutzen. Der Zugriff auf Transfer Family und Amazon S3 ermöglicht eine hohe Verfügbarkeit, da er über die elastischen Netzwerkschnittstellen erfolgt, die sich in zwei privaten Subnetzen und Availability Zones befinden.
4. Transfer Family authentifiziert Benutzer und verwendet SFTP, um Ihre Dateien aus der Legacy-Umgebung zu empfangen und in einen S3-Bucket zu verschieben.

Automatisierung und Skalierung

Nachdem der Transfer Family Family-Service eingerichtet wurde, können Sie eine unbegrenzte Anzahl von Dateien vom Mainframe auf Amazon S3 übertragen, indem Sie einen JCL-Job als SFTP-Client verwenden. Sie können die Dateiübertragung auch automatisieren, indem Sie einen Mainframe-Batch-Job-Scheduler verwenden, um die SFTP-Jobs auszuführen, wenn Sie bereit sind, die Mainframe-Dateien zu übertragen.

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.
- Mit der AWS Transfer Family können Sie Ihre wiederkehrenden business-to-business Dateiübertragungen an Amazon S3 und Amazon EFS mithilfe der Protokolle SFTP, FTPS und FTP sicher skalieren.

Epen

Erstellen Sie den S3-Bucket und die Zugriffsrichtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Erstellen Sie einen S3-Bucket, um die Dateien zu hosten, die Sie aus Ihrer Legacy-Umgebung übertragen.	Allgemeines AWS
Erstellen Sie die IAM-Rolle und -Richtlinie.	Transfer Family verwendet Ihre AWS Identity and Access Management (IAM) -Rolle, um Zugriff auf den S3-Bucket zu gewähren, den Sie zuvor erstellt haben. Erstellen Sie eine IAM-Rolle, die die folgende IAM-Richtlinie umfasst: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "UserFolderListing", "Action": [ "s3:ListBucket", "s3:GetBucketLocation" ], "Effect": "Allow", "Resource": [`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"arn:aws:s3:::<your-bucket-name>"
	            ]
	        },
	        {
	            "Sid": "HomeDirObjectAccess",
	            "Effect": "Allow",
	            "Action": [
	"s3:PutObject",
	"s3:GetObjectAcl",
	"s3:GetObject",
	"s3:DeleteObjectVersion",
	"s3:DeleteObject",
	"s3:PutObjectAcl",
	"s3:GetObjectVersion"
	            ],
	            "Resource": "arn:aws:s3:::<your-bucket-name>/*"
	        }
	    ]
	}</pre>
	Hinweis: Sie müssen bei der Erstellung der IAM-Rolle den Anwendungsfall Transfer auswählen.	

Definieren Sie den Transferservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SFTP-Server.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Transfer Family Family-Konsole und wählen Sie dann Server erstellen aus. 2. Wählen Sie nur SFTP (SSH File Transfer Protocol) — Dateiübertragung über das Secure Shell-Protokoll und wählen Sie dann Weiter. 3. Wählen Sie für Identity Provider die Option Service managed und dann Next aus. 4. Wählen Sie als Endpunkttyp die Option VPC Hosted aus. 5. Wählen Sie für Access die Option Intern aus. 6. Wählen Sie unter VPC Ihre VPC aus. 7. Wählen Sie im Abschnitt Availability Zones Ihre Availability Zones und Subnetze aus. 8. Wählen Sie im Abschnitt Sicherheitsgruppen Ihre Sicherheitsgruppe aus und klicken Sie dann auf Weiter.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie für Domain Amazon S3 und dann Weiter aus. 10. Behalten Sie die Standardoptionen auf der Seite Zusätzliche Details konfigurieren bei und wählen Sie dann Weiter. 11. Wählen Sie Create Server (Server erstellen) aus. Hinweis: Weitere Informationen zur Einrichtung eines SFTP-Servers finden Sie unter Erstellen eines SFTP-fähigen Servers (AWS Transfer Family Family-Benutzerhandbuch).	
Holen Sie sich die Serveradresse.	1. Öffnen Sie die Transfer Family Family-Konsole und wählen Sie Ihre Server-ID in der Spalte Server-ID aus. 2. Wählen Sie im Abschnitt Endpunktdetails für Endpunkttyp die Endpunkt-ID aus. Dadurch gelangen Sie zur Amazon VPC-Konsole. 3. Suchen Sie auf der Registerkarte Details der Amazon VPC-Konsole nach den DNS-Namen neben DNS-Namen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SFTP-Client-Schlüsselpaar.	Erstellen Sie ein SSH-Schlüsselpaar für Microsoft Windows oder MacOS/Linux/UNIX.	Allgemeines AWS, SSH

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SFTP-Benutzer.	1. Öffnen Sie die Transfer Family Family-Konsole, wählen Sie im Navigationsbereich Server und wählen Sie dann Ihren Server aus. 2. Wählen Sie in der Spalte Server-ID die Server-ID für Ihren Server aus und klicken Sie dann auf Benutzer hinzufügen. 3. Geben Sie für Username einen Benutzernamen ein, der Ihrem SSH-Schlüsselpaar-Benutzernamen entspricht. 4. Wählen Sie unter Rolle die IAM-Rolle aus, die Sie zuvor erstellt haben. 5. Wählen Sie für das Home-Verzeichnis den S3-Bucket aus, den Sie zuvor erstellt haben. 6. Geben Sie für öffentliche SSH-Schlüssel das key pair ein, das Sie zuvor erstellt haben. 7. Wählen Sie Hinzufügen aus.	Allgemeines AWS

Übertragen Sie die Mainframe-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie den privaten SSH-Schlüssel an den Mainframe.	Verwenden Sie SFTP oder SCP, um den privaten SSH-Schlüssel an die Legacy-Umgebung zu senden.
	
	SFTP-Beispiel:
	
	`sftp [USERNAME@mainframeIP]`
	`[password]`
	`cd [/u/USERNAME]`
	`put [your-key-pair-file]`
	
	SCP-Beispiel:
	
	`scp [your-key-pair-file] [USERNAME@MainframeIP]:/[u/USERNAME]`
	
	Als Nächstes speichern Sie den SSH-Schlüssel im z/OS Unix-Dateisystem unter dem Benutzernamen, der später den Dateiübertragungs-Batchjob ausführen wird (z. B.). `/u/CONTROLM`
	
	Hinweis: Weitere Informationen zur z/OS Unix-Shell finden Sie unter Eine Einführung in die z/OS-Shells (IBM-Dokumentation).
		Mainframe, z/OS Unix-Shell, FTP, SCP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den JCL-SFTP-Client.	Da Mainframes keinen systemeigenen SFTP-Client haben, müssen Sie das BPXBATCH-Hilfsprogramm verwenden, um den SFTP-Client von der z/OS Unix-Shell aus auszuführen.
	
	Erstellen Sie im ISPF-Editor den JCL-SFTP-Client. Beispielsweise:
	
	`//JOBNAM JOB ...`
	`//************`
	`**********`
	`**********`
	`**********`
	`****`
	`//SFTP EXEC PGM=BPXBATCH,REGION=0M`
	`//STDPARM DD *`
	`SH cp "//'MAINFRAME.FILE.NAME'" filename.txt;`
	`echo 'put filename.txt' > uplcmd;`
	`sftp -b uplcmd -i ssh_private_key_file ssh_username@<transfer service ip or DNS>;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`
	
	Hinweis: Weitere Informationen zur Ausführung eines
		JCL, Mainframe, z/OS Unix-Shell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Befehls in der z/OS Unix-Shell finden Sie unter The BPXBATCH utility (IBM-Dokumentation). Weitere Informationen zum Erstellen oder Bearbeiten von JCL-Jobs in z/OS finden Sie unter Was ist ISPF? und Der ISPF-Editor (IBM-Dokumentation).	
Führen Sie den JCL-SFTP-Client aus.	1. Geben Sie im ISPF-Editor SUB ein und drücken Sie dann die EINGABETASTE, nachdem der JCL-Job erstellt wurde. 2. Überwachen Sie die Batch-Job-Aktivität des Mainframes zur Dateiübertragung in SDSF. Hinweis: Weitere Informationen zur Überprüfung der Aktivität von Batch-Jobs finden Sie im z/OS SDSF User's Guide (IBM-Dokumentation).	Mainframe, JCL, ISPF

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Dateiübertragung.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann im Navigationsbereich Buckets aus. 2. Wählen Sie den Bucket aus, der Ihrer Transfer Family zugeordnet ist. 3. Suchen Sie auf der Registerkarte „Objekte“ im Bereich „Objekte“ nach der Datei, die Sie vom Mainframe übertragen haben.	Allgemeines AWS
Automatisieren Sie den JCL-SFTP-Client.	Verwenden Sie den Job-Scheduler, um den JCL-SFTP-Client automatisch auszulösen. Hinweis: Sie können Mainframe-Job-Scheduler wie BMC Control-M oder CA Workload Automation verwenden, um Batch-Jobs für Dateiübertragungen auf der Grundlage von Zeit und anderen Abhängigkeiten von Batch-Jobs zu automatisieren.	Jobplaner

Zugehörige Ressourcen

- So funktioniert die AWS Transfer Family

- Mainframe-Modernisierung mit AWS

Übertragen Sie umfangreiche Db2-z/OS-Daten in CSV-Dateien an Amazon S3

Erstellt von Bruno Sahinoglu (AWS), Ister (AWS) und Abhijit K Shirsagar (AWS)

Code-Repository: Entladen von DB2 z/OS zu S3	Umgebung: Produktion	Quelle: Db2
Ziel: Amazon S3	R-Typ: Plattformwechsel	Workload: IBM
Technologien: Mainframe; Data Lakes; Datenbanken; Softwareentwicklung und -tests; Migration	AWS-Services: Amazon Aurora; AWS Glue ;Amazon S3; AWS Transfer Family; Amazon Athena	

Übersicht

Ein Mainframe ist in vielen Unternehmen immer noch ein Aufzeichnungssystem, das eine riesige Datenmenge enthält, einschließlich Master-Datenentitäten mit Aufzeichnungen über aktuelle und historische Geschäftstransaktionen. Es ist oft isoliert und kann nicht einfach von den verteilten Systemen innerhalb desselben Unternehmens aufgerufen werden. Mit dem Aufkommen der Cloud-Technologie und der Big-Data-Deokratisierung möchten Unternehmen die in den Mainframe-Daten versteckten Erkenntnisse nutzen, um neue Geschäftskapazitäten zu entwickeln.

Mit diesem Ziel möchten Unternehmen ihre Mainframe-Db2-Daten in ihrer Amazon Web Services (AWS) Cloud-Umgebung öffnen. Die geschäftlichen Gründe sind mehrere und die Übertragungsmethoden unterscheiden sich von Fall zu Fall. Möglicherweise möchten Sie Ihre Anwendung direkt mit dem Mainframe verbinden oder Ihre Daten nahezu in Echtzeit replizieren. Wenn der Anwendungsfall darin besteht, ein Data Warehouse oder einen Data Lake zu speist, ist eine up-to-date Kopie kein Problem mehr, und das in diesem Muster beschriebene Verfahren kann ausreichend sein, insbesondere wenn Sie Lizenzkosten für Produkte von Drittanbietern vermeiden möchten. Ein weiterer Anwendungsfall könnte die Mainframe-Datenübertragung für ein Migrationsprojekt sein. In einem Migrationsszenario sind Daten für die Durchführung des funktionalen Gleichheitstests erforderlich. Der in diesem Beitrag beschriebene Ansatz ist eine kostengünstige Möglichkeit, die Db2-Daten in die AWS Cloud-Umgebung zu übertragen.

Da Amazon Simple Storage Service (Amazon S3) einer der am stärksten integrierten AWS-Services ist, können Sie von dort aus auf die Daten zugreifen und Erkenntnisse direkt sammeln, indem Sie andere AWS-Services wie Amazon Athena ,AWS Lambda-Funktionen oder Amazon verwenden QuickSight . Sie können die Daten auch mithilfe von AWS Glue oder AWS Database Migration Service (AWS DMS) in Amazon Aurora oder Amazon DynamoDB laden. Vor diesem Hintergrund beschreibt dies, wie Db2-Daten in CSV-Dateien im ASCII-Format auf dem Mainframe entladen und an Amazon S3 übertragen werden.

Zu diesem Zweck wurden Mainframe-Skripts entwickelt, um Job Control Languages (JCLs) zu generieren, um so viele Db2-Tabellen wie nötig zu entladen und zu übertragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Benutzer des IBM z/OS-Betriebssystems mit der Berechtigung, Restructured Extended Executor (REXX)- und JCL-Skripts auszuführen.
- Zugriff auf z/OS Unix System Services (USS), um private und öffentliche SSH-Schlüssel (Secure Shell) zu generieren.
- Ein beschreibbarer S3-Bucket. Weitere Informationen finden Sie unter Erstellen Ihres ersten S3-Buckets in der Amazon S3-Dokumentation.
- Ein AWS Transfer Family SSH File Transfer Protocol (SFTP)-fähiger Server, der den als Identitätsanbieter verwalteten Service und Amazon S3 als AWS-Speicherservice verwendet. Weitere Informationen finden Sie unter Erstellen eines SFTP-fähigen Servers in der AWS Transfer Family-Dokumentation.

Einschränkungen

- Dieser Ansatz eignet sich nicht für die Datensynchronisierung nahezu in Echtzeit oder in Echtzeit.
- Daten können nur von Db2 z/OS nach Amazon S3 verschoben werden, nicht umgekehrt.

Architektur

Quelltechnologie-Stack

- Mainframe mit Db2 auf z/OS

Zieltechnologie-Stack

- AWS Transfer Family
- Amazon S3
- Amazon Athena
- Amazon QuickSight
- AWS Glue
- Amazon Relational Database Service (Amazon RDS)
- Amazon Aurora
- Amazon Redshift

Quell- und Zielarchitektur

Das folgende Diagramm zeigt den Prozess zum Generieren, Extrahieren und Übertragen von Db2-z/OS-Daten im ASCII-CSV-Format in einen S3-Bucket.

1. Eine Liste von Tabellen wird für die Datenmigration aus dem Db2-Katalog ausgewählt.
2. Die Liste wird verwendet, um die Generierung von Entladeaufträgen mit den numerischen Spalten und Datenspalten im externen Format voranzutreiben.
3. Die Daten werden dann mithilfe von AWS Transfer Family an Amazon S3 übertragen.
4. Ein AWS Glue Extract, Transform, Load (ETL)-Auftrag kann die Daten transformieren und im angegebenen Format in einen verarbeiteten Bucket laden, oder AWS Glue kann die Daten direkt in die Datenbank einlesen.
5. Amazon Athena und Amazon QuickSight können verwendet werden, um die Daten abzufragen und zu rendern, um Analysen voranzutreiben.

Das folgende Diagramm zeigt einen logischen Ablauf des gesamten Prozesses.

1. Die erste JCL namens TABNAME verwendet das Db2-Dienstprogramm DSNTIAUL, um die Liste der Tabellen zu extrahieren und zu generieren, die Sie aus Db2 entladen möchten. Um Ihre Tabellen auszuwählen, müssen Sie die SQL-Eingabe manuell anpassen, um Filterkriterien auszuwählen und hinzuzufügen, die ein oder mehrere Db2-Schemas enthalten.

2. Die zweite JCL namens REXXEXEC verwendet das JCL-Skeleton und das REXX-Programm, das bereitgestellt wird, um die vom JCL TABNAME erstellte Tabellenliste zu verarbeiten und eine JCL pro Tabellenname zu generieren. Jede JCL enthält einen Schritt zum Entladen der Tabelle und einen weiteren Schritt zum Senden der Datei an den S3-Bucket mithilfe des SFTP-Protokolls.
3. Der letzte Schritt besteht darin, die JCL auszuführen, um die Tabelle zu entladen und die Datei an AWS zu übertragen. Der gesamte Prozess kann mit einem lokalen Scheduler oder in AWS automatisiert werden.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- AWS Glue ist ein vollständig verwalteter ETL-Service (Extract, Transform, Load). Es hilft Ihnen, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon QuickSight ist ein Cloud-Scale Business Intelligence (BI)-Service, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Amazon Redshift ist ein verwalteter Data Warehouse-Service im Petabyte-Bereich in der AWS Cloud.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Transfer Family ist ein sicherer Übertragungsservice, mit dem Sie Dateien in und aus AWS-Speicherservices übertragen können.

Mainframe-Tools

- SSH File Transfer Protocol (SFTP) ist ein sicheres Dateiübertragungsprotokoll, das die Fernanmeldung zu und die Dateiübertragung zwischen Servern ermöglicht. SSH bietet Sicherheit, indem der gesamte Datenverkehr verschlüsselt wird.

- DSNTIAUL ist ein Beispielprogramm, das von IBM zum Entladen von Daten bereitgestellt wird.
- DSNUTILB ist ein Hilfsprogramm, das von IBM zum Entladen von Daten mit verschiedenen Optionen von DSNTIAUL bereitgestellt wird.
- z/OS OpenSSH ist ein Port von Open Source Software SSH, der auf dem Unix System Service unter dem IBM-Betriebssystem z/OS ausgeführt wird. SSH ist ein sicheres, verschlüsseltes Verbindungsprogramm zwischen zwei Computern, die in einem TCP/IP-Netzwerk ausgeführt werden. Es bietet mehrere Dienstprogramme, einschließlich ssh-keygen.
- Das REXX-Skript (Restructured Extended Executor) wird verwendet, um die JCL-Generierung mit den Schritten Db2 Unload und SFTP zu automatisieren.

Code

Der Code für dieses Muster ist im GitHub deloaddb2-Repository verfügbar.

Bewährte Methoden

Beim ersten Entladen sollten die generierten JCLs die gesamten Tabellendaten entladen.

Führen Sie nach dem ersten vollständigen Entladen inkrementelle Entladungen durch, um die Leistung zu verbessern und Kosten zu sparen. pdate die SQL-Abfrage in der JCL-Vorlage, um Änderungen am Entladevorgang zu berücksichtigen.

Sie können das Schema manuell oder mithilfe eines Skripts auf Lambda mit dem Db2 SYSPUNCH als Eingabe konvertieren. Für einen industriellen Prozess ist AWS Schema Conversion Tool (SCT) die bevorzugte Option.

Verwenden Sie abschließend einen Mainframe-basierten Scheduler oder einen Scheduler auf AWS mit einem Agenten auf dem Mainframe, um den gesamten Prozess zu verwalten und zu automatisieren.

Polen

Einrichten des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Anweisungen finden Sie unter Erstellen Ihres ersten S3-Buckets.	Allgemeines AWS

Einrichten des Transfer Family-Servers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SFTP-fähigen Server.	Gehen Sie wie folgt vor, um einen SFTP-Server in der AWS Transfer Family-Konsole zu öffnen und zu erstellen: 1. Aktivieren Sie auf der Seite Protokolle auswählen das Kontrollkästchen SFTP (SSH File Transfer Protocol) – Dateiübertragung über Secure Shell. 2. Wählen Sie für den Identitätsanbieter die Option Serviceverwaltet aus. 3. Wählen Sie für den Endpunkt Öffentlich zugänglich aus. 4. Wählen Sie für die Domain Amazon S3 aus. 5. Behalten Sie auf der Seite Zusätzliche Details konfiguri	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eren die Standardeinstellungen bei. 6. Erstellen Sie den Server.	
Erstellen Sie eine IAM-Rolle für Transfer Family.	Um eine AWS Identity and Access Management (IAM)-Rolle für Transfer Family für den Zugriff auf Amazon S3 zu erstellen, folgen Sie den Anweisungen unter Erstellen einer IAM-Rolle und -Richtlinie.	AWS-Administrator
Fügen Sie einen serviceverwalteten Amazon S3-Benutzer hinzu.	Um den serviceverwalteten Amazon S3-Benutzer hinzuzufügen, folgen Sie den Anweisungen in der AWS-Dokumentation und verwenden Sie Ihre Mainframe-Benutzer-ID.	Allgemeines AWS

Sichern des Kommunikationsprotokolls

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SSH-Schlüssel.	Führen Sie in Ihrer Mainframe-USS-Umgebung den folgenden Befehl aus. `ssh-keygen -t rsa` Hinweis: Wenn Sie zur Eingabe einer Passphrase	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aufgefordert werden, lassen Sie sie leer.	

Geben Sie die richtigen Autorisierungsstufen für den SSH-Ordner und die Schlüssel dateien an.	Standardmäßig werden die öffentlichen und privaten Schlüssel im Benutzerv erzeichnis gespeichert `/u/home/username/.ssh` .
	
	Sie müssen die Autorisierung 644 für die Schlüsseldateien und 700 für den Ordner erteilen.
	
	`chmod 644 .ssh/id_rsa`
	`chmod 700 .ssh`
		Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie den Inhalt des öffentlichen Schlüssels in Ihren serviceverwalteten Amazon S3-Benutzer.	Öffnen Sie die AWS Transfer Family-Konsole, um den von USS generierten öffentlichen Schlüsselinhalt zu kopieren. 1. Klicken Sie im Navigationsbereich auf Servers (Server). 2. Wählen Sie die Kennung in der Spalte Server-ID aus, um die Serverdetails anzuzeigen 3. Wählen Sie unter Benutzer einen Benutzernamen aus, um die Benutzerdetails anzuzeigen 4. Wählen Sie unter Öffentliche SSH-Schlüssel die Option Öffentlichen SSH-Schlüssel hinzufügen aus, um den öffentlichen Schlüssel einem Benutzer hinzuzufügen. Geben Sie für den öffentlichen SSH-Schlüssel Ihren öffentlichen Schlüssel ein. Ihr Schlüssel wird vom Service validiert, bevor Sie Ihren neuen Benutzer hinzufügen können. 5. Wählen Sie Schlüssel hinzufügen.	Mainframe-Entwickler

Generieren der JCLs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die Db2-Tabellenliste im Umfang.	Geben Sie Eingabe-SQL an, um eine Liste der Tabellen zu erstellen, die für die Datenmigration vorgesehen sind. In diesem Schritt müssen Sie Auswahlkriterien angeben, die die Db2-Katalogtabelle SYSIBM.SYSTABLES mithilfe einer SQL-Klausel abfragen. Filter können so angepasst werden, dass sie bestimmte Schema- oder Tabellennamen enthalten, die mit einem bestimmten Präfix oder basierend auf einem Zeitstempel für das inkrementelle Entladen beginnen. Die Ausgabe wird in einem physischen sequentiellen Datensatz (PS) auf dem Mainframe erfasst. Dieser Datensatz dient als Eingabe für die nächste Phase der JCL-Generierung. Bevor Sie den JCL TABNAME verwenden (Sie können ihn bei Bedarf umbenennen), nehmen Sie die folgenden Änderungen vor: 1. Ersetzen Sie <Jobcard> durch eine Auftragsk	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lasse und einen Benutzer, der zum Ausführen von Db2-Dienstprogrammen autorisiert ist. 2. Ersetzen Sie <HLQ1> oder passen Sie die Namen der Ausgabedatensätze an Ihre Standortstandards an. 3. Aktualisieren Sie den STEPLIB-Stack von PDSEs (partitionierter Datensatz erweitert) gemäß Ihren Website-Standards. Das Beispiel in diesem Muster verwendet die IBM-Stand ardeinstellungen. 4. Ersetzen Sie den PLAN-Namen und die LIB durch Ihre installationsspezi fischen Werte. 5. Ersetzen Sie <Schema> und <Präfix> durch Ihre Auswahlkriterien für den Db2-Katalog. 6. Speichern Sie die resultier ende JCL in einer PDS-Bibliothek (partitionierter Datensatz). 7. Senden Sie die JCL. Db2-Tabellenlisten-Extrakti onsauftrag	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<Jobcard>
	//*
	//* UNLOAD ALL THE TABLE
	 NAMES FOR A PARTICULAR
	 SCHEMA
	//*
	//STEP01 EXEC PGM=IEFBR
	14
	//*
	//DD1 DD DISP=(MOD
	,DELETE,DELETE),
	// UNIT=SYSDA,
	// SPACE=(1000,
	(1,1)),
	// DSN=<HLQ1
	>.DSN81210.TABLIST
	//*
	//DD2 DD DISP=(MOD
	,DELETE,DELETE),
	// UNIT=SYSDA,
	// SPACE=(1000,
	(1,1)),
	// DSN=<HLQ1
	>.DSN81210.SYSPUNCH
	//*
	//UNLOAD EXEC PGM=IKJEF
	T01,DYNAMNBR=20
	//SYSTSPRT DD
	 SYSOUT=*
	//STEPLIB DD
	 DISP=SHR,DSN=DSNC1
	0.DBCG.SDSNEXIT
	// DD DISP=SHR,
	DSN=DSNC10.SDSNLOAD
	// DD DISP=SHR,
	DSN=CEE.SCEERUN
	// DD DISP=SHR,
	DSN=DSNC10.DBCG.RU
	NLIB.LOAD
	//SYSTSIN DD *
	  DSN SYSTEM(DBCG)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> RUN PROGRAM(D
	SNTIAUL) PLAN(DSNT
	IB12) PARMS('SQL') -
	       LIB('DSNC
	10.DBCG.RUNLIB.LOAD')
	  END
	//SYSPRINT DD SYSOUT=*
	//*
	//SYSUDUMP DD SYSOUT=*
	//*
	//SYSREC00 DD DISP=(NEW
	,CATLG,DELETE),
	// UNIT=SYSD
	A,SPACE=(32760,(10
	00,500)),
	// DSN=<HLQ1
	>.DSN81210.TABLIST
	//*
	//SYSPUNCH DD DISP=(NEW
	,CATLG,DELETE),
	// UNIT=SYSD
	A,SPACE=(32760,(10
	00,500)),
	// VOL=SER=S
	CR03,RECFM=FB,LREC
	L=120,BLKSIZE=12
	// DSN=<HLQ1
	>.DSN81210.SYSPUNCH
	//*
	//SYSIN DD *
	   SELECT CHAR(CREA
	TOR), CHAR(NAME)
	     FROM SYSIBM.SY
	STABLES
	    WHERE OWNER =
	 '<Schema>'
	      AND NAME LIKE
	 '<Prefix>%'
	      AND TYPE = 'T';
	/*</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die JCL-Vorlagen.	Die JCL-Vorlagen, die mit diesem Muster bereitgestellt werden, enthalten eine generische Auftragskarte und Bibliotheksnamen. Die meisten Mainframe-Standorte haben jedoch ihre eigenen Benennungsstandards für Datensatznamen, Bibliotheksnamen und Auftragskarten. Beispielsweise kann eine bestimmte Auftragsklasse erforderlich sein, um Db2-Aufträge auszuführen. Die Implementierungen JES2 und JES3 von Job Entry Subsytem können zusätzliche Änderungen verursachen. Standard-Ladebibliotheken haben möglicherweise einen anderen ersten Qualifizierer als `SYS1`, was der IBM-Standard ist. Passen Sie daher die Vorlagen so an, dass sie Ihre standortspezifischen Standards berücksichtigen, bevor Sie sie ausführen. Nehmen Sie die folgenden Änderungen in der -Skeleton-JCL UNLDSKEL vor: 1. Ändern Sie die Auftragskarte mit einer Auftragsklasse und einem Benutzer,	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der zum Ausführen von Db2-Dienstprogrammen autorisiert ist. 2. Passen Sie die Namen der Ausgabedatensätze an Ihre Standortstandards an. 3. Aktualisieren Sie den STEPLIB-Stack von PDSEs gemäß Ihren Website-S tandards. Das Beispiel in diesem Muster verwendet die IBM-Standardeinste llungen. 4. Ersetzen Sie durch Ihren Db2-Subsystemnamen und <DSN> Ihre Korrelations-ID. 5. Speichern Sie die resultier ende JCL in einer PDS-Bibliothek, die Teil Ihres ISPSLIB-Stacks ist. Dabei handelt es sich um die standardmäßige Bibliothek mit -Skeleton-Vorlagen für ISPF. Entladen und SFTP-JCL-Skeleton `//&USRPFX.U JOB (DB2UNLOAD),'JOB', CLASS=A,MSGCLASS=A, //  TIME=1440 ,NOTIFY=&USRPFX //* DELETE DATASETS`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`//STEP01 EXEC PGM=IEFBR14`
	`//DD01 DD DISP=(MOD,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(TRK,(1,1)),`
	`// DSN=&USRPFX..DB2.PUNCH.&JOBNAME`
	`//DD02 DD DISP=(MOD,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(TRK,(1,1)),`
	`// DSN=&USRPFX..DB2.UNLOAD.&JOBNAME`
	`//*`
	`//* RUNNING DB2 EXTRACTION BATCH JOB FOR AWS DEMO`
	`//*`
	`//UNLD01 EXEC PGM=DSNUTILB,REGION=0M,`
	`// PARM='<DSN>,UNLOAD'`
	`//STEPLIB DD DISP=SHR,DSN=DSNC10.DBCG.SDSNEXIT`
	`// DD DISP=SHR,DSN=DSNC10.SDSNLOAD`
	`//SYSPRINT DD SYSOUT=*`
	`//UTPRINT DD SYSOUT=*`
	`//SYSOUT DD SYSOUT=*`
	`//SYSPUN01 DD DISP=(NEW,CATLG,DELETE),`
	`// SPACE=(CYL,(1,1),RLSE),`
	`// DSN=&USRPFX..DB2.PUNCH.&JOBNAME`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`//SYSREC01 DD`
	` DISP=(NEW,CATLG,DE`
	`LETE),`
	`//  SPACE=(CY`
	`L,(10,50),RLSE),`
	`// DSN=&USRPFX..DB2.U`
	`NLOAD.&JOBNAME`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSIN  DD *`
	`  UNLOAD`
	`  DELIMITED COLDEL ','`
	`  FROM TABLE &TABNAME`
	`  UNLDDN SYSREC01`
	`  PUNCHDDN SYSPUN01`
	`  SHRLEVEL CHANGE`
	` ISOLATION UR;`
	` /*`
	`//*`
	`//* FTP TO AMAZON S3`
	` BACKED FTP SERVER IF`
	` UNLOAD WAS SUCCESSFUL`
	`//*`
	`//SFTP EXEC PGM=BPXBA`
	`TCH,COND=(4,LE),RE`
	`GION=0M`
	`//STDPARM DD *`
	` SH cp "//'&USRP`
	`FX..DB2.UNLOAD.&JO`
	`BNAME'"`
	`  &TABNAME..csv;`
	` echo "ascii`
	` " >> uplcmd;`
	` echo "PUT &TABNAME.`
	`.csv " >>>> uplcmd;`
	` sftp -b uplcmd -i .ssh/`
	`id_rsa &FTPUSER.`
	`@&FTPSITE;`
	` rm &TABNAME..csv;`
	` //SYSPRINT DD SYSOUT=*`
	` //STDOUT DD SYSOUT=*`
	` //STDENV DD *`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`//STDERR DD SYSOUT=*`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die JCL für Massenentladungen.	Dieser Schritt beinhaltet die Ausführung eines REXX-Skripts in einer ISPF-Umgebung mithilfe von JCL. Geben Sie die Liste der Tabellen im Umfang an, die im ersten Schritt als Eingabe für die Massen-JCL-Generierung anhand des `TABLIST DD` Namens erstellt wurden. Die JCL generiert eine neue JCL pro Tabellenname in einem benutzerdefinierten partitionierten Datensatz, der für den `ISPFILE DD` Namen angegeben ist. Weisen Sie diese Bibliothek im Voraus zu. Jede neue JCL besteht aus zwei Schritten: einem Schritt zum Entladen der Db2-Tabelle in eine Datei und einem Schritt zum Senden der Datei an den S3-Bucket. Nehmen Sie die folgenden Änderungen in der JCL REXXEXEC vor (Sie können den Namen ändern): 1. Ersetzen Sie durch `Job card user ID` eine Mainframe-Benutzer-ID, die über Entladeberechtigung für die Tabellen verfügt. Ersetzen Sie den	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ISPTLIB` <HLQ1> Wert `SYSPROC`, `ISPPLIB`, `ISPSLIBISPMLIB`, und oder passen Sie an, `DSN` um Ihre Website-Standards zu erfüllen. Um Ihre installat ionsspezifischen Werte zu ermitteln, verwenden Sie den Befehl `TSO ISRDDN`. 2. Ersetzen Sie durch <MFUSER> eine Benutzer-ID, die über Berechtigungen zur Auftragsausführung in Ihrer Installation verfügt. 3. Ersetzen Sie <FTPUSER> durch eine Benutzer-ID, die in Ihrer Installation über die USS- und FTP-Berechtigung verfügt. Es wird davon ausgegangen, dass diese Benutzer-ID und ihre SSH-Sicherheitssch lüssel im entsprechenden Unix Systems Services-Verzeichnis auf dem Mainframe vorhanden sind. 4. Ersetzen Sie durch <AWS `TransferFamily IP>` die IP-Adresse der AWS Transfer Family oder den Domänennamen. Diese Adresse wird für den SFTP-Schritt verwendet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Reichen Sie die JCL ein, nachdem Sie die Website-Standardnutzung angewendet und das REXX-Programm wie unten beschrieben aktualisiert haben.
	
	Massen-JCL-Generierungsauftrag
	
	`//RUNREXX JOB (CREATEJCL),'RUNS ISPF TABLIST', CLASS=A,MSGCLASS=A,`
	
	`//  TIME=1440 ,NOTIFY=&SYSUID`
	`//* Most of the values required can be updated to your site specific`
	`//* values using the command 'TSO ISRDDN' in your ISPF session.`
	`//* Update all the lines tagged with //update marker to desired`
	`//* site specific values.`
	`//ISPF EXEC PGM=IKJEFT01,REGION=2048K,DYNAMNBR=25`
	`//SYSPROC DD DISP=SHR,DSN=USER.Z23D.CLIST`
	`//SYSEXEC DD DISP=SHR,DSN=<HLQ1>.TEST.REXXLIB`
	`//ISPPLIB DD DISP=SHR,DSN=ISP.SISPPENU`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`//ISPSLIB DD DISP=SHR,DSN=ISP.S ISPSENU`
	`// DD DISP=SHR,DSN=<HLQ1 >.TEST.ISPSLIB`
	`//ISPMLIB DD DSN=ISP.SISPMENU,D ISP=SHR`
	`//ISPTLIB DD DDNAME=ISPTABL`
	`// DD DSN=ISP.S ISPTENU,DISP=SHR`
	`//ISPTABL DD LIKE=ISP.SISPTENU, UNIT=VIO`
	`//ISPPROF DD LIKE=ISP.SISPTENU, UNIT=VIO`
	`//ISPLOG DD SYSOUT=*,RECFM=VA, LRECL=125`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSUDUMP DD SYSOUT=*`
	`//SYSDBOUT DD SYSOUT=*`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSUDUMP DD SYSOUT=*`
	`//SYSDBOUT DD SYSOUT=*`
	`//SYSHELP DD DSN=SYS1.HELP,DISP =SHR`
	`//SYSOUT DD SYSOUT=*`
	`//* Input list of tablenames`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>//TABLIST DD
	DISP=SHR,DSN=<HLQ1
	>.DSN81210.TABLIST
	//* Output pds
	//ISPFILE DD
	DISP=SHR,DSN=<HLQ1
	>.TEST.JOBGEN
	//SYSTSIN DD *
	ISPSTART CMD(ZSTEPS
	<MFUSER> <FTPUSER> <AWS
	TransferFamily IP>)
	/*</pre>
	Bevor Sie das REXX-Skript verwenden, nehmen Sie die folgenden Änderungen vor:
	1. Speichern Sie das REXX-Skript in einer PDS-Bibliothek, die unter dem SYSEXECStack in der im vorherigen Schritt bearbeiteten JCL REXXEXEC definiert ist, mit ZSTEPS als Mitgliedsnamen. Wenn Sie sie umbenennen möchten, sollten Sie die JCL entsprechend Ihren Anforderungen aktualisieren.
	2. Dieses Skript verwendet die Trace-Option, um zusätzliche Informationen zu drucken, falls Fehler auftreten. Sie können stattdessen Fehlerbehandlungscode nach	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den TSO Anweisung en EXECIOISPEXEC, und hinzufügen und die Ablaufverfolgungszeile entfernen.
	3. Dieses Skript generiert Mitgliedsnamen unter Verwendung der LODnnnnn Namenskonvention, die bis zu 100.000 Mitglieder unterstützen kann. Wenn Sie mehr als 100.000 Tabellen haben, verwenden Sie ein kürzeres Präfix und passen Sie die Zahlen in der tempjob Anweisung an.
	
	ZSTEPS REXX-Skript
	
	`/*REXX - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */`
	`/* 10/27/2021 - added new parms to accommodate ftp */`
	`Trace "o"`
	`parse arg usrpfx ftpuser ftpsite`
	`Say "Start"`
	`Say "Ftpuser: " ftpuser "Ftpsite:" ftpsite`
	`Say "Reading table name list"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"EXECIO * DISKR TABLIST (STEM LINE. FINIS" DO I = 1 TO LINE.0 Say I suffix = I Say LINE.i Parse var LINE.i schema table rest tabname = schema !! "." !! table Say tabname tempjob= "LOD" !! RIGHT("0000" !! i, 5) jobname=tempjob Say tempjob ADDRESS ISPEXEC "FTOPEN " ADDRESS ISPEXEC "FTINCL UNLDSKEL" /* member will be saved in ISPDSN library allocated in JCL */ ADDRESS ISPEXEC "FTCLOSE NAME("tem pjob")" END ADDRESS TSO "FREE F(TABLIST) " ADDRESS TSO "FREE F(ISPFILE) " exit 0	

Ausführen der JCLs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Schritt Db2 Entladen aus.	Nach der JCL-Generierung haben Sie so viele JCLs wie Tabellen, die entladen werden müssen. Diese Geschichte verwendet ein JCL-generiertes Beispiel, um die Struktur und die wichtigsten Schritte zu erläutern. Von Ihrer Seite aus ist keine Aktion erforderlich. Die folgenden Informationen dienen nur als Referenz. Wenn Sie beabsichtigen, die JCLs einzureichen, die Sie im vorherigen Schritt generiert haben, fahren Sie mit der Aufgabe LODnnnnn JCLs senden fort. Wenn Sie Db2-Daten mithilfe einer JCL mit dem von IBM bereitgestellten DSNUTILB Db2-Dienstprogramm entladen, müssen Sie sicherstellen, dass die entladenen Daten keine komprimierten numerischen Daten enthalten. Verwenden Sie dazu den `DELIMITED` Parameter DSNUTILB.	Mainframe-Entwickler, Systemingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der `DELIMITED` Parameter unterstützt das Entladen der Daten im CSV-Format, indem ein Zeichen als Trennzeic hen und doppelte Anführung szeichen für das Textfeld hinzugefügt, das Padding in der Spalte VARCHAR entfernt und alle numerischen Felder in EXTERNAL FORMAT konvertiert werden, einschlie ßlich der DATE-Felder. Das folgende Beispiel zeigt, wie der Entladeschritt in der generierten JCL aussieht, wobei das Kommazeichen als Trennzeichen verwendet wird. `UNLOAD DELIMITED COLDEL ',' FROM TABLE SCHEMA_NAME.TBNAME UNLDDN SYSREC01 PUNCHDDN SYSPUN01 SHRLEVEL CHANGE ISOLATION UR;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den SFTP-Schritt aus.	Um das SFTP-Protokoll aus einer JCL zu verwenden, verwenden Sie das Hilfsprogramm BPXBATCH. Das SFTP-Dienstprogramm kann nicht direkt auf die MVS-Datensätze zugreifen. Sie können den Kopierbefehl (`cp`) verwenden, um die sequenzielle Datei in das USS-Verzeichnis `&USRPFX..DB2.UNLOAD.&JOBNAME` zu kopieren, wo sie wird`&TABNAME..csv` . Führen Sie den `sftp` Befehl mit dem privaten Schlüssel (`id_rsa`) aus und verwenden Sie die RACF-Benutzer-ID als Benutzernamen, um eine Verbindung mit der IP-Adresse der AWS Transfer Family herzustellen. `SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'" &TABNAME..csv; echo "ascii " >> uplcmd; echo "PUT &TABNAME..csv " >>>> uplcmd; sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTP_TF_SITE;`	Mainframe-Entwickler, Systemingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rm &TABNAME..csv;`	
Senden Sie die LODnnnnn-JCLs.	Die vorherige JCL hat alle LODnnnnn-JCL-Tabellen generiert, die entladen, in CSV umgewandelt und in den S3-Bucket übertragen werden müssen. Führen Sie den `submit` Befehl für alle generierten JCLs aus.	Mainframe-Entwickler, Systemingenieur

Zugehörige Ressourcen

Weitere Informationen zu den verschiedenen Tools und Lösungen, die in diesem Dokument verwendet werden, finden Sie im Folgenden:

- z/OS-OpenSSH-Benutzerhandbuch
- Db2 z/OS – Beispiel für UNLOAD-Steueranweisungen
- Db2 z/OS – Entladen getrennter Dateien
- Transfer Family – Erstellen eines SFTP-fähigen Servers
- Transfer Family – Arbeiten mit serviceverwalteten Benutzern

Zusätzliche Informationen

Nachdem Sie Ihre Db2-Daten auf Amazon S3 gespeichert haben, haben Sie viele Möglichkeiten, neue Erkenntnisse zu entwickeln. Da Amazon S3 in AWS-Datenanalyseservices integriert ist, können Sie diese Daten frei nutzen oder auf verteilter Seite verfügbar machen. Sie können z. B. Folgendes tun:

- Erstellen Sie einen Data Lake auf Amazon S3 und extrahieren Sie wertvolle Erkenntnisse mithilfe von query-in-place, Analysen und Machine-Learning-Tools, ohne die Daten zu verschieben.

- Initiieren Sie eine Lambda-Funktion, indem Sie einen Workflow zur Verarbeitung nach dem Hochladen einrichten, der in AWS Transfer Family integriert ist.
- Entwickeln Sie neue Microservices für den Zugriff auf die Daten in Amazon S3 oder in einer vollständig verwalteten Datenbank, indem Sie AWS Glue verwenden, einen Serverless-Datenintegrationsservice, der das Erkennen, Vorbereiten und Kombinieren von Daten für Analysen, Machine Learning und Anwendungsentwicklung vereinfacht.

Da Sie in einem Migrationsanwendungsfall beliebige Daten vom Mainframe auf S3 übertragen können, haben Sie folgende Möglichkeiten:

- Außerbetriebnahme der physischen Infrastruktur und Erstellung einer kostengünstigen Datenarchivierungsstrategie mit Amazon S3 Glacier und S3 Glacier Deep Archive.
- Erstellen Sie skalierbare, dauerhafte und sichere Backup- und Wiederherstellungslösungen mit Amazon S3 und anderen AWS-Services wie S3 Glacier und Amazon Elastic File System (Amazon EFS), um vorhandene On-Premises-Funktionen zu erweitern oder zu ersetzen.

Mehr Muster

- Replizieren von Mainframe-Datenbanken in AWS mithilfe von Precisely Connect

Management & Governance

Themen

Identifizieren und warnen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS-Schlüssel verschlüsselt sind

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Management und Governance; Analytik; Big Data; Cloudnativ; Infrastruktur; Sicherheit, Identität, Compliance	AWS-Services: AWS CloudTrail; Amazon CloudWatch; AWS Identity and Access Management ; Amazon Kinesis ; AWS Lambda ; Amazon SNS

Übersicht

Aus Compliance-Gründen müssen einige Organisationen die Verschlüsselung für Datenbereitstellungsressourcen wie Amazon Data Firehose aktiviert haben. Dieses Muster zeigt eine Möglichkeit, zu überwachen, zu erkennen und zu benachrichtigen, wenn Ressourcen nicht konform sind.

Um die Verschlüsselungsanforderung aufrechtzuerhalten, kann dieses Muster auf Amazon Web Services (AWS) verwendet werden, um eine automatisierte Überwachung und Erkennung von Firehose-Bereitstellungsressourcen bereitzustellen, die nicht mit dem AWS Key Management Service (AWS KMS)-Schlüssel verschlüsselt sind. Die Lösung sendet Warnmeldungen und kann erweitert werden, um eine automatische Behebung durchzuführen. Diese Lösung kann auf ein einzelnes Konto oder eine Umgebung mit mehreren Konten angewendet werden, z. B. auf eine Umgebung, die AWS Landing Zone oder AWS Control Tower verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Firehose-Bereitstellungsdat
- Ausreichende Berechtigungen und Vertrautheit mit AWS CloudFormation, das in dieser Infrastrukturautomatisierung verwendet wird

Einschränkungen

Die Lösung ist nicht in Echtzeit, da sie AWS- CloudTrail Ereignisse zur Erkennung verwendet, und es gibt eine Verzögerung zwischen dem Zeitpunkt, an dem eine unverschlüsselte Ressource erstellt und die Benachrichtigung gesendet wird.

Architektur

Zieltechnologie-Stack

Die Lösung verwendet Serverless-Technologie und die folgenden Services:

- AWS CloudTrail
- Amazon CloudWatch
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- AWS Identity and Access Management (IAM)
- Amazon Data Firehose
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)

Zielarchitektur

1. Ein Benutzer erstellt oder ändert Firehose.
2. Ein CloudTrail Ereignis wird erkannt und abgeglichen.
3. Lambda wird aufgerufen.
4. Nicht konforme Ressourcen werden identifiziert.
5. E-Mail-Benachrichtigung wird gesendet.

Automatisierung und Skalierung

Mit AWS können CloudFormation StackSetsSie diese Lösung mit einem einzigen Befehl auf mehrere AWS-Regionen oder -Konten anwenden.

Tools

- AWS CloudTrail – AWS CloudTrail ist ein AWS-Service, der Sie bei der Aktivierung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos unterstützt. Aktionen eines Benutzers, einer Rolle oder eines AWS-Services werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen, die in der AWS-Managementkonsole, der AWS-Befehlszeilenschnittstelle sowie AWS SDKs und API-Operationen durchgeführt werden.
- Amazon CloudWatch Events – Amazon CloudWatch Events liefert einen near-real-time Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben.
- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- IAM – AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- Amazon Data Firehose – Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Echtzeit-Streaming-Daten. Mit Firehose müssen Sie keine Anwendungen schreiben oder Ressourcen verwalten. Sie konfigurieren Ihre Datenproduzenten so, dass sie Daten an Firehose senden, und es stellt die Daten automatisch an das angegebene Ziel bereit.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten (auch bekannt als Produzenten und Verbraucher) bereitstellt.

Sekunden

Verschlüsselung für Compliance erzwingen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie AWS bereit CloudFormation StackSets.	Verwenden Sie in der AWS CLI die `firehose-encryption-checker.yaml` Vorlage (angefügt), um das Stack-Set zu erstellen, indem Sie den folgenden Befehl ausführen. Geben Sie einen gültigen Amazon-Ressourcennamen (ARN) für das Amazon-Amazon SNS-Thema für den Parameter an. Die Bereitstellung sollte erfolgreich CloudWatch Ereignisregeln, die Lambda-Funktion und eine IAM-Rolle mit den erforderlichen Berechtigungen erstellen, wie in der Vorlage beschrieben. `aws cloudformation create-stack-set --stack-set-name my-stack-set --template-body file://firehose-encryption-checker.yaml`	Cloud-Architekt, Systemadministrator
Erstellen Sie Stack-Instances.	Stacks müssen in den AWS-Regionen Ihrer Wahl sowie in einem oder mehreren Konten erstellt werden. Um Stack-Ins	Cloud-Architekt, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tances zu erstellen, führen Sie den folgenden Befehl aus und ersetzen Sie den Stack-Nam en, die Kontonummern und die Regionen durch Ihre eigenen. `aws cloudformation create-stack-instances --stack-set-name my-stack-set --accounts 123456789012 223456789012 --regions us-east-1 us-east-2 us-west-1 us-west-2 --operation-preferences FailureToleranceCount=1`	

Zugehörige Ressourcen

- Arbeiten mit AWS CloudFormation StackSets
- Was ist Amazon CloudWatch Events?

Zusätzliche Informationen

AWS Config unterstützt den Ressourcentyp Firehose Delivery Stream nicht, daher kann eine AWS Config-Regel nicht in der Lösung verwendet werden.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren des Hinzufügens oder Aktualisierens von Windows-Registrierungseinträgen mit AWS Systems Manager

Erstellt von Appasahebali (AWS)

Erstellt von: AWS	Umgebung: PoC oder Pilotprojekt	Technologien: Cloudnati v DevOps; Infrastruktur; Modernisierung; Sicherhei t, Identität, Compliance; Management und Governance
Workload: Microsoft	AWS-Services: AWS Systems Manager	

Übersicht

AWS Systems Manager ist ein Remote-Verwaltungstool für Amazon Elastic Compute Cloud (Amazon EC2)-Instances. Systems Manager bietet Transparenz und Kontrolle über Ihre Infrastruktur in Amazon Web Services. Dieses zahlreiche Tool kann verwendet werden, um Änderungen an der Windows-Registrierung zu beheben, die vom Scanbericht zu Sicherheitsschwachstellen als Schwachstellen identifiziert werden.

Dieses Muster deckt die Schritte ab, um die Sicherheit Ihrer EC2-Instances beim Ausführen des Windows-Betriebssystems zu gewährleisten, indem Registrierungsänderungen automatisiert werden, die für die Sicherheit Ihrer Umgebung empfohlen werden. Das Muster verwendet den Befehl Ausführen, um ein Befehlsdokument auszuführen. Der Code ist angehängt und ein Teil davon ist im Abschnitt Code enthalten.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto
- Berechtigungen für den Zugriff auf die EC2-Instance und Systems Manager

Architektur

Zieltechnologie-Stack

- Eine Virtual Private Cloud (VPC) mit zwei Subnetzen und einem NAT-Gateway (Network Address Translation)
- Ein Systems Manager-Befehlsdokument zum Hinzufügen oder Aktualisieren des Registrierungsnamens und -werts
- Systems Manager Run Command zum Ausführen des Befehlsdokuments auf den angegebenen EC2-Instances

Zielarchitektur

Tools

Tools

- IAM-Richtlinien und -Rollen – AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- Amazon Simple Storage Service – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern. In diesem Muster wird ein S3-Bucket verwendet, um die Systems Manager-Protokolle zu speichern.
- AWS Systems Manager – AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur in AWS anzeigen und steuern können. Systems Manager hilft Ihnen, Sicherheit und Compliance aufrechtzuerhalten, indem es Ihre verwalteten Instances scannt und alle erkannten Richtlinienverstöße meldet (oder Korrekturmaßnahmen ergreift).
- AWS Systems Manager-Befehlsdokument – AWS Systems Manager-Befehlsdokumente werden von Run Command verwendet. Die meisten Befehlsdokumente werden auf allen Linux- und Windows Server-Betriebssystemen unterstützt, die von Systems Manager unterstützt werden.
- AWS Systems Manager Run Command – AWS Systems Manager Run Command bietet Ihnen die Möglichkeit, die Konfiguration Ihrer verwalteten Instances remote und sicher zu verwalten. Mit Run Command können Sie allgemeine administrative Aufgaben automatisieren und einmalige Konfigurationsänderungen in großem Umfang durchführen.

Code

Sie können den folgenden Beispielcode verwenden, um einen Microsoft Windows-Registrierungsnamen zu `Version`, einen Registrierungspfad zu `HKCU:\Software\ScriptingGuys\Scripts`und einen Wert zu hinzuzufügen oder zu aktualisieren2.

```
#Windows registry path which needs to add/update
$registryPath ='HKCU:\\Software\\ScriptingGuys\\Scripts'
#Windows registry Name  which needs to add/update
$Name = 'Version'
#Windows registry value  which needs to add/update
$value = 2
# Test-Path cmdlet to see if the registry key exists.
IF(!(Test-Path $registryPath))
        {
           New-Item -Path $registryPath -Force | Out-Null
           New-ItemProperty -Path $registryPath -Name $name -Value     $value ` -
PropertyType DWORD -                 Force | Out-        Null
        } ELSE {
                      New-ItemProperty -Path $registryPath -Name $name -Value $value `
 -PropertyType            DWORD        -Force | Out-Null
            }
echo 'Registry Path:'$registryPath
 echo 'Registry Name:'$registryPath
 echo 'Registry Value:'(Get-ItemProperty -Path $registryPath -Name $Name).version
```

Das vollständige JSON-Codebeispiel (Systems Manager Command Document JavaScript Object Notation) ist angehängt.

Polen

Richten Sie eine VPC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie in der AWS-Managementkonsole eine VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gateway. Weitere Informationen finden Sie in der AWS-Dokumentation.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherhei tsgruppen.	Stellen Sie sicher, dass jede Sicherheitsgruppe den Zugriff für das Remote Desktop Protocol (RDP) von der Quell-IP-Adresse aus zulässt.	Cloud-Administrator

Erstellen einer IAM-Richtlinie und einer IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richt linie.	Erstellen Sie eine IAM-Richtlinie, die Zugriff auf Amazon S3, Amazon EC2 und Systems Manager bietet.	Cloud-Administrator
Erstellen Sie eine IAM-Rolle.	Erstellen Sie eine IAM-Rolle und fügen Sie die IAM-Richtlinie an, die Zugriff auf Amazon S3, Amazon EC2 und Systems Manager bietet.	Cloud-Administrator

Ausführen der Automatisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Systems Manager-Befehlsdokument.	Erstellen Sie ein Systems Manager-Befehlsdokument, das die Microsoft Windows-R egistrierungsänderungen zum Hinzufügen oder Aktualisieren bereitstellt.	Cloud-Administrator
Führen Sie den Systems Manager Run Command aus.	Führen Sie den Systems Manager Run Command	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus und wählen Sie das Befehlsdokument und die Systems Manager-Ziel-Instances aus. Dadurch wird die Microsoft Windows-Registrierungsänderung im ausgewählten Befehlsdokument an die Ziel-Instances übertragen.	

Zugehörige Ressourcen

- AWS Systems Manager
- AWS Systems Manager-Dokumente
- AWS Systems Manager Run Command

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Stoppen und Starten einer Amazon RDS-DB-Instance mithilfe von AWS Systems Manager Maintenance Windows

Erstellt von Ashita Dsilva (AWS)

Umgebung: Produktion	Technologien: Verwaltung und Steuerung; Kostenmanagement; Datenbanken; Cloud-nativ	AWS-Services: AWS Systems Manager; Amazon RDS

Übersicht

Dieses Muster zeigt, wie eine Amazon Relational Database Service (Amazon RDS) -DB-Instance mithilfe von AWS Systems Manager Maintenance Windows nach einem bestimmten Zeitplan automatisch gestoppt und gestartet wird (z. B. das Herunterfahren einer DB-Instance außerhalb der Geschäftszeiten, um die Kosten zu senken).

AWS Systems Manager Automation stellt die Runbooks `AWS-StopRdsInstance` und `AWS-StartRdsInstance` Runbooks zum Stoppen und Starten von Amazon RDS-DB-Instances bereit. Das bedeutet, dass Sie keine benutzerdefinierte Logik mit AWS Lambda Lambda-Funktionen schreiben oder eine Amazon CloudWatch Events-Regel erstellen müssen.

AWS Systems Manager bietet zwei Funktionen für die Planung von Aufgaben: State Manager und Maintenance Windows. State Manager legt die erforderliche Statuskonfiguration für Ressourcen in Ihrem Amazon Web Services (AWS) -Konto einmalig oder nach einem bestimmten Zeitplan fest und verwaltet sie. Maintenance Windows führt während eines bestimmten Zeitfensters Aufgaben für die Ressourcen in Ihrem Konto aus. Sie können den Ansatz dieses Musters zwar mit State Manager oder Maintenance Windows verwenden, wir empfehlen jedoch, Maintenance Windows zu verwenden, da es eine oder mehrere Aufgaben basierend auf der zugewiesenen Priorität ausführen kann und auch AWS Lambda-Funktionen und AWS Step Functions Functions-Aufgaben ausführen kann. Weitere Informationen zu State Manager und Maintenance Windows finden Sie unter Choising between State Manager und Maintenance Windows in der AWS Systems Manager Manager-Dokumentation.

Dieses Muster enthält detaillierte Schritte zur Konfiguration von zwei separaten Wartungsfenstern, die Cron-Ausdrücke verwenden, um eine Amazon RDS-DB-Instance zu stoppen und dann zu starten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine bestehende Amazon RDS-DB-Instance, die Sie nach einem bestimmten Zeitplan beenden und starten möchten.
- Cron-Ausdrücke für Ihren gewünschten Zeitplan. Beispielsweise wird der `(0 9 * * 1-5)` Cron-Ausdruck montags bis freitags morgens um 09:00 Uhr ausgeführt.
- Vertrautheit mit Systems Manager.

Einschränkungen

- Eine Amazon RDS-DB-Instance kann für bis zu sieben Tage gleichzeitig gestoppt werden. Nach sieben Tagen wird die DB-Instance automatisch neu gestartet, um sicherzustellen, dass sie alle erforderlichen Wartungsupdates erhält.
- Sie können eine DB-Instance nicht stoppen, bei der es sich um eine Read Replica handelt oder die über eine Read Replica verfügt.
- Sie können eine Amazon RDS for SQL Server-DB-Instance in einer Multi-AZ-Konfiguration nicht stoppen.
- Servicekontingente gelten für Maintenance Windows und Systems Manager Automation. Weitere Informationen zu Servicekontingenten finden Sie unter AWS Systems Manager Manager-Endpunkte und Kontingente in der allgemeinen AWS-Referenzdokumentation.

Architektur

Das folgende Diagramm zeigt den Workflow zum automatischen Stoppen und Starten einer Amazon RDS-DB-Instance.

Der Workflow umfasst die folgenden Schritte:

1. Erstellen Sie ein Wartungsfenster und verwenden Sie Cron-Ausdrücke, um den Stopp- und Startzeitplan für Ihre Amazon RDS-DB-Instances zu definieren.

2. Registrieren Sie mithilfe des `AWS-StartRdsInstance` Runbooks `AWS-StopRdsInstance` oder eine Systems Manager Automation-Task im Wartungsfenster.

3. Registrieren Sie ein Ziel für das Wartungsfenster, indem Sie eine tagbasierte Ressourcengruppe für Ihre Amazon RDS-DB-Instances verwenden.

Technologie-Stack

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- Amazon RDS
- Systems Manager

Automatisierung und Skalierung

Sie können mehrere Amazon RDS-DB-Instances gleichzeitig stoppen und starten, indem Sie die erforderlichen Amazon RDS-DB-Instances taggen, eine Ressourcengruppe erstellen, die alle markierten DB-Instances umfasst, und diese Ressourcengruppe als Ziel für das Wartungsfenster registrieren.

Tools

- AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt.
- AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren können.
- Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert.
- Mit AWS Resource Groups können Sie AWS-Ressourcen in Gruppen organisieren, Ressourcen taggen und Aufgaben für gruppierte Ressourcen verwalten, überwachen und automatisieren.
- AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können.
- AWS Systems Manager Automation vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von Amazon Elastic Compute Cloud (Amazon EC2) -Instances und anderen AWS-Ressourcen.
- AWS Systems Manager Maintenance Windows hilft Ihnen dabei, einen Zeitplan für die Ausführung potenziell störender Aktionen auf Ihren Instances festzulegen.

Epen

Erstellen und konfigurieren Sie die IAM-Servicerolle für Systems Manager Automation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die IAM-Servicerolle für Systems Manager Automation.	Melden Sie sich bei der AWS-Managementkonsole an und erstellen Sie eine Servicerolle für Systems Manager Automation. Sie können eine der folgenden beiden Methoden verwenden, um diese Servicerolle zu erstellen: • Verwenden Sie AWS CloudFormation , um eine Servicerolle für Systems Manager Automation zu konfigurieren • Verwenden Sie IAM, um Rollen für Systems Manager Automation zu konfigurieren Der Systems Manager Automation-Workflow ruft Amazon RDS auf, indem er eine Servicerolle verwendet, um Start- und Stoppaktionen auf der Amazon RDS-DB-Instance durchzuführen. Die Servicerolle muss mit der folgenden Inline-Richtlinie konfiguriert werden, die über Berechtigungen zum Starten	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Stoppen der Amazon RDS-DB-Instance verfügt: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "RdsStartStop", "Effect": "Allow", "Action": [ "rds:StopDBInstance", "rds:StartDBInstance" ], "Resource": "<RDS_Instance_ARN>" }, { "Sid": "RdsDescribe", "Effect": "Allow", "Action": "rds:DescribeDBInstances", "Resource": "*" } ] }` Stellen Sie sicher, dass Sie es `<RDS_Instance_ARN>` durch den Amazon Resource	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Name (ARN) Ihrer Amazon RDS-DB-Instance ersetzen. Wichtig: Stellen Sie sicher, dass Sie den ARN der Servicerolle aufzeichnen.	

Erstellen Sie eine Ressourcengruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kennzeichnen Sie die Amazon RDS-DB-Instances.	Öffnen Sie die Amazon RDS-Konsole und kennzeichnen Sie die Amazon RDS-DB-Instances, die Sie der Ressourcengruppe hinzufügen möchten. Ein Tag besteht aus Metadaten, die einer AWS-Ressource zugewiesen sind und aus einem Schlüssel-Wert-Paar bestehen. Wir empfehlen, Action als Tag-Schlüssel und StartStopals Wert zu verwenden. Weitere Informationen dazu finden Sie in der Amazon RDS-Dokumentation unter Hinzufügen, Auflisten und Entfernen von Tags.	AWS-Administrator
Erstellen Sie eine Ressourcengruppe für Ihre markierten Amazon RDS-DB-Instances.	Öffnen Sie die AWS-Ressourcengruppen-Konsole und erstellen Sie eine Ressourcengruppe auf der Grundlage	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Tags, das Sie für Ihre Amazon RDS-DB-Instances erstellt haben. Stellen Sie sicher, dass Sie unter Gruppierungskriterien AWS: :RDS: :DBInstance als Ressourcentyp auswählen und dann das Schlüssel-Wert-Paar des Tags angeben (z. B. „Action-“). StartStop Dadurch wird sicherges tellt, dass der Service nur nach Amazon RDS-DB-In stances sucht und nicht nach anderen Ressourcen, die über dieses Tag verfügen. Stellen Sie sicher, dass Sie den Namen der Ressource ngruppe aufzeichnen. Weitere Informationen und detaillierte Schritte finden Sie unter Tag-basierte Abfragen erstellen und Gruppen erstellen in der Dokumentation zu AWS-Ressourcengruppen.	

Konfigurieren Sie ein Wartungsfenster zum Stoppen der Amazon RDS-DB-Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Wartungsf enster.	1. Öffnen Sie die AWS Systems Manager Manager-Konsole, wählen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Maintenance Windows und dann Create a maintenance window aus. Geben Sie einen Namen für Ihr Wartungsfenster ein (z. B. „StopRdsInstance“), geben Sie eine Beschreib ung ein und deaktivieren Sie dann Allow unregistered targets. 2. Wählen Sie Cron/Rate expression und geben Sie den Zeitplanausdruck an, um zu definieren, wann die Amazon RDS-DB-In stances gestoppt werden sollen. Geben Sie 1 für die Dauer und 0 für „Aufgaben beenden“ ein. Standardm äßig wird in der Zeitzone UTC angezeigt. Sie können die Zeitzone ändern, um das Wartungsfenster auf der Grundlage des in Ihrem Cron-Ausdruck definierten Zeitstempels zu starten. 3. Wählen Sie Create maintenance window (Wartungsfenster erstellen) aus. Das System kehrt zur Seite des Wartungsfensters zurück, und der Status Ihres Wartungsfensters ist Aktiviert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Die Aufgabe zum Stoppen der DB-Instance wird fast sofort ausgeführt, wenn sie initiiert wird, und erstreckt sich nicht über die gesamte Dauer des Wartungsfensters. Dieses Muster enthält die Mindestwerte für die Dauer und die Initiierung von Aufgaben beenden, da es sich dabei um die erforderlichen Parameter für ein Wartungsfenster handelt. Weitere Informationen und detaillierte Schritte finden Sie unter Erstellen eines Wartungsfensters (Konsole) in der AWS Systems Manager Manager-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie dem Wartungsfenster ein Ziel zu.	1. Wählen Sie in der AWS Systems Manager Manager-Konsole Maintenance Windows, dann Actions und anschließend Register targets aus. 2. Geben Sie im Bereich Ziele die Option Ressourcengruppe auswählen und wählen Sie dann den Namen einer vorhandenen Ressourcengruppe in Ihrem Konto aus. 3. Wählen Sie für Ressourcentypen AWS: :RDS: :DBInstance und dann Ziel registrieren aus. Weitere Informationen und detaillierte Schritte finden Sie unter Zuweisen von Zielen zu einem Wartungsfenster (Konsole) in der AWS Systems Manager Manager-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie dem Wartungsfenster eine Aufgabe zu.	1. Wählen Sie in der AWS Systems Manager Manager-Konsole Maintenance Windows und dann Ihr Wartungsfenster aus. Wählen Sie Aktionen und dann Automatisierungsaufgabe registrieren aus. 2. Wählen Sie für Dokument die Option StopRdsAWS-Instance aus. 3. Wählen Sie im Abschnitt Ziele die Option Registrierte Zielgruppen auswählen und wählen Sie dann das Wartungsfensterziel aus, das Sie für das aktuelle Wartungsfenster registriert haben. 4. Geben Sie für die Ratensteuerung 100 Prozent für Parallelität und Fehlerschwellenwert an. Sie können die Werte für die Ratenkontrolle entsprechend Ihren Anforderungen an die Parallelität von Aufgaben und den Schwellenwert für Fehler ändern. Weitere Informationen dazu finden Sie unter Über Parallelität und Fehlerschwellenwerte in	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der AWS Systems Manager Manager-Dokumentation. 5. Lassen Sie dieses Feld im Abschnitt IAM-Servicerolle für Servicerolle leer oder erstellen Sie Ihre eigene benutzerdefinierte Rolle. Wenn Sie das Feld leer lassen, erstellt Systems Manager automatisch die serviceverknüpfte Rolle AWSServiceRoleForAmazonSSM und ordnet sie dann der Aufgabe zu. Informationen zum Erstellen Ihrer eigenen benutzerdefinierten Rolle finden Sie unter Erstellen einer benutzerdefinierten Servicerolle für Wartungsfenster (Konsole) und ordnen Sie diese benutzerdefinierte Rolle dann der Aufgabe zu. 6. Geben Sie im Abschnitt Eingabeparameter die folgenden Parameter für das Runbook an: • InstanceId: `{{RESOURCE_ID}}` • AutomationAssumeRolle: Geben Sie den ARN der Servicerolle an, die Sie für Systems Manager	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Automation erstellt haben. • Hinweis: Für wird ein Pseudo-Parameter verwendet InstanceId, um die Amazon RDS-DB-Ressourcen-ID aus dem ARN zu extrahier en. Weitere Informationen zu Pseudo-Parametern finden Sie unter Über Pseudo-Parameter in der AWS Systems Manager Manager-Dokumentation. 7. Wählen Sie Automatis ierungsaufgabe registrieren aus. Wichtig: Die Option Servicero lle definiert die Servicerolle, die für das Wartungsfenster zur Ausführung von Aufgaben erforderlich ist. Diese Rolle ist jedoch nicht identisch mit der Servicerolle, die Sie zuvor für Systems Manager Automation erstellt haben. Weitere Informationen und detaillierte Schritte finden Sie unter Zuweisen von Aufgaben zu einem Wartungsf enster (Konsole) in der AWS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Systems Manager Manager-Dokumentation.	

Konfigurieren Sie ein Wartungsfenster zum Starten der Amazon RDS-DB-Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie ein Wartungsfenster, um die Amazon RDS-DB-Instances zu starten.	Wiederholen Sie die Schritte aus dem Fenster Wartung konfigurieren, um die Amazon RDS-DB-Instances zu beenden. Epic, um ein weiteres Wartungsfenster zu konfigurieren, um die Amazon RDS-DB-Instances zu einem geplanten Zeitpunkt zu starten. Wichtig: Sie müssen die folgenden Änderungen vornehmen, wenn Sie das Wartungsfenster für den Start der DB-Instances konfigurieren: • Verwenden Sie einen neuen Namen für das Wartungsfenster (z. B. "StartRds Instance“). • Ersetzen Sie den Cron-Ausdruck durch den Cron-Ausdruck, den Sie zum Starten der DB-Instances verwenden möchten.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Ersetzen Sie das **`AWS-StopRdsInstance`** Runbook durch in Task. **`AWS-StartRdsInstance`**	

Zugehörige Ressourcen

- Verwenden Sie Dokumente von Systems Manager Automation, um Instances zu verwalten und Kosten außerhalb der Geschäftszeiten zu senken (AWS-Blogbeitrag)

Zentralisieren der Softwarepaketverteilung in AWS Organizations mithilfe von Terraform

Erstellt von Pradip kumar Pandey (AWS), Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Mayuri Shinde (AWS) und Pratap Kumar N Bol (AWS)

Umgebung: Produktion	Technologien: Management und Governance; Infrastruktur	AWS-Services: AWS Organizations ;AWS Systems Manager

Übersicht

Unternehmen verwalten häufig mehrere AWS-Konten, die auf mehrere verteilt sindAWS-Regionen, um eine starke Isolationsbarriere zwischen Workloads zu schaffen. Um sicher und konform zu bleiben, installieren ihre Verwaltungsteams agentenbasierte Tools wie CrowdStrike, SentinelOneoder TrendMicro Tools für Sicherheitsscans und den Amazon- CloudWatch Agenten , Datadog Agent oder AppDynamics Agenten für die Überwachung. Diese Teams stehen häufig vor Herausforderungen, wenn sie die Verwaltung und Verteilung von Softwarepaketen in dieser großen Landschaft zentral automatisieren möchten.

Distributor, eine Funktion von AWS Systems Manager, automatisiert den Prozess der Paketierung und Veröffentlichung von Software auf verwalteten Microsoft-Windows- und Linux-Instances in der Cloud und auf On-Premises-Servern über eine einzige vereinfachte Schnittstelle. Dieses Muster zeigt, wie Sie Terraform verwenden können, um die Verwaltung der Installation von Software weiter zu vereinfachen und Skripts mit AWS Organizations minimalem Aufwand über eine große Anzahl von Instances und Mitgliedskonten in auszuführen.

Diese Lösung funktioniert für Amazon-, Linux- und Windows-Instances, die von Systems Manager verwaltet werden.

Voraussetzungen und Einschränkungen

- Ein Distributor-Paket, das die zu installierende Software enthält
- Terraform Version 0.15.0 oder höher

- Amazon Elastic Compute Cloud (Amazon EC2)-Instances, die von Systems Manager verwaltet werden und über grundlegende Berechtigungen für den Zugriff auf Amazon Simple Storage Service (Amazon S3) im Zielkonto verfügen
- Eine Landing Zone für Ihre Organisation, die mithilfe von eingerichtet wird AWS Control Tower
- (Optional) Account Factory für Terraform (AFT)

Architektur

Ressourcendetails

Dieses Muster verwendet Account Factory for Terraform (AFT), um alle erforderlichen AWS Ressourcen zu erstellen, und die Code-Pipeline, um die Ressourcen in einem Bereitstellungskonto bereitzustellen. Die Code-Pipeline wird in zwei Repositorys ausgeführt:

- Die globale Anpassung enthält Terraform-Code, der für alle bei AFT registrierten Konten ausgeführt wird.
- Kontoanpassungen enthalten Terraform-Code, der im Bereitstellungskonto ausgeführt wird.

Sie können diese Lösung auch ohne AFT bereitstellen, indem Sie Terraform-Befehle im Ordner Kontoanpassungen ausführen.

Der Terraform-Code stellt die folgenden Ressourcen bereit:

- AWS Identity and Access Management (IAM)-Rolle und -Richtlinien
  - SystemsManager–AutomationExecutionRole erteilt dem Benutzer Berechtigungen zum Ausführen von Automatisierungen in den Zielkonten.
  - SystemsManager–AutomationAdministrationRole erteilt dem Benutzer Berechtigungen zum Ausführen von Automatisierungen in mehreren Konten und Organisationseinheiten (OUs).
- Komprimierte Dateien und manifest.json für das Paket
  - In Systems Manager enthält ein Paket mindestens eine ZIP-Datei mit Software oder installierbaren Komponenten.
  - Das JSON-Manifest enthält Zeiger auf Ihre Paketcodedateien.
- S3-Bucket
  - Das verteilte Paket, das in der gesamten Organisation gemeinsam genutzt wird, wird sicher in einem Amazon S3-Bucket gespeichert.

- AWS Systems Manager -Dokumente (SSM-Dokumente)
  - `DistributeSoftwarePackage` enthält die Logik zum Verteilen des Softwarepakets an jede Ziel-Instance in den Mitgliedskonten.
  - `AddSoftwarePackageToDistributor` enthält die Logik zum Verpacken der installierbaren Softwarekomponenten und zum Hinzufügen zu Automation, einer Funktion von AWS Systems Manager.
- Systems Manager -Zuordnung.
  - Für die Bereitstellung der Lösung wird eine Systems Manager-Zuordnung verwendet.

Architektur und Workflow

Die Abbildung zeigt die folgenden Schritte:

1. Um die Lösung von einem zentralen Konto aus auszuführen, laden Sie Ihre Pakete oder Software zusammen mit den Bereitstellungsschritten in einen S3-Bucket hoch.
2. Ihr benutzerdefiniertes Paket wird im Abschnitt Dokumente der Systems Manager-Konsole auf der Registerkarte Eigentum von mir verfügbar.
3. State Manager, eine Funktion von Systems Manager, erstellt, plant und führt eine Zuordnung für das Paket in der gesamten Organisation aus. Die Zuordnung gibt an, dass das Softwarepaket auf einem verwalteten Knoten installiert sein muss und ausgeführt werden muss, bevor es auf dem Zielknoten installiert werden kann.
4. Die Zuordnung weist Systems Manager an, das Paket auf dem Zielknoten zu installieren.
5. Bei nachfolgenden Installationen oder Änderungen können Benutzer dieselbe Zuordnung regelmäßig oder manuell von einem einzigen Ort aus ausführen, um Bereitstellungen über -Konten hinweg durchzuführen.
6. In Mitgliedskonten sendet Automation Bereitstellungsbefehle an Distributor.
7. Distributor verteilt Softwarepakete auf Instances.

Diese Lösung verwendet das Verwaltungskonto in AWS Organizations, aber Sie können auch ein Konto (delegierter Administrator) festlegen, um dieses im Namen der Organisation zu verwalten.

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet Amazon S3, um das verteilte Paket zu zentralisieren und sicher zu speichern.
- AWS Systems Manager hilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt werdenAWS Cloud. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS Ressourcen in großem Umfang. Dieses Muster verwendet die folgenden Systems Manager-Funktionen:
  - Distributor unterstützt Sie beim Verpacken und Veröffentlichen von Software auf von Systems Manager verwalteten Instances.
  - Automatisierung vereinfacht häufige Wartungs-, Bereitstellungs- und Abhilfeaufgaben für viele - AWSServices.
  - Documents führt Aktionen auf Ihren von Systems Manager verwalteten Instances in Ihrer gesamten Organisation und Ihren Konten durch.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

Andere Tools

- Terraform ist ein Infrastructure as Code (IaC HashiCorp)-Tool von , mit dem Sie Cloud- und On-Premises-Ressourcen erstellen und verwalten können.

Code-Repository

Die Anweisungen und der Code für dieses Muster sind im GitHub zentralen Paketverteilungs-Repository verfügbar.

Bewährte Methoden

- Um einer Zuordnung Tags zuzuweisen, verwenden Sie die AWS Command Line Interface (AWS CLI) oder die AWS Tools for PowerShell. Das Hinzufügen von Tags zu einer Zuordnung über die Systems-Manager-Konsole wird nicht unterstützt. Weitere Informationen finden Sie unter Markieren von Systems Manager-Ressourcen in der Systems Manager-Dokumentation.
- Um eine Zuordnung mithilfe einer neuen Version eines Dokuments auszuführen, das von einem anderen Konto freigegeben wurde, legen Sie die Dokumentversion auf fest`default`.

- Um nur den Zielknoten zu markieren, verwenden Sie einen Tag-Schlüssel. Wenn Sie Ihre Knoten mithilfe mehrerer Tag-Schlüssel anvisieren möchten, verwenden Sie die Ressourcengruppenoption.

Polen

Konfigurieren von Quelldateien und Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	1. Klonen Sie das GitHub zentrale Paketverteilungs-Repository:
	`git clone https://github.com/aws-samples/aws-organization-centralised-package-distribution`
	2. Das Terraform-Code-Repository erfordert zwei Anpassungsordner, die von AFT verwaltet werden. Vergewissern Sie sich, dass Ihre lokale Kopie des Repositorys die folgenden Ordner enthält:
	`$ cd centralised-package-distribution`
	`$ ls`
	`global-customization account-customization`
		DevOps Techniker

Aktualisieren Sie globale Variablen.	Aktualisieren Sie die folgenden Eingabepa	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rameter in der -`global-customization/variables.tf` Datei. Diese Variablen gelten für alle Konten, die von AFT erstellt und verwaltet werden. • `account_id` : Die ID des Kontos, in dem die Distributor-Lösung bereitgestellt wird. • `aws_region` : Die AWS-Region, in der die Zuordnung bereitgestellt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kontovariablen aktualisieren.	Aktualisieren Sie die folgenden Eingabepa rameter in der `-account-c ustomization/varia bles.tf` Datei. Diese Variablen gelten nur für bestimmte Konten, die von AFT erstellt und verwaltet werden. • `package_bucket_nam e` : Der Name des S3-Buckets, der die Paketvert eilungsdatei enthält. • `package_name` : Der Name der Paketvert eilungsdatei. • `package_version` : Die Paketversion des Installat ionsprogramms.	DevOps Techniker

Anpassen von Parametern und Bereitstellungsdateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Eingabeparameter für die State Manager-Zuordnung.	Aktualisieren Sie die folgenden Eingabepa rameter in der `-account-c ustomization/assoc iation.tf` Datei, um den Status zu definieren, den Sie auf Ihren Instances beibehalt en möchten. Sie können die Standardparameterwerte	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	verwenden, wenn sie Ihren Anwendungsfall unterstützen.
	• `targetAccounts` : Die Organisationseinheits-(OU)-IDs innerhalb von AWS Organizations, die Konten mit den Ziel-Instances für die Verteilung darstellen. OU-IDs beginnen mit „ou“.
	• `targetRegions` : Die AWS-Regionen (z. B. „us-east-1 oder „ap-south east-2“), in der die Ziel-Inst ances ausgeführt werden.
	• `action`: Geben Sie an, ob das Paket installiert oder deinstalliert werden soll.
	• `installationType` : Einer der folgenden Installat ionstypen:
	  • `uninstall` : Das Paket ist deinstalliert.
	  • `reinstall` : Die Anwendung wird offline geschaltet, bis der Neuinstallationsvorgang abgeschlossen ist.
	  • `In-place update`: Die Anwendung ist verfügbar , während der Installat ion neue oder aktualisi erte Dateien hinzugefügt werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `name`: Der Name des zu installierenden oder zu deinstallierenden Pakets. • `version`: Die Version des zu installierenden oder zu deinstallierenden Pakets. Wenn keine Version des Pakets installiert ist, gibt das System einen Fehler zurück. • `bucketName` : Der S3-Bucket-Name, in dem das Paket bereitgestellt wurde. Dieser Bucket sollte nur aus den Paketen und der Manifestdatei bestehen. • `bucketPrefix` : Das S3-Präfix, in dem die Paketkomponenten gespeichert sind. • `AutomationAssumeRole` : Der Amazon-Ressourcenname (ARN) von `SystemsManager-AutomationAdministrationRole` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie komprimierte Dateien und die -`manifest.json` Datei für das Paket vor.	Dieses Muster bietet Beispieldateien zur PowerShell Installation (.msi für Windows und .rpm für Linux) mit Installations- und Deinstallationsskripten im `account-customization/package` Ordner . 1. Ersetzen Sie die PowerShell installierbaren Dateien durch Ihre eigenen Dateien oder stellen Sie Ihre installierbare Datei, installieren und deinstallieren Sie Skripts und die Manifestdatei bereit, um ein Paket im `account-customization` Ordner in Ihrem Konto zu erstellen. 2. Passen Sie die `manifest.json` Standarddatei, die Terraform generiert, im `account-customization` Ordner an Ihre Anforderungen an.	DevOps Techniker

Ausführen von Terraform-Befehlen zur Bereitstellung von Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie die Terraform-Konfiguration.	Um die Lösung automatisch mit AFT bereitzustellen,	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	übertragen Sie den Code an AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
	Sie können diese Lösung auch bereitstellen, ohne AFT zu verwenden, indem Sie einen Terraform-Befehl aus dem `account-customization` Ordner ausführen. Um das Arbeitsverzeichnis zu initialisieren, das die Terraform -Dateien enthält, führen Sie Folgendes aus:
	`$ terraform init`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Änderungen in der Vorschau.	Um eine Vorschau der Änderungen anzuzeigen, die Terraform an der Infrastruktur vornehmen wird, führen Sie den Befehl aus: `$ terraform plan` Mit diesem Befehl wird die Terraform-Konfigur ation ausgewertet, um den gewünschten Status der deklarierten Ressourcen zu ermitteln. Außerdem wird der gewünschte Status mit der tatsächlichen Infrastru ktur verglichen, die innerhalb des Workspace bereitgestellt werden soll.	DevOps Techniker
Änderungen anwenden.	Führen Sie den folgenden Befehl aus, um die Änderunge n zu implementieren, die Sie an den `variables.tf` Dateien vorgenommen haben: `$ terraform apply`	DevOps Techniker

Validieren von Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Erstellung von SSM-Dokumenten.	1. Wählen Sie in der Systems Manager-Konsole im	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	linken Navigationsbereich Dokumente aus. 2. Wählen Sie die Registerkarte Owned by me (In meinem Besitz) aus. Sie sollten die `AddSoftwarePackageToDistributor` Pakete `DistributeSoftwarePackage` und sehen.	
Validieren Sie die erfolgreiche Bereitstellung von Automatisierungen.	1. Wählen Sie in der Systems Manager-Konsole im linken Navigationsbereich Automation aus. 2. In der Liste Automatisierungsausführungen sollten Sie die neuesten - `DistributeSoftwarePackage` und -`AddSoftwarePackageToDistributor` Bereitstellungen sehen. 3. Wählen Sie Ausführungs-ID, um zu überprüfen, ob sie erfolgreich abgeschlossen wurden.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob das Paket auf den Ziel-Instances des Mitgliedskontos bereitgestellt wurde.	1. Wählen Sie in der Systems Manager-Konsole im Navigationsbereich Run Command aus. 2. In Befehlsverlauf sehen Sie jeden Aufruf und seinen Status. 3. Wählen Sie eine beliebige Befehls-ID aus, um den Bereitstellungsverlauf für jede Ziel-Instance anzuzeigen. 4. Wählen Sie die Instance-ID und überprüfen Sie den Abschnitt Ausgabe für die Verteilung.	DevOps Techniker

Fehlerbehebung

Problem	Lösung
Die State Manager-Zuordnung ist fehlgesch lagen oder bleibt im Status „Ausstehend“ hängen.	Weitere Informationen zur Fehlerbehebung finden Sie im -AWSWissenscenter.
Eine geplante Zuordnung konnte nicht ausgeführt werden.	Ihre Zeitplanspezifikation ist möglicherweise ungültig. State Manager unterstützt derzeit nicht die Angabe von Monaten in Cron-Ausd rücken für Zuordnungen. Verwenden Sie Cron- oder Rate-Ausdrücke, um den Zeitplan zu bestätigen.

Zugehörige Ressourcen

- Zentralisierte Paketverteilung (GitHub Repository)
- Account Factory für Terraform (AFT)
- Anwendungsfälle und bewährte Methoden (AWS Systems Manager-Dokumentation)

Konfigurieren von VPC-Flow-Protokollen für die Zentralisierung über AWS-Konten hinweg

Erstellt von Benjamin Bol (AWS) und Aman Bolr Gandhi (AWS)

Umgebung: Produktion	Technologien: Management und Governance	AWS-Services: Amazon VPC; Amazon S3

Übersicht

In einer Virtual Private Cloud (VPC) von Amazon Web Services (AWS) kann die Funktion VPC Flow Logs nützliche Daten für die Fehlerbehebung bei Betrieb und Sicherheit bereitstellen. Es gibt jedoch Einschränkungen bei der Verwendung von VPC-Flow-Protokollen in einer Umgebung mit mehreren Konten. Insbesondere werden kontoübergreifende Flow-Protokolle von Amazon CloudWatch Logs nicht unterstützt. Stattdessen können Sie die Protokolle zentralisieren, indem Sie einen Amazon Simple Storage Service (Amazon S3)-Bucket mit der entsprechenden Bucket-Richtlinie konfigurieren.

Hinweis: In diesem Muster werden die Anforderungen für das Senden von Flow-Protokollen an einen zentralen Ort erörtert. Wenn Sie jedoch auch möchten, dass Protokolle lokal in Mitgliedskonten verfügbar sind, können Sie mehrere Flow-Protokolle für jede VPC erstellen. Benutzer ohne Zugriff auf das Log-Archive-Konto können zur Fehlerbehebung Datenverkehrsprotokolle sehen. Alternativ können Sie ein einzelnes Flow-Protokoll für jede VPC konfigurieren, die Protokolle an CloudWatch Logs sendet. Anschließend können Sie einen Amazon-Data-Firehose-Abonnementfilter verwenden, um die Protokolle an einen S3-Bucket weiterzuleiten. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Organizations-Organisation mit einem Konto, das zum Zentralisieren von Protokollen verwendet wird (z. B. Protokollarchiv)

Einschränkungen

Wenn Sie den von AWS Key Management Service (AWS KMS) verwalteten Schlüssel verwenden, `aws/s3` um Ihren zentralen Bucket zu verschlüsseln, erhält er keine Protokolle von einem anderen Konto. Stattdessen wird ein Fehler angezeigt, der wie folgt aussieht.

```
"Unsuccessful": [
        {
            "Error": {
                "Code": "400",
                "Message": "LogDestination: <bucketName> is undeliverable"
            },
            "ResourceId": "vpc-1234567890123456"
        }
    ]
```

Dies liegt daran, dass die von AWS verwalteten Schlüssel eines Kontos nicht kontenübergreifend gemeinsam genutzt werden können.

Die Lösung besteht darin, entweder die von Amazon S3 verwaltete Verschlüsselung (SSE-S3) oder einen vom Kunden verwalteten Schlüssel von AWS KMS zu verwenden, den Sie für Mitgliedskonten freigeben können.

Architektur

Zieltechnologie-Stack

Im folgenden Diagramm werden zwei Flow-Protokolle für jede VPC bereitgestellt. Eine sendet Protokolle an eine lokale CloudWatch Protokollgruppe. Der andere sendet Protokolle an einen S3-Bucket in einem zentralen Protokollierungskonto. Die Bucket-Richtlinie erlaubt dem Protokollbereitstellungsdienst, Protokolle in den Bucket zu schreiben.

Wichtig: Machen Sie sich mit den Risiken vertraut, die mit der für diese Lösung erforderlichen Bucket-Richtlinie verbunden sind. Da der Prinzipal, der in diesen Bucket schreibt, ein Service-Prinzipal und kein AWS Identity and Access Management (IAM)-Prinzipal ist, ist die `aws:PrincipalOrgID` Bedingung keine gültige Bedingung. Das bedeutet, dass es derzeit keine Möglichkeit gibt, Schreibvorgänge basierend auf der übergeordneten Organisation des Kontos einzuschränken.

Um den Bucket zu sichern, verwenden Sie einen hard-to-guess Bucket-Namen und behandeln Sie den Bucket-Namen als sensiblen Wert, der außerhalb der Organisation nicht offengelegt werden sollte. Stellen Sie sicher, dass Sie in der Bucket-Richtlinie Berechtigungen mit den geringsten Rechten verwenden und nicht mehr als - `s3:putObject` und -`s3:GetBucketAcl`Berechtigungen

gewähren. Wenn Sie in einer Umgebung mit statischen Konten arbeiten, können Sie den Zugriff mit einem Verweigerungseffekt blockieren, außer von bestimmten Konten, obwohl dies für die meisten Organisationen nicht betrieblich möglich ist.

Zielarchitektur

Automatisierung und Skalierung

Jede VPC ist so konfiguriert, dass Protokolle an den S3-Bucket im zentralen Protokollierungskonto gesendet werden. Verwenden Sie eine der folgenden Automatisierungslösungen, um sicherzustellen, dass Flow-Protokolle angemessen konfiguriert sind:

- AWS CloudFormation StackSets
- AWS Control Tower Account Factory für Terraform (AFT)
- Eine AWS Config-Regel mit Korrektur

Tools

Tools

- Amazon CloudWatch Logs hilft Ihnen, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS. Dieses Muster verwendet die Funktion VPC Flow Logs, um Informationen über den IP-Datenverkehr zu und von Netzwerkschnittstellen in Ihrer VPC zu erfassen.

Bewährte Methoden

Die Verwendung von Infrastructure as Code (IaC) kann den Bereitstellungsprozess von VPC Flow Logs erheblich vereinfachen. Wenn Sie Ihre VPC-Bereitstellungsdefinitionen abziehen, um ein Flow-

Protokoll-Ressourcenkonstrukt einzuschließen, werden Ihre VPCs automatisch mit Flow-Protokollen bereitgestellt. Dies wird im nächsten Abschnitt demonstriert.

Zentralisierte Flow-Protokolle

Beispielsyntax für das Hinzufügen zentraler Flow-Protokolle zu einem VPC-Modul in HashiCorp Terraform

Dieser Code erstellt ein Flow-Protokoll, das Protokolle von einer VPC an einen zentralen S3-Bucket sendet. Beachten Sie, dass dieses Muster die Erstellung des S3-Buckets nicht abdeckt.

Empfohlene Bucket-Richtlinienanweisungen finden Sie im Abschnitt Zusätzliche Informationen.

```
variable "vpc_id" {
  type        = string
  description = "ID of the VPC for which you want to create a Flow Log"
}

locals {
  # For more details: https://docs.aws.amazon.com/vpc/latest/userguide/flow-
logs.html#flow-logs-custom
  custom_log_format_v5 = "$${version} $${account-id} $${interface-id} $${srcaddr} $
${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes} $${start} $${end}
 $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-id} $${tcp-flags} $
${type} $${pkt-srcaddr} $${pkt-dstaddr} $${region} $${az-id} $${sublocation-type} $
${sublocation-id} $${pkt-src-aws-service} $${pkt-dst-aws-service} $${flow-direction} $
${traffic-path}"
}

resource "aws_flow_log" "centralized" {
  log_destination      = "arn:aws:s3:::centralized-vpc-flow-logs-
<log_archive_account_id>" # Optionally, a prefix can be added after the ARN.
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = var.vpc_id
  log_format           = local.custom_log_format_v5 # If you want fields from VPC Flow
 Logs v3+, you will need to create a custom log format.
  tags                 = {
    Name = "centralized_flow_log"
  }
}
```

Lokale Flow-Protokolle

Beispielsyntax für das Hinzufügen lokaler Flow-Protokolle zu einem VPC-Modul in Terraform mit den erforderlichen Berechtigungen

Dieser Code erstellt ein Flow-Protokoll, das Protokolle von einer VPC an eine lokale CloudWatch Logs-Gruppe sendet.

```
data "aws_region" "current" {}

variable "vpc_id" {
  type        = string
  description = "ID of the VPC for which you want to create a Flow Log"
}

resource "aws_iam_role" "local_flow_log_role" {
  name = "flow-logs-policy-${var.vpc_id
}"

  assume_role_policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
}

resource "aws_iam_role_policy" "logs_permissions" {
  name = "flow-logs-policy-${var.vpc_id}"
  role = aws_iam_role.local_flow_log_role.id

  policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:${data.aws_region.current.name}:*:log-group:vpc-flow-
logs*"
    }
  ]
}
EOF
}

resource "aws_cloudwatch_log_group" "local_flow_logs" {
  # checkov:skip=CKV_AWS_338:local retention is set to 30, centralized S3 bucket can
 retain for long-term
  name              = "vpc-flow-logs/${var.vpc_id}"
  retention_in_days = 30
}

resource "aws_flow_log" "local" {
  iam_role_arn    = aws_iam_role.local_flow_log_role.arn
  log_destination = aws_cloudwatch_log_group.local_flow_logs.arn
  traffic_type    = "ALL"
  vpc_id          = var.vpc_id
  tags            = {
    Name = "local_flow_log"
  }
}
```

Sekunden

Bereitstellen der Infrastruktur von VPC Flow Logs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie die Verschlüs selungsstrategie und erstellen Sie die Richtlinie für den zentralen S3-Bucket.	Der zentrale Bucket unterstüt zt den `aws/s3` AWS KMS-Schlüssel nicht, daher müssen Sie entweder SSE-S3 oder einen vom Kunden verwalteten AWS KMS-Schlüssel verwenden . Wenn Sie einen AWS KMS-Schlüssel verwenden, muss die Schlüsselrichtlinie Mitgliedskonten erlauben, den Schlüssel zu verwenden.	-Compliance
Erstellen Sie den zentralen Flow-Protokoll-Bucket.	Erstellen Sie den zentralen Bucket, an den Flow-Prot okolle gesendet werden, und wenden Sie die Verschlüs selungsstrategie an, die Sie im vorherigen Schritt ausgewähl t haben. Dies sollte sich in einem Protokollarchiv oder einem ähnlich bestimmten Konto befinden. Rufen Sie die Bucket-Ri chtlinie aus dem Abschnitt Zusätzliche Informationen ab und wenden Sie sie auf Ihren zentralen Bucket an, nachdem Sie Platzhalter mit	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihren umgebungsspezifischen Werten aktualisiert haben.	
Konfigurieren Sie VPC-Flow-Protokolle, um Protokolle an den zentralen Flow-Protokoll-Bucket zu senden.	Fügen Sie jeder VPC, aus der Sie Daten sammeln möchten, Flow-Protokolle hinzu. Die skalierbarste Methode hierfür ist die Verwendung von IaC-Tools wie AFT oder AWS Cloud Development Kit (AWS CDK). Sie können beispielsweise ein Terraform-Modul erstellen, das eine VPC zusammen mit einem Flow-Protokoll bereitstellt. Bei Bedarf fügen Sie die Flow-Protokolle manuell hinzu.	Netzwerkadministrator
Konfigurieren Sie VPC-Flow-Protokolle für das Senden an lokale CloudWatch Protokolle.	(Optional) Wenn Sie möchten, dass Flow-Protokolle in den Konten sichtbar sind, in denen die Protokolle generiert werden, erstellen Sie ein weiteres Flow-Protokoll, um Daten an CloudWatch Protokolle im lokalen Konto zu senden. Alternativ können Sie die Daten an einen kontospezifischen S3-Bucket im lokalen Konto senden.	Allgemeines AWS

Zugehörige Ressourcen

- So erleichtern Sie die Datenanalyse und erfüllen die Sicherheitsanforderungen mithilfe zentraler Flow-Protokolldaten (Blogbeitrag)

- So aktivieren Sie VPC Flow Logs automatisch mithilfe von AWS Config-Regeln (Blogbeitrag)

Zusätzliche Informationen

Bucket-Richtlinie

Dieses Beispiel für eine Bucket-Richtlinie kann auf Ihren zentralen S3-Bucket für Flow-Protokolle angewendet werden, nachdem Sie Werte für Platzhalternamen hinzugefügt haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>"
        },
        {
            "Sid": "DenyUnencryptedTraffic",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
```

```
            "Resource": [
                "arn:aws:s3:::<BUCKET_NAME>/*",
                "arn:aws:s3:::<BUCKET_NAME>"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Wenn Sie über eine statische Liste von Konten verfügen, können Sie die folgende Anweisung hinzufügen, um Konten außerhalb dieser Liste zu verweigern.

```
{
    "Sid": "AccountDenyList",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "NotResource": [
        "arn:aws:s3:::<BUCKET_NAME>/<OPTIONAL_PREFIX>/AWSLogs/<ACCOUNT_ID1>/*",
        "arn:aws:s3:::<BUCKET_NAME>/<OPTIONAL_PREFIX>/AWSLogs/<ACCOUNT_ID2>/*",
        "arn:aws:s3:::<BUCKET_NAME>/<OPTIONAL_PREFIX>/AWSLogs/<ACCOUNT_ID3>/*",
    ]
}
```

Als Alternative zum vorherigen `NotResource`-`Deny`Muster können Sie stattdessen jeder Ihrer `Allow` Anweisungen Bedingungen hinzufügen, um genehmigte Konten anzugeben.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": [
            "111111111111",
            "222222222222"
        ]
    }
}
```

Hinzufügen eines Präfixes

Sie können Schreibvorgänge auf ein bekanntes Präfix innerhalb des Buckets auch einschränken, wenn Sie Bedenken hinsichtlich unerwünschter externer Schreibvorgänge in den Bucket in einem Szenario haben, in dem der Bucket-Name öffentlich zugänglich wird. Wenn Sie dies implementieren, aktualisieren Sie die `log_destination` in der `aws_flow_log` Ressource, um das Präfix nach dem Amazon-Ressourcennamen (ARN) des Buckets einzuschließen. Die folgende Anweisung schränkt beispielsweise Schreibvorgänge auf ein bestimmtes Präfix ein.

```
{
    "Sid": "PrefixAllowList",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "NotResource": [
        "arn:aws:s3:::<BUCKET_NAME>/<PREFIX>/*"
    ]
}
```

Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog

Erstellt von Bibhuti Sahu (AWS) und Rob Hill (AWS) (AWS)

Umgebung: Produktion	Technologien: Verwaltung und Verwaltung DevOps; Web- und mobile Apps	Arbeitslast: Microsoft
AWS-Services: Amazon CloudWatch Logs		

Übersicht

Dieses Muster beschreibt, wie das Open-Source-Logging-Framework NLog verwendet wird, um die Nutzung von.NET-Anwendungen und Ereignisse in Amazon CloudWatch Logs zu protokollieren. In der CloudWatch Konsole können Sie die Protokollnachrichten der Anwendung nahezu in Echtzeit einsehen. Sie können auch Messwerte einrichten und Alarme so konfigurieren, dass Sie benachrichtigt werden, wenn ein Metrik-Schwellenwert überschritten wird. Mithilfe von CloudWatch Application Insights können Sie automatisierte oder benutzerdefinierte Dashboards anzeigen, die potenzielle Probleme für die überwachten Anwendungen aufzeigen. CloudWatch Application Insights soll Ihnen helfen, laufende Probleme mit Ihren Anwendungen und Ihrer Infrastruktur schnell zu isolieren.

Um Protokollnachrichten in CloudWatch Logs zu schreiben, fügen Sie das `AWS.Logger.NLog` NuGet Paket dem .NET-Projekt hinzu. Anschließend aktualisieren Sie die `NLog.config` Datei, um CloudWatch Logs als Ziel zu verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine.NET-Web- oder Konsolenanwendung, die:
  - Verwendet unterstützte.NET Framework- oder .NET Core-Versionen. Weitere Informationen finden Sie unter Produktversionen.

  - Verwendet NLog, um Protokolldaten an Application Insights zu senden.
- Berechtigungen zum Erstellen einer IAM-Rolle für einen AWS-Service. Weitere Informationen finden Sie unter Berechtigungen für Servicerollen.
- Berechtigungen zur Übergabe einer Rolle an einen AWS-Service. Weitere Informationen finden Sie unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS-Service.

Produktversionen

- .NET Framework Version 3.5 oder höher
- .NET Core-Versionen 1.0.1, 2.0.0 oder höher

Architektur

Zieltechnologie-Stack

- NLog
- CloudWatch Amazon-Protokolle

Zielarchitektur

1. Die .NET-Anwendung schreibt Protokolldaten in das NLog-Protokollierungsframework.
2. NLog schreibt die Protokolldaten in Logs. CloudWatch
3. Sie verwenden CloudWatch Alarme und benutzerdefinierte Dashboards, um die .NET-Anwendung zu überwachen.

Tools

AWS-Services

- Amazon CloudWatch Application Insights hilft Ihnen dabei, den Zustand Ihrer Anwendungen und der zugrunde liegenden AWS-Ressourcen zu beobachten.
- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Bei den AWS-Tools für PowerShell handelt es sich um eine Reihe von PowerShell Modulen, die Ihnen helfen, Operationen auf Ihren AWS-Ressourcen von der PowerShell Befehlszeile aus zu skripten.

Andere Tools

- Logger.nlog ist ein NLog-Ziel, das Protokolldaten in Logs aufzeichnet. CloudWatch
- NLog ist ein Open-Source-Logging-Framework für .NET-Plattformen, mit dem Sie Protokolldaten in Ziele wie Datenbanken, Protokolldateien oder Konsolen schreiben können.
- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.
- Visual Studio ist eine integrierte Entwicklungsumgebung (IDE), die Compiler, Tools zur Codevervollständigung, Grafikdesigner und andere Funktionen zur Unterstützung der Softwareentwicklung umfasst.

Bewährte Methoden

- Legen Sie eine Aufbewahrungsrichtlinie für die Zielprotokollgruppe fest. Dies muss außerhalb der NLog-Konfiguration erfolgen. Standardmäßig werden Protokolldaten auf unbestimmte Zeit in CloudWatch Logs gespeichert.
- Halten Sie sich an die Best Practices für die Verwaltung von AWS-Zugriffsschlüsseln.

Epen

Richten Sie Zugriff und Tools ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie.	Folgen Sie den Anweisungen unter Richtlinien mit dem JSON-Editor erstellen in der IAM-Dokumentation. Geben Sie die folgende JSON-	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Richtlinie ein, die über die geringsten Rechte verfügt, die erforderlich sind, damit CloudWatch Logs Logs Logs lesen und schreiben kann. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "logs:CreateLogGroup", "logs:CreateLogStream", "logs:GetLogEvents", "logs:PutLogEvents", "logs:DescribeLogGroups", "logs:DescribeLogStreams", "logs:PutRetentionPolicy" ], "Resource": [ "*" ] } ]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>}</pre>	
Erstellen Sie eine IAM-Rolle.	Folgen Sie den Anweisungen unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service in der IAM-Dokumentation. Wählen Sie die Richtlinie aus, die Sie zuvor erstellt haben. Dies ist die Rolle, die CloudWatch Logs bei der Durchführung von Protokollierungsaktionen einnimmt.	AWS-Administrator, AWS DevOps
Richten Sie AWS-Tools für ein PowerShell.	1. Folgen Sie den Anweisungen für Ihr Betriebssystem unter Installation der AWS-Tools für PowerShell. 2. Verwenden Sie die AWS-Tools für PowerShell Cmdlets, um Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel in einem Profil zu speichern. Anweisungen finden Sie in der PowerShell Dokumentation unter Profile verwalten in den AWS-Tools.	Allgemeines AWS

NLog konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das NuGet Paket.	1. Wählen Sie in Visual Studio Datei und dann Projekt oder Lösung öffnen aus. 2. Wählen Sie das Projekt aus, in dem Sie NLog installieren möchten. 3. Wählen Sie in Visual Studio Tools, NuGet Package Manager, Package Manager Console aus. 4. Installieren Sie das `AWS.Logger.NLog` NuGet Paket, indem Sie den folgenden Befehl eingeben. `Install-Package AWS.Logger.NLog -Version 3.1.0`	App-Developer
Konfigurieren Sie das Logging-Ziel.	1. Öffnen Sie die `NLog.config` Datei. 2. Geben Sie für `type` das Ziel ein`AWSTarget` . 3. Geben Sie für `logGroup` das Ziel den Namen der Protokollgruppe ein, die Sie verwenden möchten. Wenn die Protokollgruppe noch nicht existiert, wird automatisch eine neue Protokollgruppe mit dem	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	angegebenen Namen erstellt. 4. Geben Sie für das Ziel die AWS-Region ein`region`, in der CloudWatch Logs konfiguriert ist. 5. Geben Sie für das Ziel `profile` den Namen des Profils ein, das Sie zuvor zum Speichern des Zugriffsschlüssels und des geheimen Schlüssels erstellt haben. 6. Speichern und schließen Sie die Datei `NLog.config` . Eine Beispielkonfigurationsdatei finden Sie im Abschnitt Zusätzliche Informationen dieses Musters. Wenn Sie Ihre Anwendung ausführen, schreibt NLog die Protokollnachrichten und sendet sie an CloudWatch Logs.	

Validieren und überwachen Sie die Protokolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokollierung.	Folgen Sie den Anweisungen unter An CloudWatc	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	h Protokolle gesendete Protokolldaten anzeigen in der Dokumentation zu den CloudWatch Protokoll en. Stellen Sie sicher, dass Protokollereignisse für die .NET-Anwendung aufgezeichnet werden. Wenn keine Protokollereignisse aufgezeichnet werden, finden Sie weitere Informationen im Abschnitt Problembehandlung in diesem Muster.	
Überwachen Sie den.NET-A nwendungsstapel.	Konfigurieren Sie die Überwachung nach CloudWatch Bedarf für Ihren Anwendungsfall. Sie können CloudWatch Logs Insights, CloudWatch Metrics Insights und CloudWatch Applicati on Insights verwenden, um Ihren .NET-Workload zu überwachen. Sie können auch Alarme so konfigurieren, dass Sie Benachrichtigungen erhalten können, und Sie können ein benutzerdefinierte s Dashboard zur Überwachu ng der Arbeitslast von einer einzigen Ansicht aus erstellen.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Protokolldaten werden nicht in CloudWatch Logs angezeigt.	Stellen Sie sicher, dass die IAM-Richtlinie mit der IAM-Rolle verknüpft ist, die CloudWatch Logs annimmt. Anweisungen finden Sie im Abschnitt Zugriff und Tools einrichten im Abschnitt Epics.

Zugehörige Ressourcen

- Arbeiten mit Log-Gruppen und Log-Streams (CloudWatch Logs-Dokumentation)
- Amazon CloudWatch Logs und .NET Logging Frameworks (AWS-Blogbeitrag)

Zusätzliche Informationen

Im Folgenden finden Sie eine `NLog.config` Beispieldatei.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog" />
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>
  <nlog>
    <extensions>
      <add assembly="NLog.AWS.Logger" />
    </extensions>
    <targets>
      <target name="aws" type="AWSTarget" logGroup="NLog.TestGroup" region="us-east-1"
 profile="demo"/>
    </targets>
    <rules>
      <logger name="*" minlevel="Info" writeTo="aws" />
    </rules>
  </nlog>
```

```
</configuration>
```

AWS Service Catalog-Produkte über verschiedene AWS-Konten und AWS-Regionen hinweg kopieren

Erstellt von Sachin Vighe (AWS) und Santoshe (AWS)

Umgebung: Produktion	Technologien: Management und Governance; Serverless	Workload: Alle anderen Workloads
AWS-Services: AWS Service Catalog ;AWS Lambda		

Übersicht

AWS Service Catalog ist ein regionaler Service, was bedeutet, dass AWS Service Catalog-Portfolios und -Produkte nur in der AWS-Region sichtbar sind, in der sie erstellt werden. Wenn Sie einen AWS Service Catalog-Hub in einer neuen Region einrichten, müssen Sie Ihre vorhandenen Produkte neu erstellen. Dies kann ein zeitaufwändiger Prozess sein.

Der Ansatz dieses Musters vereinfacht diesen Prozess, indem beschrieben wird, wie Produkte aus einem AWS Service Catalog-Hub in einem AWS-Quellkonto oder einer AWS-Quellregion in einen neuen Hub in einem Zielkonto oder einer Zielregion kopiert werden. Weitere Informationen zum Hub- und Spoke-Modell von AWS Service Catalog finden Sie unter Hub- und Spoke-Modell von AWS Service Catalog: So automatisieren Sie die Bereitstellung und Verwaltung von AWS Service Catalog für viele Konten im AWS Management and Governance Blog.

Das Muster enthält auch die separaten Codepakete, die zum Kopieren von AWS Service Catalog-Produkten über Konten oder in andere Regionen hinweg erforderlich sind. Mit diesem Muster kann Ihre Organisation Zeit sparen, vorhandene und frühere Produktversionen in einem neuen AWS Service Catalog-Hub verfügbar machen, das Risiko manueller Fehler minimieren und den Ansatz über mehrere Konten oder Regionen hinweg skalieren.

Hinweis: Der Abschnitt „PiCs“ dieses Musters bietet zwei Optionen zum Kopieren von Produkten. Sie können Option 1 verwenden, um Produkte über -Konten hinweg zu kopieren, oder Option 2 wählen, um Produkte über Regionen hinweg zu kopieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vorhandene AWS Service Catalog-Produkte in einem Quellkonto oder einer Region.
- Ein vorhandener AWS Service Catalog-Hub in einem Zielkonto oder einer Region.
- Wenn Sie Produkte kontenübergreifend kopieren möchten, müssen Sie das AWS Service Catalog-Portfolio, das die Produkte enthält, freigeben und dann in Ihr Zielkonto importieren. Weitere Informationen dazu finden Sie unter Freigeben und Importieren von Portfolios in der AWS Service Catalog-Dokumentation.

Einschränkungen

- AWS Service Catalog-Produkte, die Sie über Regionen oder Konten hinweg kopieren möchten, können nicht mehreren Portfolios angehören.

Architektur

Das folgende Diagramm zeigt das Kopieren von AWS Service Catalog-Produkten von einem Quellkonto in ein Zielkonto.

Das folgende Diagramm zeigt das Kopieren von AWS Service Catalog-Produkten aus einer Quellregion in eine Zielregion.

Technologie-Stack

- Amazon CloudWatch
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Service Catalog

Automatisierung und Skalierung

Sie können den Ansatz dieses Musters skalieren, indem Sie eine Lambda-Funktion verwenden, die abhängig von der Anzahl der empfangenen Anfragen oder der Anzahl der AWS Service Catalog-Produkte, die Sie kopieren müssen, skaliert werden kann. Weitere Informationen dazu finden Sie unter Lambda-Funktionsskalierung in der AWS Lambda-Dokumentation.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Service Catalog hilft Ihnen dabei, Kataloge von IT-Services, die für AWS genehmigt sind, zentral zu verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Code

Sie können das - `cross-account-copy`Paket (angefügt) verwenden, um AWS Service Catalog-Produkte kontenübergreifend zu kopieren, oder das -`cross-region-copy`Paket (angefügt), um Produkte regionsübergreifend zu kopieren.

Das `cross-account-copy` Paket enthält die folgenden Dateien:

- `copyconf.properties` – Die Konfigurationsdatei, die die Regions- und AWS-Konto-ID-Parameter für das kontenübergreifende Kopieren von Produkten enthält.
- `scProductCopyLambda.py` – Die Python-Funktion zum Kopieren von Produkten über -Konten hinweg.
- `createDestAccountRole.sh` – Das Skript zum Erstellen einer IAM-Rolle im Zielkonto.
- `createSrcAccountRole.sh` – Das Skript zum Erstellen einer IAM-Rolle im Quellkonto.
- `copyProduct.sh` – Das Skript zum Erstellen und Aufrufen der Lambda-Funktion zum Kopieren von Produkten über -Konten hinweg.

Das `cross-region-copy` Paket enthält die folgenden Dateien:

- `copyconf.properties` – Die Konfigurationsdatei, die die Regions- und AWS-Konto-ID-Parameter für das regionsübergreifende Kopieren von Produkten enthält.
- `scProductCopyLambda.py` – Die Python-Funktion zum Kopieren von Produkten über -Regionen hinweg.
- `copyProduct.sh` – Das Skript zum Erstellen einer IAM-Rolle und zum Erstellen und Aufrufen der Lambda-Funktion zum Kopieren von Produkten über Regionen hinweg.

Polen

Option 1 – Kopieren von AWS Service Catalog-Produkten über -Konten hinweg

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Konfigurationsdatei.	1. Laden Sie das `-cross-account-copy` Paket (angefügt) auf Ihren lokalen Computer herunter. 2. Aktualisieren Sie die `copyconf.properties` Konfigurationsdatei mit den folgenden Werten: • `srcRegion` – Geben Sie die Quellregion an, die die Produkte enthält. • `destRegion` – Geben Sie die Zielregion für die Produkte an. • `sourceAccountId` – Geben Sie die AWS-Konto-ID für Ihr Quellkonto an. • `destAccountId` – Geben Sie die AWS-Konto-ID für Ihr Zielkonto an.	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Ihre Anmeldeinformationen für AWS CLI im Zielkonto.	Konfigurieren Sie Ihre Anmeldeinformationen für den Zugriff auf AWS CLI in Ihrem Zielkonto, indem Sie den `aws configure` Befehl ausführen und die folgenden Werte angeben:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Weitere Informationen dazu finden Sie unter Konfigurationsgrundlagen in der AWS Command Line Interface-Dokumentation.
		AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Ihre Anmeldeinformationen für AWS CLI im Quellkonto.	Konfigurieren Sie Ihre Anmeldeinformationen für den Zugriff auf AWS CLI in Ihrem Quellkonto, indem Sie den `aws configure` Befehl ausführen und die folgenden Werte angeben:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Weitere Informationen dazu finden Sie unter Konfigurationsgrundlagen in der AWS Command Line Interface-Dokumentation.
		AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Ausführungsrolle in Ihrem Zielkonto.	Führen Sie das `createDestAccountRole.sh` Skript in Ihrem Zielkonto aus. Das Skript implementiert die folgenden Aktionen: • Erstellt eine Lambda-Ausführungsrolle in Ihrem Zielkonto • Erstellt die IAM-Richtlinie für die Lambda-Ausführungsrolle und fügt sie an	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator
Erstellen Sie die kontoüber greifende IAM-Rolle in Ihrem Quellkonto.	Führen Sie das `createSrcAccountRole.sh` Skript in Ihrem Quellkonto aus. Das Skript implementiert die folgenden Aktionen: • Erstellt eine kontoüber greifende IAM-Rolle in Ihrem Quellkonto, die von der Lambda-Ausführungsrolle im Zielkonto übernommen wird, um Produkte zu kopieren • Erstellt eine IAM-Richtlinie für die kontoübergreifende Rolle in Ihrem Quellkonto und fügt sie an	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das copyProduct-Skript im Zielkonto aus.	Führen Sie das `copyProduct.sh` Skript in Ihrem Zielkonto aus. Das Skript implementiert die folgenden Aktionen: • Erstellt die Lambda-Funktion und ruft sie auf, um Produkte aus dem Quellkonto in das Zielkonto zu kopieren	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Option 2 – Kopieren von AWS Service Catalog-Produkten aus einer Quellregion in eine Zielregion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Konfigurationsdatei.	1. Laden Sie das `-cross-region-copy` Paket (angefügt) auf Ihren lokalen Computer herunter. 2. Aktualisieren Sie die `copyconf.properties` Konfigurationsdatei mit den folgenden Werten: • `srcRegion` – Geben Sie die Quellregion an, die die Produkte enthält. • `destRegion` – Geben Sie die Zielregion für die Produkte an. • `accountId` – Geben Sie Ihre AWS-Konto-ID an.	AWS-Systemadministrator, Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Ihre Anmeldeinformationen für AWS CLI.	Konfigurieren Sie Ihre Anmeldeinformationen für den Zugriff auf AWS CLI in Ihrer Umgebung, indem Sie den `aws configure` Befehl ausführen und die folgenden Werte angeben:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Weitere Informationen dazu finden Sie unter Konfigurationsgrundlagen in der AWS Command Line Interface-Dokumentation.
		AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das copyProduct-Skript aus.	Führen Sie das `copyProduct.sh` Skript in Ihrer Zielregion aus. Das Skript implementiert die folgenden Aktionen: • Erstellt eine Lambda-Ausführungsrolle • Erstellt die IAM-Richtlinie für die Lambda-Ausführungsrolle und fügt sie an • Erstellt die Lambda-Funktion und ruft sie auf, um Produkte aus der Quellregion in die Zielregion zu kopieren	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Zugehörige Ressourcen

- Erstellen einer Lambda-Ausführungsrolle (AWS Lambda-Dokumentation)
- Erstellen einer Lambda-Funktion (AWS Lambda-Dokumentation)
- AWS Service Catalog – API-Referenz
- AWS Service Catalog-Dokumentation

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen von Alarmen für benutzerdefinierte Metriken mithilfe der Amazon CloudWatch -Anomalieerkennung

Erstellt von Ram Kandaswamy (AWS) und Raheem Jiwani (AWS)

Umgebung: Produktion	Technologien: Management und Governance; DevOps; Betrieb; Cloudnativ	AWS-Services: Amazon CloudWatch

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie Amazon verwenden, CloudWatch um Alarme zu erstellen, die Metriken überwachen und Benachrichtigungen senden oder automatisch Änderungen vornehmen, wenn ein Schwellenwert überschritten wird.

Um zu vermeiden, dass Sie durch statische Schwellenwerte eingeschränkt werden, können Sie Alarme erstellen, die auf vergangenen Mustern basieren und Sie benachrichtigen, wenn sich bestimmte Metriken außerhalb des normalen Betriebsfensters befinden. Sie können beispielsweise die Reaktionszeiten Ihrer API von Amazon API Gateway aus überwachen und Benachrichtigungen über Anomalien erhalten, die verhindern, dass Sie ein Service Level Agreement (SLA) einhalten.

Dieses Muster beschreibt, wie die CloudWatch Anomalieerkennung für benutzerdefinierte Metriken verwendet wird. Das Muster zeigt Ihnen, wie Sie eine benutzerdefinierte Metrik in Amazon CloudWatch Logs Insights erstellen oder eine benutzerdefinierte Metrik mit einer AWS Lambda-Funktion veröffentlichen und dann die Anomalieerkennung einrichten und Benachrichtigungen mit Amazon Simple Notification Service (Amazon SNS) erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandenes SNS-Thema, das zum Senden von E-Mail-Benachrichtigungen konfiguriert ist. Weitere Informationen dazu finden Sie unter Erste Schritte mit Amazon SNS in der Amazon SNS-Dokumentation.

- Eine vorhandene Anwendung, konfiguriert mit CloudWatch Protokollen .

Einschränkungen

- CloudWatch -Metriken unterstützen keine Millisekunden-Zeitintervalle. Weitere Informationen zur Granularität regulärer und benutzerdefinierter Metriken finden Sie unter Amazon CloudWatch FAQs .

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Protokolle, die von - CloudWatch Protokollen erstellte und aktualisierte Metriken verwenden, werden an gestreamt CloudWatch.
2. Ein Alarm wird basierend auf Schwellenwerten ausgelöst und sendet eine Warnung an ein SNS-Thema.
3. Amazon SNS sendet Ihnen eine E-Mail-Benachrichtigung.

Technologie-Stack

- CloudWatch
- AWS Lambda
- Amazon SNS

Tools

- Amazon Cloudwatch – CloudWatch bietet eine zuverlässige, skalierbare und flexible Überwachungslösung.
- AWS Lambda – Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten bereitstellt.

Polen

Einrichten der Anomalieerkennung für eine benutzerdefinierte Metrik

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 – Erstellen Sie eine benutzerdefinierte Metrik mit einer Lambda-Funktion.	Laden Sie die `lambda_function.py` Datei (angefügt) herunter und ersetzen Sie dann die `lambda_function.py` Beispieldatei im aws-lambda-developer-guideRepository in der AWS-Dokumentation GitHub. Dadurch erhalten Sie eine Lambda-Beispielfunktion, die benutzerdefinierte Metriken an - CloudWatch Protokolle sendet. Die Lambda-Funktion verwendet die Boto3-API, um in zu integrieren CloudWatch. Nachdem Sie die Lambda-Funktion ausgeführt haben, können Sie sich bei der AWS-Managementkonsole anmelden, die CloudWatch Konsole öffnen und die veröffentlichte Metrik ist unter Ihrem veröffentlichten Namespace verfügbar.	DevOps Techniker, AWS DevOps
Option 2 – Erstellen Sie benutzerdefinierte Metriken aus CloudWatch Protokollgruppen.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudWatch Konsole und wählen Sie	DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann Protokollgruppen aus. Wählen Sie die Protokoll gruppe aus, für die Sie eine Metrik erstellen möchten. Wählen Sie Aktionen und dann Metrikfilter erstellen aus. Geben Sie für Filtermuster das Filtermuster ein, das Sie verwenden möchten. Weitere Informationen finden Sie unter Filter- und Mustersyntax in der - CloudWatch Dokumentation. Um Ihr Filtermuster zu testen, geben Sie ein oder mehrere Protokollereigniss e unter Testmuster ein. Jedes Protokollereignis muss innerhalb einer einzelnen Zeile liegen, da Zeilenumb rüche verwendet werden, um Protokollereignisse im Anzeigebereich Log event messages (Ereignis meldungen protokollieren) zu trennen. Nachdem Sie das Muster getestet haben, können Sie unter Metrikdetails einen Namen und einen Wert für Ihre Metrik eingeben. Weitere Informationen und Schritte zum Erstellen einer benutzerdefinierten Metrik finden Sie unter Erstellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eines Metrikfilters für eine Protokollgruppe in der - CloudWatch Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Alarm für Ihre benutzerdefinierte Metrik.	Wählen Sie in der CloudWatch Konsole Alarme und dann Alarm erstellen aus. Wählen Sie Metrik auswählen und geben Sie den Namen der Metrik, die Sie zuvor erstellt haben, in das Suchfeld ein. Wählen Sie die Registerkarte Grafische Metriken und konfigurieren Sie die Optionen entsprechend Ihren Anforderungen. Wählen Sie unter Bedingungen die Option Anomalieerkennung anstelle statischer Schwellenwerte aus. Dies zeigt Ihnen ein Band, das auf zwei Standardabweichungen basiert. Sie können Schwellenwerte einrichten und an Ihre Anforderungen anpassen. Wählen Sie Weiter aus. Hinweis: Das Band ist dynamisch und hängt von der Qualität der Datenpunkte ab. Wenn Sie mit der Aggregation weiterer Daten beginnen, werden das Band und die Schwellenwerte automatisch aktualisiert.	DevOps Techniker, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie SNS-Benachrichtigungen ein.	Wählen Sie unter Benachrichtigung das SNS-Thema aus, das benachrichtigt werden soll, wenn sich der Alarm im `ALARM` Status, `OK` Status oder `INSUFFICIENT_DATA` Zustand befindet. Um zu erreichen, dass der Alarm mehrere Benachrichtigungen für den gleichen Alarmstatus oder für verschiedene Statuswerte sendet, wählen Sie Benachrichtigung hinzufügen. Wählen Sie Weiter aus. Geben Sie einen Namen und eine Beschreibung für den Alarm ein. Der Name darf nur ASCII-Zeichen enthalten. Wählen Sie anschließend Weiter. Vergewissern Sie sich unter Vorschau und erstellen, dass die Informationen und Bedingungen korrekt sind, und wählen Sie dann Alarm erstellen aus.	DevOps Techniker, AWS DevOps

Zugehörige Ressourcen

- Veröffentlichen von benutzerdefinierten Metriken in CloudWatch
- Verwenden der CloudWatch Anomalieerkennung
- Alarmereignisse und Amazon EventBridge

- Was sind die bewährten Methoden, die Sie beim Pushen benutzerdefinierter Metriken an Cloud Watch befolgen sollten? (Video)
- Einführung in CloudWatch Application Insights (Video)
- Erkennen von Anomalien mit CloudWatch (Video)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Dokumentieren Ihres AWS-Landing-Zone-Designs

Erstellt von Bol Daehnert (AWS), Bolian Langer (AWS) und Bol Lodemann (AWS)

Umgebung: Produktion	Technologien: Management und Governance; Infrastruktur; Sicherheit, Identität, Compliance	AWS-Services: AWS Control Tower

Übersicht

Eine Landing Zone ist eine gut strukturierte Umgebung mit mehreren Konten, die auf bewährten Methoden für Sicherheit und Compliance basiert. Es ist der unternehmensweite Container, der alle Ihre Organisationseinheiten (OUs AWS-Konten),Benutzer und andere Ressourcen enthält. Eine Landing Zone kann so skaliert werden, dass sie den Anforderungen eines Unternehmens beliebiger Größe entspricht. AWS verfügt über zwei Möglichkeiten zum Erstellen Ihrer Landing Zone: eine servicebasierte Landing Zone mit AWS Control Tower oder eine angepasste Landing Zone, die Sie erstellen. Jede Option erfordert ein anderes Maß an AWS Wissen.

AWS erstellt, AWS Control Tower um Ihnen Zeit zu sparen, indem Sie die Einrichtung einer Landing Zone automatisieren. AWS Control Tower wird von verwaltet AWS und verwendet bewährte Methoden und Richtlinien, um Ihnen bei der Erstellung Ihrer grundlegenden Umgebung zu helfen. AWS Control Tower verwendet integrierte Services wie AWS Service Catalog und AWS Organizations, um Konten in Ihrer Landing Zone bereitzustellen und den Zugriff auf diese Konten zu verwalten.

AWS Landing Zone-Projekte unterscheiden sich in Anforderungen, Implementierungsdetails und operativen Maßnahmen. Es gibt Anpassungsaspekte, die bei jeder Implementierung der Landing Zone behandelt werden müssen. Dazu gehören (ist aber nicht darauf beschränkt), wie die Zugriffsverwaltung gehandhabt wird, welcher Technologie-Stack verwendet wird und welche Überwachungsanforderungen für Operational Excellence gelten. Dieses Muster enthält eine Vorlage, die Ihnen hilft, Ihr Landing-Zone-Projekt zu dokumentieren. Mithilfe der Vorlage können Sie Ihr Projekt schneller dokumentieren und Ihren Entwicklungs- und Betriebsteams helfen, Ihre Landing Zone zu verstehen.

Voraussetzungen und Einschränkungen

Einschränkungen

Dieses Muster beschreibt nicht, was eine Landing Zone ist oder wie eine implementiert wird. Weitere Informationen zu diesen Themen finden Sie im Abschnitt Verwandte Ressourcen.

Epics

Erstellen des Entwurfsdokuments

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die wichtigsten Stakeholder.	Identifizieren Sie wichtige Service- und Teammanager, die mit Ihrer Landing Zone verknüpft sind.	Projektmanager
Passen Sie die Vorlage an.	Laden Sie die Vorlage im Abschnitt Anhänge herunter und aktualisieren Sie die Vorlage dann wie folgt: 1. Entfernen Sie alle Abschnitte, die nicht für die Landing Zone oder Prozesse Ihrer Organisation gelten. 2. Fügen Sie alle Abschnitte hinzu, die für Ihre Organisation eindeutig sind.	Projektmanager
Schließen Sie die Vorlage ab.	Füllen Sie die Vorlage in Treffen mit den Stakeholdern oder mithilfe eines write-and-review Prozesses wie folgt aus: 1. Verwenden Sie die Anleitungen und Informati	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen in den blauen Feldern, um jeden Abschnitt abzuschließen. 2. Ersetzen oder entfernen Sie alle gelben Felder durch benutzerdefinierte Werte für Ihre Organisation. 3. Ersetzen oder entfernen Sie alle Image-Felder durch Ihre benutzerdefinierte Architektur oder Flussdiagramme. 4. Füllen Sie den Abschnitt Revisionsverlauf und Beitragende der Vorlage aus.	
Teilen Sie das Entwurfsdokument.	Wenn Ihre Dokumentation zum Design der Landing Zone abgeschlossen ist, speichern Sie sie in einem gemeinsamen Repository oder an einem zentralen Ort, an dem alle Stakeholder darauf zugreifen können. Wir empfehlen Ihnen, Standard-Dokumentenkontrollprozesse zu verwenden, um Revisionen des Entwurfsdokuments aufzuzeichnen und zu genehmigen.	Projektmanager

Zugehörige Ressourcen

- AWS Control Tower -Dokumentation

  - Planen Ihrer AWS Control Tower Landing Zone
  - AWS Strategie für mehrere Konten für Ihre AWS Control Tower Landing Zone
  - Administrative Tipps für die Einrichtung der Landing Zone
  - Erwartungen an die Konfiguration der Landing Zone
- Anpassungen für AWS Control Tower (AWS Solutions Library)
- Einrichten einer sicheren und skalierbaren AWS Umgebung mit mehreren Konten (AWS Prescriptive Guidance)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Richten Sie die CloudFormation AWS-Drift-Erkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein

Umgebung: Produktion	Technologien: Management und Verwaltung; Cloud-native Technologien; Infrastruktur; Betrieb; Modernisierung	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon SNS; AWS Config; AWS Lambda; AWS CloudFormation		

Übersicht

Kunden von Amazon Web Services (AWS) suchen häufig nach einer effizienten Methode, um Diskrepanzen bei der Ressourcenkonfiguration, einschließlich Abweichungen in CloudFormation AWS-Stacks, zu erkennen und diese so schnell wie möglich zu beheben. Dies ist insbesondere dann der Fall, wenn AWS Control Tower- oder AWS Landing Zone-Lösungen verwendet werden.

Dieses Muster bietet eine präskriptive Lösung, die das Problem effizient löst, indem konsolidierte Änderungen an der Ressourcenkonfiguration verwendet und auf diese Änderungen reagiert wird, um Ergebnisse zu erzielen. Die Lösung ist für Szenarien konzipiert, in denen mehrere CloudFormation Stapel in mehr als einer Region oder in mehr als einem Konto oder einer Kombination aus beidem erstellt werden. Die Lösung hat folgende Ziele:

- Vereinfachen Sie den Prozess zur Drifterkennung
- Richten Sie Benachrichtigungen und Warnmeldungen ein
- Richten Sie eine konsolidierte Berichterstattung ein

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS Config ist in allen Regionen und Konten aktiviert, die überwacht werden müssen

Einschränkungen

- Der generierte Bericht unterstützt nur die Ausgabeformate .csv oder .json.

Architektur

Zieltechnologie-Stack

Die aktuellen Leitlinien werden Unternehmen dabei helfen, dieses Ziel zu erreichen, indem sie eine Kombination der folgenden Dienste nutzen:

- AWS Config-Regel
- CloudWatch Amazon-Regel
- AWS Identity and Access Management (IAM)
- AWS Lambda
- Amazon-Simple-Notification-Service (Amazon-SNS)

1. Die AWS Config-Regel erkennt Abweichungen.
2. Die Ergebnisse der Drift-Erkennung in anderen Konten werden an das Verwaltungskonto gesendet.
3. Die CloudWatch Regel ruft Lambda auf.
4. Lambda fragt die AWS Config-Regel nach aggregierten Ergebnissen ab.
5. Lambda benachrichtigt Amazon SNS, das daraufhin eine E-Mail-Benachrichtigung über die Abweichung sendet.

Automatisierung und Skalierung

Die hier vorgestellte Lösung kann sowohl für zusätzliche Regionen als auch für Konten skaliert werden.

Tools

AWS Config — AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die

Konfigurationen und Beziehungen im Laufe der Zeit verändern. Mit AWS Config können Sie die Konfigurationen Ihrer AWS-Ressourcen bewerten, prüfen und auswerten.

Amazon CloudWatch — Amazon CloudWatch überwacht Ihre AWS-Ressourcen und die Anwendungen, die Sie auf AWS ausführen, in Echtzeit. Sie können CloudWatch damit Metriken sammeln und verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können.

AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.

Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht.

Epen

Automatisieren Sie die Drifterkennung für CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Aggregator.	Erstellen Sie in der AWS Config-Konsole einen Aggregator im Verwaltungskonto. Stellen Sie sicher, dass die Datenreplikation aktiviert ist, damit AWS Config Daten von den Quellkonten abrufen kann. Wählen Sie außerdem alle zutreffenden Regionen und Konten aus. Sie können Konten basierend auf Organisationen auswählen. Dies ist der empfohlene Ansatz, da neue Konten in der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Organisation automatisch Teil des Aggregators sind.	
Erstellen Sie eine von AWS verwaltete Regel.	Fügen Sie die von `cloudformation-stack-drift-detection-check` AWS verwaltete Regel hinzu. Die Regel benötigt einen Parameterwert:`cloudformationArn`. Geben Sie die IAM-Rolle Amazon Resource Name (ARN) ein, die berechtigt ist, Stack-Drift zu erkennen. Darüber hinaus muss die Rolle über eine Vertrauensrichtlinie verfügen, die es AWS Config ermöglicht, die Rolle zu übernehmen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Abschnitt für erweiterte Abfragen des Aggregators.	Um driftete Stapel aus mehreren Quellen abzurufen , erstellen Sie die folgende Abfrage: `SELECT resourceId, configuration.driftInformation.stackDriftStatus WHERE resourceType = 'AWS::CloudFormation::Stack'  AND configuration.driftInformation.stackDriftStatus IN ('DRIFTED')`	Cloud-Architekt, Entwickler
Automatisieren Sie die Ausführung der Abfrage und veröffentlichen Sie sie.	Erstellen Sie eine Lambda-Funktion mit dem angehängten Code. Lambda veröffentlicht die Ergebnisse in einem Amazon SNS SNS-Thema, das als Umgebungsvariable in der Lambda-Funktion bereitgestellt wird. Um Benachrichtigungen zu erhalten, müssen Sie außerdem ein E-Mail-Abonnement für ein vorhandenes Amazon SNS SNS-Thema erstellen.	Cloud-Architekt, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudWatch Regel.	Erstellen Sie eine zeitplanb asierte CloudWatch Regel, um die Lambda-Funktion aufzurufen, die für die Alarmierung zuständig ist.	Cloud-Architekt

Zugehörige Ressourcen

Ressourcen

- Was ist AWS Config?
- Konzepte: Datenaggregation mit mehreren Konten und mehreren Regionen
- Datenaggregation mit mehreren Konten und mehreren Regionen
- Erkennung nicht verwalteter Konfigurationsänderungen an Stacks und Ressourcen
- IAM: Übergeben Sie eine IAM-Rolle an einen bestimmten AWS-Service
- Was ist Amazon SNS?

Zusätzliche Informationen

Überlegungen

Es ist nicht optimal, maßgeschneiderte Lösungen zu verwenden, die API-Aufrufe in bestimmten Intervallen beinhalten, um die Drifterkennung für jeden CloudFormation Stack oder für Stack-Sets zu initiieren. Dies führt zu einer großen Anzahl von API-Aufrufen und beeinträchtigt die Leistung. Aufgrund der Anzahl der API-Aufrufe kann es zu einer Drosselung kommen. Ein weiteres potenzielles Problem ist eine Verzögerung bei der Erkennung, wenn Ressourcenänderungen nur anhand eines Zeitplans erkannt werden.

HÄUFIG GESTELLTE FRAGEN

F: Sollte ich eine auf Add-ons basierende Lösung mit AWS Landing Zone verwenden?

Antwort: Da die Funktion für erweiterte Abfragen in AWS Config zusammen mit dem Aggregator verfügbar ist, wird empfohlen, AWS Config anstelle eines Add-ons zu verwenden.

F: Wie funktioniert diese Lösung? CloudFormation StackSets

Antwort: Da Stack-Sets aus Stapeln bestehen, können Sie diese Lösung verwenden. Details zur Stack-Instanz sind auch als Teil der Lösung verfügbar.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verbessern Sie die betriebliche Leistung, indem Sie Amazon DevOps Guru über mehrere AWS-Regionen, Konten und OUs hinweg mit dem AWS-CDK aktivieren

Erstellt von Dr. Rahul Gaikwad (AWS)

Code-Repository: Beispielcode für Amazon DevOps Guru	Umgebung: PoC oder Pilotprojekt	Technologien: Management und Governance; Cloudnativ; DevOpsBetrieb; Sicherheit, Identität, Compliance; Serverless
AWS-Services: Amazon API Gateway; AWS CDK; Amazon DevOps Guru; Amazon DynamoDB ;AWS Organizations		

Übersicht

Dieses Muster zeigt die Schritte zum Aktivieren des Amazon DevOps -Guru-Service in mehreren Amazon Web Services (AWS)-Regionen, -Konten und Organisationseinheiten (OUs) mithilfe des AWS Cloud Development Kit (AWS CDK) in TypeScript. Sie können AWS-CDK-Stacks verwenden, um AWS CloudFormation StackSets vom Administratorkonto (primär) aus bereitzustellen und Amazon DevOps Guru über mehrere Konten hinweg zu aktivieren, anstatt sich bei jedem Konto anzumelden und DevOps Guru für jedes Konto einzeln zu aktivieren.

Amazon DevOps Guru bietet Funktionen für künstliche Intelligenz (AIOps mit denen Sie die Verfügbarkeit Ihrer Anwendungen verbessern und betriebliche Probleme schneller beheben können. DevOps Guru reduziert Ihren manuellen Aufwand, indem Empfehlungen auf Basis von Machine Learning (ML) angewendet werden, ohne dass ML-Erfahrung erforderlich ist. DevOps Guru analysiert Ihre Ressourcen und Betriebsdaten. Wenn es Anomalien erkennt, werden Metriken, Ereignisse und Empfehlungen bereitgestellt, die Ihnen bei der Behebung des Problems helfen.

Dieses Muster beschreibt drei Bereitstellungsoptionen für die Aktivierung von Amazon DevOps Guru:

- Für alle Stack-Ressourcen über mehrere Konten und Regionen hinweg
- Für alle Stack-Ressourcen über OUs hinweg
- Für bestimmte Stack-Ressourcen über mehrere Konten und Regionen hinweg

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. (Siehe Installieren, Aktualisieren und Deinstallieren der AWS CLI in der AWS CLI-Dokumentation.)
- AWS CDK Toolkit, installiert und konfiguriert. (Siehe AWS CDK Toolkit in der AWS CDK-Dokumentation.)
- Node Package Manager (npm), installiert und für das AWS-CDK in konfiguriert TypeScript. (Siehe Herunterladen und Installieren von Node.js und npm in der npm-Dokumentation.)
- Python3 installiert und konfiguriert, um ein Python-Skript auszuführen, um Datenverkehr in die Serverless-Beispielanwendung einzufügen. (Siehe Python-Einrichtung und -Nutzung in der Python-Dokumentation.)
- Pip, installiert und konfiguriert, um die Python-Anforderungsbibliothek zu installieren. (Siehe die Pip-Installationsanweisungen auf der - PyPI Website.)

Produktversionen

- AWS CDK Toolkit Version 1.107.0 oder höher
- npm Version 7.9.0 oder höher
- Node.js Version 15.3.0 oder höher

Architektur

Technologien

Die Architektur für dieses Muster umfasst die folgenden Services:

- Amazon DevOps Guru
- AWS CloudFormation

- Amazon API Gateway
- AWS Lambda
- Amazon DynamoDB
- Amazon CloudWatch
- AWS CloudTrail

AWS-CDK-Stacks

Das Muster verwendet die folgenden AWS-CDK-Stacks:

- `CdkStackSetAdminRole` – Erstellt eine AWS Identity and Access Management (IAM)-Administratorrolle, um eine Vertrauensstellung zwischen den Administrator- und Zielkonten herzustellen.
- `CdkStackSetExecRole` – Erstellt eine IAM-Rolle, die dem Administratorkonto vertraut.
- `CdkDevopsGuruStackMultiAccReg` – Aktiviert DevOps Guru in mehreren AWS-Regionen und -Konten für alle Stacks und richtet Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen ein.
- `CdkDevopsGuruStackMultiAccRegSpecStacks` – Aktiviert DevOps Guru über mehrere AWS-Regionen und -Konten hinweg für bestimmte Stacks und richtet Amazon SNS-Benachrichtigungen ein.
- `CdkDevopsguruStackOrgUnit` – Aktiviert DevOps Guru über OUs hinweg und richtet Amazon SNS-Benachrichtigungen ein.
- `CdkInfrastructureStack` – Stellt Beispiele für Serverless-Anwendungskomponenten wie API Gateway, Lambda und DynamoDB im Administratorkonto bereit, um Fehlersimulation und Generierung von Erkenntnissen zu demonstrieren.

Beispielanwendungsarchitektur

Das folgende Diagramm veranschaulicht die Architektur einer Beispielanwendung für Serverless, die über mehrere Konten und Regionen hinweg bereitgestellt wurde. Das Muster verwendet das Administratorkonto, um alle AWS-CDK-Stacks bereitzustellen. Es verwendet auch das Administratorkonto als eines der Zielkonten für die Einrichtung von DevOps Guru.

1. Wenn DevOps Guru aktiviert ist, wird zunächst das Verhalten jeder Ressource untersucht und anschließend Betriebsdaten aus CloudWatch verkauften Metriken erfasst.

2. Wenn es eine Anomalie erkennt, korreliert es sie mit den Ereignissen von CloudTrailund generiert einen Einblick.
3. Die Erkenntnis bietet eine korrelierte Abfolge von Ereignissen zusammen mit vorgeschriebenen Empfehlungen, damit der Operator die culprit-Ressource identifizieren kann.
4. Amazon SNS sendet Benachrichtigungen an den Operator.

Automatisierung und Skalierung

Das mit diesem Muster bereitgestellte GitHub Repository verwendet das AWS-CDK als Infrastructure as Code (IaC)-Tool, um die Konfiguration für diese Architektur zu erstellen.IaC AWS CDK hilft Ihnen, Ressourcen zu orchestrieren und DevOps Guru über mehrere AWS-Konten, Regionen und OUs hinweg zu aktivieren.

Tools

AWS-Services

- AWS CDK – AWS Cloud Development Kit (AWS CDK) hilft Ihnen, Ihre Cloud-Infrastruktur als Code in einer von fünf unterstützten Programmiersprachen zu definieren: TypeScript, JavaScript, Python, Java und C#.
- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool, das eine konsistente Befehlszeilenschnittstelle für die Interaktion mit AWS-Services und -Ressourcen bietet.

Code

Der Quellcode für dieses Muster ist auf GitHubim Amazon- DevOps Guru-CDK-Samples-Repository verfügbar. Der AWS-CDK-Code ist in geschrieben TypeScript. Um das Repository zu klonen und zu verwenden, folgen Sie den Anweisungen im nächsten Abschnitt.

Wichtig: Einige der Beiträge in diesem Muster sind AWS-CDK- und AWS-CLI-Befehlsbeispiele, die für Unix, Linux und macOS formatiert sind. Ersetzen Sie für Windows den umgekehrten Schrägstrich (\) am Ende jeder Zeile durch ein Pflegezeichen (^).

Sekunden

Vorbereiten der AWS-Ressourcen für die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie von AWS benannte Profile.	Richten Sie Ihre von AWS benannten Profile wie folgt ein, um Stacks in einer Umgebung mit mehreren Konten bereitzustellen.
	
	Für das Administratorkonto:
	
	`$aws configure --profile administrator`
	`AWS Access Key ID [****]: <your-administrator-access-key-ID>`
	`AWS Secret Access Key [****]: <your-administrator-secret-access-key>`
	`Default region name [None]: <your-administrator-region>`
	`Default output format [None]: json`
	
	Für das Zielkonto:
	
	`$aws configure --profile target`
	`AWS Access Key ID [****: <your-target-access-key-ID>`
	`AWS Secret Access Key [****]: <your-target-secret-access-key>`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Default region name [None]: <your-target-region>`
	`Default output format [None]: json`
	
	Weitere Informationen finden Sie unter Verwenden benannter Profile in der AWS CLI-Dokumentation.	

Überprüfen Sie die AWS-Profilkonfigurationen.	(Optional) Sie können Ihre AWS-Profilkonfigurationen in den `config` Dateien `credentials` und überprüfen, indem Sie den Anweisungen unter Festlegen und Anzeigen von Konfigurationseinstellungen in der AWS CLI-Dokumentation folgen.	DevOps Techniker
Überprüfen Sie die AWS-CDK-Version.	Überprüfen Sie die Version des AWS CDK Toolkits, indem Sie den folgenden Befehl ausführen: `$cdk --version` Dieses Muster erfordert Version 1.107.0 oder höher. Wenn Sie eine frühere Version des AWS-CDK haben, folgen Sie den Anweisungen in der AWS-CDK-Dokumentation, um es zu aktualisieren.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie den Projektcode.	Klonen Sie das GitHub Repository für dieses Muster mit dem Befehl : `$git clone https://github.com/aws-samples/amazon-devopsguru-cdk-samples.git`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Paketabhä ngigkeiten und kompilieren Sie die TypeScript Dateien.	Installieren Sie die Paketabhä ngigkeiten und kompilieren Sie die TypeScript Dateien, indem Sie die folgenden Befehle ausführen:
	`$cd amazon-devopsguru-cdk-samples`
	`$npm install`
	`$npm fund`
	Mit diesen Befehlen werden alle Pakete aus dem Beispiel-Repository installiert.
	Wichtig: Wenn Sie Fehler zu fehlenden Paketen erhalten, verwenden Sie einen der folgenden Befehle:
	`$npm ci`
	–oder–
	`$npm install -g @aws-cdk/<package-name>`
	Die Liste der Paketnamen und -versionen finden Sie im `-Dependencies` Abschnitt der `-/amazon-devopsguru-cdk-samples/package.json` Datei. Weitere Informationen finden Sie unter
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	npm ci und npm install in der npm-Dokumentation.	

Erstellen (Synthetisieren) der AWS-CDK-Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine E-Mail-Adresse für Amazon SNS-Benachrichtigungen.	Gehen Sie wie folgt vor, um eine E-Mail-Adresse für Amazon SNS-Benachrichtigungen anzugeben: 1. Bearbeiten Sie die Dateien `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-stack.ts` und `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-org-uni-stack.ts` . 2. Aktualisieren Sie im `DevOpsGuruTopic Subscription` Abschnitt , den `Endpoint` Parameter mit Ihrer E-Mail-Adresse. 3. Speichern und schließen Sie die Dateien.	DevOps Techniker
Erstellen Sie den Projektcode.	Erstellen Sie den Projektcode und synthetisieren Sie die	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Stacks, indem Sie den Befehl ausführen:
	`npm run build && cdk synth`
	Die Ausgabe sollte folgender maßen oder ähnlich aussehen:
	`$npm run build && cdk synth`
	`> cdk-devopsguru@0.1.0 build`
	`> tsc`
	`Successfully synthesized to ~/amazon-devopsguru-cdk-samples/cdk.out`
	`Supply a stack id (CdkDevopsGuruStackMultiAccReg,CdkDevopsGuruStackMultiAccRegSpecStacks, CdkDevopsguruStackOrgUnit, CdkInfrastructureStack, CdkStackSetAdminRole, CdkStackSetExecRole) to display its template.`
	Weitere Informationen und Schritte finden Sie unter Ihre erste AWS-CDK-App in der AWS-CDK-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Listen Sie die AWS-CDK-Stacks auf.	Führen Sie den folgenden Befehl aus, um alle AWS-CDK-Stacks aufzulisten:
	`$cdk list`
	Der Befehl zeigt die folgende Liste an:
	`CdkDevopsGuruStack`
	`MultiAccReg`
	`CdkDevopsGuruSt`
	`ackMultiAccRegSpec`
	`Stacks`
	`CdkDevopsguruStackOr`
	`gUnit`
	`CdkInfrastructureStac`
	`k`
	`CdkStackSetAdminRole`
	`CdkStackSetExecRole`
		DevOps Techniker

Option 1 – DevOps Guru für alle Stack-Ressourcen über mehrere Konten hinweg aktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CDK-Stacks zum Erstellen von IAM-Rollen bereit.	Dieses Muster verwendet AWS CloudFormation StackSets, um Stack-Operationen über mehrere Konten hinweg auszuführen. Wenn Sie Ihr erstes StackSet erstellen, müssen Sie die folgenden IAM-Rollen erstellen, um die erforderl	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ichen Berechtigungen in Ihren AWS-Konten einzurichten: • `AWSCloudFormationStackSetAdministrationRole` • `AWSCloudFormationStackSetExecutionRole` Hinweis: Die Rollen müssen genau diese Namen haben. 1. Erstellen Sie die IAM-`AWSCloudFormationStackSetAdministrationRole` Rolle im Administratorkonto (primär), indem Sie den folgenden CLI-Befehl ausführen: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Erstellen Sie die IAM-`AWSCloudFormationStackSetExecutionRole` Rolle in allen Zielkonten, in denen Sie die Stack-Instances ausführen möchten. Um diese Rolle zu erstellen, führen Sie die folgenden CLI-Befehle aus:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$cdk deploy CdkStackSetExecRole \ --parameters AdministratorAccountId=<administrator-account-ID> \ --profile administrator`
	
	`$cdk deploy CdkStackSetExecRole \ --parameters AdministratorAccountId=<administrator-account-ID> \ --profile target`
	
	Weitere Informationen finden Sie unter Selbstverwaltete Berechtigungen erteilen in der AWS- CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS-CDK-Stack bereit, um DevOps Guru für mehrere Konten zu aktivieren.	Der AWS-CDK-`CdkDevopsGuruStackMultiAccReg` Stack erstellt Stack-Sets, um Stack-Instances über mehrere Konten und Regionen hinweg bereitzustellen. Um den Stack bereitzustellen, führen Sie den folgenden CLI-Befehl mit den angegebenen Parametern aus: `$cdk deploy CdkDevopsGuruStackMultiAccReg \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` Derzeit ist Amazon DevOps Guru in den AWS-Regionen verfügbar, die unter Häufig gestellte DevOps Fragen zu Guru aufgeführt sind.	DevOps Techniker

Option 2 – DevOps Guru für alle Stack-Ressourcen über OUs hinweg aktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie OU-IDs.	Identifizieren Sie in der AWS Organizations-Konsole die IDs der Organisationseinheiten, in denen Sie DevOps Guru aktivieren möchten.	DevOps Techniker
Aktivieren Sie serviceverwaltete Berechtigungen für OUs	Wenn Sie AWS Organizations für die Kontoverwaltung verwenden, müssen Sie serviceverwaltete Berechtigungen erteilen, um DevOps Guru zu aktivieren. Anstatt die IAM-Rollen manuell zu erstellen, verwenden Sie den organisationsbasierten vertrauenswürdigen Zugriff und serviceverknüpfte Rollen (SLRs).	DevOps Techniker

Stellen Sie den AWS-CDK-Stack für die Aktivierung von DevOps Guru über OUs hinweg bereit.	Der AWS-CDK-`CdkDevopsguruStackOrgUnit` Stack ermöglicht den DevOps Guru-Service über OUs hinweg. Um den Stack bereitzustellen, führen Sie den folgenden Befehl mit den angegebenen Parametern aus:
	`$cdk deploy CdkDevopsguruStackOrgUnit \`
	`--profile administrator \`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--parameters RegionIds="<region-1>,<region-2>" \ --parameters OrganizationalUnitIds="<OU-1>,<OU-2>"`	

Option 3 – DevOps Guru für bestimmte Stack-Ressourcen über mehrere Konten hinweg aktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CDK-Stacks zum Erstellen von IAM-Rollen bereit.	Wenn Sie noch nicht die erforderlichen IAM-Rollen erstellt haben, die in der ersten Option angezeigt werden, gehen Sie zuerst wie folgt vor: 1. Erstellen Sie die IAM-`AWSCloudFormationStackSetAdministrationRole` Rolle im Administratorkonto (primär), indem Sie den folgenden CLI-Befehl ausführen: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Erstellen Sie die IAM-`AWSCloudFormationStackSetExecutionRole` Rolle in allen Zielkonten, in denen	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie die Stack-Instances ausführen möchten. Um diese Rolle zu erstellen, führen Sie die CLI-Befehle aus:
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile administrator`
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile target`
	
	Weitere Informationen finden Sie unter Selbstverwaltete Berechtigungen erteilen in der AWS- CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie vorhandene Stacks.	Wenn Sie DevOps Guru bereits mit der ersten Option für alle Stack-Ressourcen aktiviert haben, können Sie den alten Stack mit dem folgenden Befehl löschen: `$cdk destroy CdkDevopsGuruStackMultiAccReg --profile administrator` Oder Sie können den `RegionIds` Parameter ändern, wenn Sie den Stack erneut bereitstellen, um einen Fehler Stacks bereits vorhanden zu vermeiden.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den AWS-CDK-Stack mit einer Stack-Liste.	1. Bearbeiten Sie die `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-spec-stack.ts` -Datei. 2. Listen Sie unter `Resources` , `CloudFormation StackNames` , die Stacks auf, für die Sie DevOps Guru aktivieren möchten. Zu Demonstrationszwecken gibt der Parameter den `CdkInfrastructureStack` Stack an, Sie können diesen Eintrag jedoch je nach Ihren Anforderungen bearbeiten. 3. Speichern und schließen Sie die Datei. 4. Um die Stack-Vorlage zu synthetisieren und zu aktualisieren, führen Sie Folgendes aus: `$cdk synth`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS-CDK-Stack bereit, um DevOps Guru für bestimmte Stack-Ressourcen über mehrere Konten hinweg zu aktivieren.	Der AWS-CDK-`CdkDevopsGuruStackMultiAccRegSpecStacks` Stack aktiviert DevOps Guru für bestimmte Stack-Ressourcen über mehrere Konten hinweg. Führen Sie den folgenden Befehl aus, um den Stack bereitzustellen: `$cdk deploy CdkDevopsGuruStackMultiAccRegSpecStacks \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` Hinweis: Wenn Sie diesen Stack zuvor für Option 1 bereitgestellt haben, ändern Sie den `RegionIds` Parameter (wobei Sie aus den verfügbaren Regionen auswählen müssen), um einen Fehler Stacks bereits vorhanden zu vermeiden.	DevOps Techniker

Bereitstellen des AWS-CDK-Infrastruktur-Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Beispiel-Serverless-Infrastruktur-Stack bereit.	Der AWS-CDK-`CdkInfrastructureStack` Stack stellt Serverless-Komponenten wie API Gateway, Lambda und eine DynamoDB-Tabelle bereit, um DevOps Guru-Insights zu demonstrieren. Führen Sie den folgenden Befehl aus, um den Stack bereitzustellen: `$cdk deploy CdkInfrastructureStack --profile administrator`	DevOps Techniker
Fügen Sie Beispieldatensätze in DynamoDB ein.	Führen Sie den folgenden Befehl aus, um die DynamoDB-Tabelle mit Beispieldatensätzen zu füllen. Geben Sie den richtigen Pfad für das `populate-shops-dynamodb-table.json` Skript an. `$aws dynamodb batch-write-item \ --request-items file://scripts/populate-shops-dynamodb-table.json \ --profile administrator` Die Ausgabe des Befehls sieht wie folgt aus:	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	"UnprocessedItems"
	: {}
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die eingefügten Datensätze in DynamoDB .	Um zu überprüfen, ob die DynamoDB-Tabelle die Beispieldatensätze aus der `-populate-shops-dynamodb-table.json` Datei enthält, greifen Sie auf die URL für die `ListRestApiEndpointMonitorOperator` API zu, die als Ausgabe des AWS-CDK-Stacks veröffentlicht wird. Sie finden diese URL auch auf der Registerkarte Outputs der AWS- CloudFormation Konsole für den `CdkInfrastructureStack` Stack. Die AWS-CDK-Ausgabe würde in etwa wie folgt aussehen:
	`CdkInfrastructureStack.CreateRestApiMonitorOperatorEndpointD1D00045 = https://oure17c5vob.execute-api.<your-region>.amazonaws.com/prod/`
	
	`CdkInfrastructureStack.ListRestApiMonitorOperatorEndpointABBDB8D8 = https://cdff8icfrn4.execute-api.<your-region>.amazonaws.com/prod/`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Warten Sie, bis die Ressourcen das Baselining abgeschlossen haben.	Dieser Serverless-Stack verfügt über einige Ressourcen. Wir empfehlen Ihnen, 2 Stunden zu warten, bevor Sie die nächsten Schritte ausführen. Wenn Sie diesen Stack in einer Produktionsumgebung bereitgestellt haben, kann es je nach der Anzahl der Ressourcen, die Sie in DevOps Guru überwacht haben, bis zu 24 Stunden dauern, bis die Basislinierung abgeschlossen ist.	DevOps Techniker

Generieren von DevOps Guru-Erkenntnissen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den AWS-CDK-Infrastruktur-Stack.	Um DevOps Guru Insights auszuprobieren, können Sie einige Konfigurationsänderungen vornehmen, um ein typisches Betriebsproblem zu reproduzieren. 1. Bearbeiten Sie die `/amazon-devopsguru-cdk-samples/lib/infrastructure-stack.ts` -Datei. 2. Ändern Sie im `DDB Table` Abschnitt die Lesekapazität	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	für die DynamoDB-Tabelle von 5 auf 1.
	3. Speichern und schließen Sie die Datei.
	4. Führen Sie die folgenden Befehle aus, um den aktualisierten AWS-CDK-Infrastruktur-Stack zu synthetisieren und bereitzustellen:
	`$cdk synth`
	`$cdk deploy CdkInfrastructureStack --profile administrator`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Injizieren Sie HTTP-Anfragen auf der API.	Injizieren Sie eingehend en Datenverkehr in Form von HTTP-Anfragen an die `ListRestApiMonitor 0peratorEndpointxx xx` API: 1. Bearbeiten Sie das Python-Skript `/amazon-d evopsguru-cdk-samp les/scripts/sendAP IRequest.py` . 2. Aktualisieren Sie die `url` Variable mit dem API-Link für `ListRestA piMonitor0peratorE ndpointxxxx` . Diese URL finden Sie in der Ausgabe des AWS-CDK-Bereitstellungsbefehls oder in der AWS Cloudform ation-Konsole auf der Registerkarte Outputs für den Stack. 3. Speichern und schließen Sie die Datei. 4. Führen Sie das Python-Sk ript mit dem Befehl aus: `$python sendAPIRe quest.py` 5. Stellen Sie sicher, dass Sie den Statuscode 200 erhalten.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Möglicherweise müssen Sie das Skript über mehrere (vorzugsweise vier) Terminals ausführen, um Datenverkehr mit hoher Geschwindigkeit zu injiziere n. 7. Nachdem das Skript etwa 10 Minuten in einer Schleife ausgeführt wurde, können Sie einen operativen Einblick in die DevOps Guru-Konsole sehen.	
Überprüfen Sie DevOps Guru Insights.	Unter Standardbedingunge n zeigt das DevOps Guru-Dashboard Null im Zähler für laufende Erkenntnisse an. Wenn eine Anomalie erkannt wird, wird eine Warnung in Form eines Insight ausgelöst . Wählen Sie im Navigatio nsbereich Insights aus, um die Details der Anomalie anzuzeigen, einschließlich einer Übersicht, aggregierter Metriken, relevanter Ereigniss e und Empfehlungen. Weitere Informationen zur Überprüfu ng von Erkenntnissen finden Sie im Blogbeitrag Gewinnen betrieblicher Erkenntnisse mit AIOps mithilfe von Amazon DevOps Guru.	DevOps Techniker

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen und Löschen von Ressourcen.	Nachdem Sie dieses Muster durchgegangen sind, sollten Sie die von Ihnen erstellte n Ressourcen entfernen, um weitere Gebühren zu vermeiden. Führen Sie die folgenden Befehle aus:
	`$cdk destroy CdkDevops GuruStackMultiAccR eg --profile administr ator`
	`$cdk destroy CdkDevops guruStackOrgUnit -- profile administrator`
	`$cdk destroy CdkDevops GuruStackMultiAccR egSpecStacks --profile administrator`
	`$cdk destroy CdkInfras tructureStack -- profile administrator`
	`$cdk destroy CdkStackS etAdminRole --profile administrator`
	`$cdk destroy CdkStackS etExecRole --profile administrator`
	`$cdk destroy CdkStackS etExecRole --profile target`
		DevOps Techniker

Zugehörige Ressourcen

- Gewinnen betrieblicher Einblicke mit AIOps unter Verwendung von Amazon DevOps Guru

- Einfache Konfiguration von Amazon DevOps Guru über mehrere Konten und Regionen hinweg mit AWS CloudFormation StackSets
- DevOps Guru-Workshop

Implementieren Sie Account Factory for Terraform (AFT) mithilfe einer Bootstrap-Pipeline

Erstellt von Vinicius Elias (AWS) und Edgar Costa Filho (AWS)

Code-Repository: aft-bootstrap-pipeline	Umgebung: Produktion	Technologien: Management und Verwaltung; Infrastruktur
Arbeitslast: Open Source	AWS-Services: AWS CodeBuild CodeCommit; AWS CodePipeline; AWS Control Tower; AWS Organizations	

Übersicht

Dieses Muster bietet eine einfache und sichere Methode für die Bereitstellung von AWS Control Tower Account Factory for Terraform (AFT) über das Verwaltungskonto von. AWS Organizations Der Kern der Lösung ist eine AWS CloudFormation Vorlage, die die AFT-Konfiguration automatisiert, indem eine Terraform-Pipeline erstellt wird, die so strukturiert ist, dass sie für die erste Bereitstellung oder nachfolgende Updates leicht angepasst werden kann.

Sicherheit und Datenintegrität haben bei uns oberste Priorität. AWS Daher wird die Terraform-Statusdatei, eine wichtige Komponente, die den Status der verwalteten Infrastruktur und Konfigurationen verfolgt, sicher in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert. Dieser Bucket ist mit verschiedenen Sicherheitsmaßnahmen konfiguriert, darunter serverseitige Verschlüsselung und Richtlinien zur Blockierung des öffentlichen Zugriffs, um sicherzustellen, dass Ihr Terraform-Status vor unbefugtem Zugriff und Datenschutzverletzungen geschützt ist.

Das Verwaltungskonto orchestriert und überwacht die gesamte Umgebung, sodass es sich um eine wichtige Ressource in der Umgebung handelt. AWS Control Tower Dieses Muster folgt AWS bewährten Methoden und stellt sicher, dass der Bereitstellungsprozess nicht nur effizient ist, sondern auch den Sicherheits- und Governance-Standards entspricht, um eine umfassende, sichere und effiziente Möglichkeit zur Bereitstellung von AFT in Ihrer Umgebung zu bieten. AWS

Weitere Informationen zu AFT finden Sie in der AWS Control Tower Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine einfache Umgebung mit AWS mehreren Konten mit mindestens den folgenden Konten: Verwaltungskonto, Protokollarchivkonto, Auditkonto und einem zusätzlichen Konto für die AFT-Verwaltung.
- Eine etablierte AWS Control Tower Umgebung. Das Verwaltungskonto sollte ordnungsgemäß konfiguriert sein, da die CloudFormation Vorlage darin bereitgestellt wird.
- Die erforderlichen Berechtigungen im AWS Verwaltungskonto. Sie benötigen ausreichende Berechtigungen, um Ressourcen wie S3-Buckets, AWS Lambda Funktionen, AWS Identity and Access Management (IAM-) Rollen und Projekte zu erstellen und AWS CodePipeline zu verwalten.
- Vertrautheit mit Terraform. Es ist wichtig, die Kernkonzepte und den Arbeitsablauf von Terraform zu verstehen, da die Bereitstellung die Generierung und Verwaltung von Terraform-Konfigurationen beinhaltet.

Einschränkungen

- Beachten Sie die AWS Ressourcenkontingente in Ihrem Konto. Durch die Bereitstellung werden möglicherweise mehrere Ressourcen erstellt, und das Erreichen von Dienstkontingenten könnte den Bereitstellungsprozess behindern.
- Die Vorlage wurde für bestimmte Versionen von Terraform und entwickelt. AWS-Services Für das Aktualisieren oder Ändern von Versionen sind möglicherweise Änderungen an der Vorlage erforderlich.

Produktversionen

- Terraform Version 1.5.7 oder höher
- AFT-Version 1.11.1 oder höher

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CodeBuild

- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- IAM
- AWS Lambda
- Amazon S3

Zielarchitektur

Das folgende Diagramm veranschaulicht die Implementierung, die in diesem Muster beschrieben wird.

Der Workflow besteht aus drei Hauptaufgaben: dem Erstellen der Ressourcen, dem Generieren des Inhalts und dem Ausführen der Pipeline.

Die Ressourcen erstellen

Die mit diesem Muster bereitgestellte CloudFormation Vorlage erstellt und richtet alle erforderlichen Ressourcen ein, abhängig von den Parametern, die Sie bei der Bereitstellung der Vorlage auswählen. Die Vorlage erstellt mindestens die folgenden Ressourcen:

- Ein CodeCommit Repository zum Speichern des AFT Terraform-Bootstrap-Codes
- Ein S3-Bucket zum Speichern der Terraform-Statusdatei, die der AFT-Implementierung zugeordnet ist
- Eine Pipeline CodePipeline
- Zwei CodeBuild Projekte zur Implementierung des Terraform-Plans und zur Anwendung von Befehlen in verschiedenen Phasen der Pipeline
- IAM-Rollen für und Dienste CodeBuild CodePipeline
- Ein zweiter S3-Bucket zum Speichern von Pipeline-Laufzeitartefakten
- Eine EventBridge Regel zum Erfassen von CodeCommit Repository-Änderungen im `main` Branch
- Eine weitere IAM-Rolle für die Regel EventBridge

Wenn Sie den `Generate AFT Files` Parameter in der Vorlage auf festlegen`true`, erstellt die CloudFormation Vorlage außerdem die folgenden zusätzlichen Ressourcen, um den Inhalt zu generieren:

- Ein S3-Bucket zum Speichern des generierten Inhalts und zur Verwendung als Quelle für das CodeCommit Repository
- Eine Lambda-Funktion, um die angegebenen Parameter zu verarbeiten und den entsprechenden Inhalt zu generieren
- Eine IAM-Funktion zum Ausführen der Lambda-Funktion
- Eine CloudFormation benutzerdefinierte Ressource, die die Lambda-Funktion ausführt, wenn die Vorlage bereitgestellt wird

Der Inhalt wird generiert

Um die AFT-Bootstrap-Dateien und deren Inhalt zu generieren, verwendet die Lösung eine Lambda-Funktion und einen S3-Bucket. Die Funktion erstellt einen Ordner im Bucket und anschließend zwei Dateien innerhalb des Ordners: `main.tf` und. `backend.tf` Die Funktion verarbeitet auch die angegebenen CloudFormation Parameter und füllt diese Dateien mit vordefiniertem Code, wodurch die jeweiligen Parameterwerte ersetzt werden.

Den Code, der als Vorlage für die Generierung der Dateien verwendet wird, finden Sie im GitHub Repository der Lösung. Im Grunde werden die Dateien wie folgt generiert.

main.tf

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory?
ref=<aft_version>"

  # Required variables
  ct_management_account_id  = "<ct_management_account_id>"
  log_archive_account_id    = "<log_archive_account_id>"
  audit_account_id          = "<audit_account_id>"
  aft_management_account_id = "<aft_management_account_id>"
  ct_home_region            = "<ct_home_region>"

  # Optional variables
  tf_backend_secondary_region = "<tf_backend_secondary_region>"
  aft_metrics_reporting       = "<false|true>"
```

```
  # AFT Feature flags
  aft_feature_cloudtrail_data_events      = "<false|true>"
  aft_feature_enterprise_support          = "<false|true>"
  aft_feature_delete_default_vpcs_enabled = "<false|true>"

  # Terraform variables
  terraform_version      = "<terraform_version>"
  terraform_distribution = "<terraform_distribution>"

}
```

Backend.tf

```
terraform {
  backend "s3" {
    region = "<aft-main-region>"
    bucket = "<s3-bucket-name>"
    key    = "aft-setup.tfstate"
  }
}
```

Wenn Sie den `Generate AFT Files` Parameter während der CodeCommit Repository-Erstellung auf setzen`true`, verwendet die Vorlage den S3-Bucket mit dem generierten Inhalt als Quelle für den `main` Branch, um das Repository automatisch zu füllen.

Die Pipeline ausführen

Nachdem die Ressourcen erstellt und die Bootstrap-Dateien konfiguriert wurden, wird die Pipeline ausgeführt. In der ersten Phase (Source) wird der Quellcode aus dem Hauptzweig des Repositorys abgerufen, und in der zweiten Phase (Build) wird der Befehl Terraform Plan ausgeführt und die zu überprüfenden Ergebnisse generiert. In der dritten Phase (Genehmigung) wartet die Pipeline auf eine manuelle Aktion, um die letzte Phase (Deploy) zu genehmigen oder abzulehnen. In der letzten Phase führt die Pipeline den `apply` Terraform-Befehl aus, indem sie das Ergebnis des vorherigen `plan` Terraform-Befehls als Eingabe verwendet. Schließlich werden eine kontoübergreifende Rolle und die Berechtigungen im Verwaltungskonto verwendet, um die AFT-Ressourcen im AFT-Verwaltungskonto zu erstellen.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Lambdaist ein Rechendienst, der Ihren Code als Reaktion auf Ereignisse ausführt und Rechenressourcen automatisch verwaltet. So können Sie schnell eine moderne, serverlose Anwendung für die Produktion erstellen.
- AWS SDK for Python (Boto3)ist ein Software-Entwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript in AWS-Services integrieren können.

Andere Tools

- Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie Infrastrukturen sicher und effizient erstellen, ändern und versionieren können. Dazu gehören Komponenten auf niedriger Ebene wie Recheninstanzen, Speicher und Netzwerke sowie Komponenten auf hoher Ebene wie DNS-Einträge und SaaS-Funktionen.
- Python ist eine leicht zu erlernende, leistungsstarke Programmiersprache. Sie verfügt über effiziente Datenstrukturen auf hoher Ebene und bietet einen einfachen, aber effektiven Ansatz für objektorientierte Programmierung.

Code-Repository

Der Code für dieses Muster ist im GitHub AFT-Bootstrap-Pipeline-Repository verfügbar.

Das offizielle AFT-Repository finden Sie unter AWS Control Tower Account Factory for Terraform unter. GitHub

Bewährte Methoden

Wenn Sie AFT mithilfe der bereitgestellten CloudFormation Vorlage bereitstellen, empfehlen wir Ihnen, bewährte Methoden zu befolgen, um eine sichere, effiziente und erfolgreiche Implementierung zu gewährleisten. Zu den wichtigsten Richtlinien und Empfehlungen für die Implementierung und den Betrieb des AFT gehören die folgenden.

- Gründliche Überprüfung der Parameter: Prüfen Sie jeden Parameter in der CloudFormation Vorlage sorgfältig und verstehen Sie ihn. Eine genaue Parameterkonfiguration ist entscheidend für die korrekte Einrichtung und Funktion von AFT.
- Regelmäßige Vorlagenaktualisierungen: Halten Sie die Vorlage mit den neuesten AWS Funktionen und Terraform-Versionen auf dem neuesten Stand. Regelmäßige Updates helfen Ihnen dabei, neue Funktionen zu nutzen und die Sicherheit zu gewährleisten.
- Versionierung: Legen Sie die Version Ihres AFT-Moduls fest und verwenden Sie, wenn möglich, eine separate AFT-Bereitstellung zum Testen.
- Umfang: Verwenden Sie AFT nur, um Infrastruktur-Leitplanken und Anpassungen bereitzustellen. Verwenden Sie es nicht, um Ihre Anwendung bereitzustellen.
- Linting und Validierung: Die AFT-Pipeline erfordert eine verknüpfte und validierte Terraform-Konfiguration. Führen Sie Lint, Validation und Test aus, bevor Sie die Konfiguration in die AFT-Repositorys übertragen.
- Terraform-Module: Erstellen Sie wiederverwendbaren Terraform-Code als Module und geben Sie immer die Terraform- und AWS Provider-Versionen an, die den Anforderungen Ihres Unternehmens entsprechen.

Epen

Richten Sie die Umgebung ein und konfigurieren Sie sie AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereite die AWS Control Tower Umgebung vor.	Richten Sie sie AWS Control Tower in Ihrer AWS Umgebung ein und konfiguri eren Sie sie, um eine zentrale Verwaltung und Steuerung für	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie zu gewährleisten AWS-Konten. Weitere Informationen finden Sie AWS Control Tower in der AWS Control Tower Dokumentation unter Erste Schritte mit.	
Starten Sie das AFT-Verwaltungskonto.	Verwenden Sie die AWS Control Tower Account Factory, um ein neues Konto AWS-Konto zu eröffnen, das als Ihr AFT-Verwaltungskonto dient. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter Konten mit AWS Service Catalog Account Factory bereitstellen.	Cloud-Administrator

Stellen Sie die CloudFormation Vorlage im Verwaltungskonto bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage.	In diesem Epic stellen Sie die mit dieser Lösung bereitgestellte CloudFormation Vorlage bereit, um die AFT-Bootstrap-Pipeline in Ihrem AWS Verwaltungskonto einzurichten. Die Pipeline stellt die AFT-Lösung in dem AFT-Verwaltungskonto bereit, das Sie im vorherigen Epic eingerichtet haben.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schritt 1: Öffnen Sie die Konsole AWS CloudFormation • Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole. Stellen Sie sicher, dass Sie in der richtigen AWS Control Tower Hauptregion tätig sind. Schritt 2: Erstellen Sie einen neuen Stack 1. Wählen Sie, ob Sie einen neuen Stapel erstellen möchten. 2. Wählen Sie die Option zum Hochladen einer Vorlagend atei und laden Sie die CloudFormation Vorlage hoch, die mit diesem Muster bereitgestellt wurde. Schritt 3: Konfigurieren Sie die Stack-Parameter • `Repository Name` : Geben Sie den Repository-Namen zum Speichern des AFT-Bootstrap-Moduls an. • `Branch Name`: Geben Sie den Quell-Repository-Zweig an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• `CodeBuild Docker Image`: Wählen Sie die Datei aus, die als CodeBuild Docker-Basisimage verwendet werden soll.
	
	Schritt 4: Entscheiden Sie sich für die Dateigenerierung
	
	• Der `Generate AFT Files` Parameter steuert, ob standardmäßige AFT-Bereitstellungsdateien generiert werden sollen. Setzen Sie diesen Parameter auf:
	  • `true`um automatisch AFT-Bereitstellungsdateien im angegebenen Repository zu erstellen und zu speichern.
	  • `false`wenn Sie die Dateierstellung manuell durchführen möchten oder die Dateien bereits vorhanden sind.
	
	Wenn Sie ausgewählt haben`false`, fahren Sie mit Schritt 8 fort. Andernfalls führen Sie zuerst die Schritte 5—7 aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Schritt 5: Füllen Sie die AWS Control Tower AFT-Konto informationen aus
	• Eingabe AWS Control Tower - und AFT-Account-spezifische Informationen:
	  • `Log Archive Account ID`: Die ID der Log Archive-Konto-ID in. AWS Control Tower
	  • `Audit Account ID`: Die ID des Audit-Kontos in AWS Control Tower.
	  • `AFT Management Account ID`: Die ID des AFT-Verwaltungskontos, das Sie im ersten Epic erstellt haben.
	  • `AFT Main Region`und`AFT Secondary Region`: Der Haupt- und der Sekundärcode AWS-Regionen für den AFT-Einsatz.
	
	Schritt 6: AFT-Optionen konfigurieren
	• Richten Sie die Berichter stattung über Kennzahlen ein:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `AFT Enable Metrics Reporting` : Aktiviert oder deaktiviert die Berichterstattung über AFT-Metriken. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter Betriebskennzahlen. • Legen Sie die AFT-Funktionsoptionen fest: • `Enable AFT CloudTrail Data Events`: Aktiviert CloudTrail Datenereignisse in allen von AFT verwalteten Konten. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter AWS CloudTrail Datenereignisse. • `Enable AFT Enterprise Support` : Aktivieren Sie Enterprise Support in allen von AFT verwalteten Konten. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter AWS Enterprise Support Plan.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `Enable AFT Delete Default VPC`: Löscht alle VPCs nur im AFT-Verwaltungskonto. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter Löschen der AWS Standard-VPC. Schritt 7: Versionen angeben • `AFT Terraform Version`: Wählen Sie die Version von Terraform aus, die in AFT-Pipelines verwendet werden soll. • `AFT Version`: Definieren Sie die AFT-Version für die Bereitstellung. Behalten Sie die Standardeinstellung (`latest`) bei, um die aktuellste AFT-Version zu verwenden. Schritt 8: Überprüfen und erstellen Sie den Stapel • Überprüfen Sie alle Parameter und Einstellungen. Wenn alles in Ordnung ist, fahren Sie mit der Erstellung des Stacks fort.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schritt 9: Überwachen Sie die Stack-Erstellung • AWS CloudFormation stellt die von Ihnen definierten Ressourcen bereit und konfiguriert sie. Überwache n Sie den Prozess der Stack-Erstellung auf der CloudFormation Konsole. Dieser Vorgang kann mehrere Minuten dauern. Schritt 10: Überprüfen Sie die Bereitstellung • Wenn der Stack-Status CREATE_COMPLETE anzeigt, stellen Sie sicher, dass alle Ressourcen korrekt erstellt wurden. • Notieren Sie sich den Wert im Abschnitt Ausgaben. `TerraformBackendBu cketName`	

Füllen und validieren Sie das AFT-Bootstrap-Repository und die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Füllen Sie das AFT-Bootstrap-Repository auf.	(Optional) Nachdem Sie die CloudFormation Vorlage bereitgestellt haben, können Sie den Inhalt im neu erstellte	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n AFT-Bootstrap-Repository auffüllen oder validieren und testen, ob die Pipeline erfolgreich ausgeführt wurde. Wenn Sie den `Generate AFT Files` Parameter auf setzen`true`, fahren Sie mit dem nächsten Artikel fort (Validierung der Pipeline). Schritt 1: Füllen Sie das Repository aus 1. Öffnen Sie die AWS CodeCommit Konsole und wählen Sie das neu erstellte Repository aus. Wenn Sie den Standardnamen beibehalten haben, wird das Repository aufgerufen`aft-setup` . 2. Klonen Sie das Repositor y mithilfe von SSH, HTTPS oder HTTPS (GRC) auf Ihren lokalen Computer und öffnen Sie es in einem Editor. 3. Erstellen Sie einen Ordner mit dem Namen `terraform` und zwei leere Dateien darin: `backend.tf` und. `main.tf`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Öffnen Sie die `backend.tf` Datei und fügen Sie diesen Codeausschnitt hinzu: `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` In der Datei: • `<aft-main-region>` Durch die AFT-Hauptregion ersetzen. Dies sollte mit der AWS Control Tower Hauptregion übereinstimmen. • `<s3-bucket-name>` Ersetzen Sie es durch den Namen des Terraform-Backend-Buckets. Sie finden dies in der `Terraform BackendBucketName` Ausgabe, die mit der zuvor bereitgestellten CloudFormation Vorlage generiert wurde. 5. Öffnen Sie die `main.tf` Datei und verwenden Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eines der im AFT-Repository verfügbaren Beispiele, um AFT bereitzustellen. Sie können beispielsweise mit Ihrem bevorzugten Anbieter für Versionskontrollsysteme (VCS) (CodeCommit, GitHub, oder Bitbucket) arbeiten oder die AFT-VPC anpassen. Weitere AFT-Eingabeoptionen finden Sie in der README-Datei im AFT-Repository. Schritt 2: Bestätigen Sie Ihre Änderungen und übertragen Sie sie • Nachdem Sie den Ordner und die Dateien erstellt und gefüllt haben, bestätigen Sie Ihre Änderungen und laden Sie den Code in das Repository hoch. Die Pipeline wird automatisch gestartet, durchläuft die Phasen Source und Build und wartet dann vor der Bereitstellungsphase auf eine Genehmigungsaktion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AFT-Bootstrap-Pipeline.	Schritt 1: Sehen Sie sich die Pipeline an • Öffnen Sie die CodePipeline Konsole und überprüfen Sie, ob die `aft-bootstrap-pipeline` Pipeline erfolgreich gestartet wurde. Es sollte einen Terraform -Plan ausführen oder auf eine manuelle Genehmigungsaktion warten. Schritt 2: Genehmigen Sie die Ergebnisse des Terraform-Plans • Sie können die Ergebnisse des Terraform-Plans überprüfen, indem Sie sich die Ausführungsprotokolle der Build-Phase ansehen und dann die Ausführung in der Genehmigungsphase genehmigen oder ablehnen. Wenn Sie zustimmen, beginnt die Pipeline mit der Bereitstellung von AFT-Ressourcen im bereitgestellten AFT-Verwaltungskonto. Schritt 3: Warten Sie auf die Bereitstellung	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Warten Sie, bis die Pipeline erfolgreich ausgeführt wurde. Dies sollte etwa 30 Minuten dauern. Alle Fehler, auf die Sie stoßen könnten, werden häufig durch API-Kontingente verursacht. In diesen Fällen können Sie die Pipeline erneut ausführen, um die Bereitstellung fortzusetzen. Schritt 4: Überprüfen Sie die erstellten Ressourcen • Greifen Sie auf das AFT-Verwaltungskonto zu und vergewissern Sie sich, dass die Ressourcen erstellt wurden.	

Fehlerbehebung

Problem	Lösung
Die in der CloudFormation Vorlage enthaltene benutzerdefinierte Lambda-Funktion schlägt während der Bereitstellung fehl.	Suchen Sie in den CloudWatch Amazon-Protokollen nach der Lambda-Funktion, um den Fehler zu identifizieren. Die Protokolle enthalten detaillierte Informationen und können helfen, das spezifische Problem zu lokalisieren. Vergewissern Sie sich, dass die Lambda-Funktion über die erforderlichen Berechtigungen verfügt und dass die Umgebungsvariablen korrekt festgelegt wurden.

Problem	Lösung
Sie stoßen auf Fehler bei der Erstellung oder Verwaltung von Ressourcen, die auf unzureich ende Berechtigungen zurückzuführen sind.	Überprüfen Sie die IAM-Rollen und -Richtlin ien, die mit der Lambda-Funktion verknüpft sind CodeBuild, und andere an der Bereitstellung beteiligte Dienste. Vergewissern Sie sich, dass sie über die erforderlichen Berechtigungen verfügen. Wenn es Probleme mit den Berechtig ungen gibt, passen Sie die IAM-Richtlinien an, um den erforderlichen Zugriff zu gewähren.
Sie verwenden eine veraltete Version der CloudFormation Vorlage mit neueren AWS-Services oder Terraform-Versionen.	Aktualisieren Sie die CloudFormation Vorlage regelmäßig, damit sie mit den neuesten Versionen AWS und Terraform-Versionen kompatibel ist. In den Versionshinweisen oder der Dokumentation finden Sie alle versionss pezifischen Änderungen oder Anforderungen.
Während der Bereitstellung erreichen Sie die AWS-Service Kontingente.	Bevor Sie die Pipeline bereitstellen, überprüfe n Sie die AWS-Service Kontingente für Ressourcen wie S3-Buckets, IAM-Rollen und Lambda-Funktionen. Die Anfrage wird bei Bedarf erhöht. Weitere Informationen finden Sie auf der AWS Website unter AWS-Service Kontingente.
Aufgrund falscher Eingabeparameter in der CloudFormation Vorlage treten Fehler auf.	Überprüfen Sie alle Eingabeparameter noch einmal auf Tippfehler oder falsche Werte. Vergewissern Sie sich, dass Ressourcen-IDs wie Konto-IDs und Regionsnamen korrekt sind.

Zugehörige Ressourcen

Sehen Sie sich die folgenden Ressourcen an, um dieses Muster erfolgreich zu implementieren. Diese Ressourcen bieten zusätzliche Informationen und Anleitungen, die bei der Einrichtung und Verwaltung von AFT mit Hilfe AWS CloudFormation von unschätzbarem Wert sein können.

AWSDokumentation:

- AWS Control Tower Das Benutzerhandbuch bietet detaillierte Informationen zur Einrichtung und Verwaltung AWS Control Tower.
- AWS CloudFormation Die Dokumentation bietet Einblicke in CloudFormation Vorlagen, Stacks und Ressourcenmanagement.

IAM-Richtlinien und bewährte Verfahren:

- Bewährte Sicherheitsmethoden in IAM erläutern, wie Sie mithilfe von IAM-Rollen und -Richtlinien zur Sicherung von AWS Ressourcen beitragen können.

Terraform auf: AWS

- Die Terraform AWS Provider-Dokumentation enthält umfassende Informationen zur Verwendung von Terraform mit. AWS

AWS-Service Kontingente:

- AWS-Service Kontingente enthält Informationen darüber, wie Sie AWS-Service Kontingente einsehen und Erhöhungen beantragen können.

Verwalten von AWS Service Catalog-Produkten in mehreren AWS-Konten und AWS-Regionen

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Management und Governance; Cloudnativ; Infrastruktur; Modernisierung	Workload: Alle anderen Workloads
AWS-Services: AWS Service Catalog; AWS CloudFormation		

Übersicht

Amazon Web Services (AWS) Service Catalog vereinfacht und beschleunigt die Verwaltung und Verteilung von Infrastructure as Code (IaC)-Vorlagen für Unternehmen. Sie verwenden AWS-CloudFormation Vorlagen, um eine Sammlung von AWS-Ressourcen (Stacks) zu definieren, die für ein Produkt erforderlich sind. AWS CloudFormation StackSets erweitert diese Funktionalität, indem es Ihnen ermöglicht, Stacks in mehreren Konten und AWS-Regionen mit einer einzigen Operation zu erstellen, zu aktualisieren oder zu löschen.

AWS Service Catalog-Administratoren erstellen Produkte mithilfe von CloudFormation Vorlagen, die von Entwicklern erstellt wurden, und veröffentlichen sie. Diese Produkte werden dann einem Portfolio zugeordnet, und es werden Einschränkungen für die Verwaltung angewendet. Um Ihre Produkte Benutzern in anderen AWS-Konten oder Organisationseinheiten (OUs) zur Verfügung zu stellen, geben Sie Ihr Portfolio normalerweise für sie frei. Dieses Muster beschreibt einen alternativen Ansatz für die Verwaltung von AWS Service Catalog-Produktangeboten, die auf AWS basieren CloudFormation StackSets. Anstatt Portfolios gemeinsam zu nutzen, verwenden Sie Stack-Set-Einschränkungen, um AWS-Regionen und -Konten festzulegen, in denen Ihr Produkt bereitgestellt und verwendet werden kann. Mit diesem Ansatz können Sie Ihre AWS Service Catalog-Produkte in mehreren Konten, OUs und AWS-Regionen bereitstellen und von einem zentralen Ort aus verwalten und gleichzeitig Ihre Governance-Anforderungen erfüllen.

Vorteile dieses Ansatzes:

- Das Produkt wird über das primäre Konto bereitgestellt und verwaltet und nicht mit anderen Konten geteilt.
- Dieser Ansatz bietet eine konsolidierte Ansicht aller bereitgestellten Produkte (Stacks), die auf einem bestimmten Produkt basieren.
- Die Konfiguration mit AWS Service Management Connector ist einfacher, da es nur auf ein Konto abzielt.
- Es ist einfacher, Produkte aus AWS Service Catalog abzufragen und zu verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS- CloudFormation Vorlagen für IaC und Versioning
- Einrichtung mehrerer Konten und AWS Service Catalog für die Bereitstellung und Verwaltung von AWS-Ressourcen

Einschränkungen

- Dieser Ansatz verwendet AWS CloudFormation StackSets, und die Einschränkungen von StackSets gelten:
  - StackSets unterstützt keine CloudFormation Vorlagenbereitstellung über Makros. Wenn Sie ein Makro zur Vorverarbeitung der Vorlage verwenden, können Sie keine StackSets-basierte Bereitstellung verwenden.
  - StackSets bietet die Möglichkeit, die Zuordnung eines Stacks zum Stack-Set aufzuheben, sodass Sie einen bestimmten Stack anvisieren können, um ein Problem zu beheben. Ein getrennter Stack kann jedoch nicht erneut mit dem Stack-Set verknüpft werden.
- AWS Service Catalog generiert automatisch StackSet Namen. Die Anpassung wird derzeit nicht unterstützt.

Architektur

Zielarchitektur

1. Der Benutzer erstellt eine AWS- CloudFormation Vorlage zur Bereitstellung von AWS-Ressourcen im JSON- oder YAML-Format.
2. Die CloudFormation Vorlage erstellt ein Produkt in AWS Service Catalog , das einem Portfolio hinzugefügt wird.
3. Der Benutzer erstellt ein bereitgestelltes Produkt, das CloudFormation Stacks in den Zielkonten erstellt.
4. Jeder Stack stellt die in den CloudFormation Vorlagen angegebenen Ressourcen bereit.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Service Catalog hilft Ihnen dabei, Kataloge von IT-Services, die für AWS genehmigt sind, zentral zu verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Polen

Bereitstellen von Produkten über -Konten hinweg

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Portfolio.	Ein Portfolio ist ein Container, der ein oder mehrere Produkte enthält, die auf der Grundlage bestimmter Kriterien gruppiert sind. Die Verwendung eines Portfolios für Ihre Produkte	AWS Service Catalog, IAM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hilft Ihnen dabei, allgemeine Einschränkungen auf Ihr gesamtes Produktset anzuwenden. Um ein Portfolio zu erstellen, folgen Sie den Anweisungen in der AWS Service Catalog-Dokumentation. Wenn Sie die AWS CLI verwenden, finden Sie hier einen Beispielbefehl: `aws servicecatalog create-portfolio --provider-name my-provider --display-name my-portfolio` Weitere Informationen finden Sie in der AWS CLI-Dokumentation.	
Erstellen Sie eine CloudFormation Vorlage.	Erstellen Sie eine CloudFormation Vorlage, die die Ressourcen beschreibt. Ressourceneigenschaftswerte sollten gegebenenfalls parametrisiert werden.	AWS CloudFormation, JSON/YAML

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Produkt mit Versionsinformationen.	Die CloudFormation Vorlage wird zu einem Produkt, wenn Sie sie im AWS Service Catalog veröffentlichen. Geben Sie Werte für die optionalen Versionsdetailparameter an, z. B. Versionstitel und Beschreibung. Dies ist hilfreich, um das Produkt später abzufragen. Um ein Produkt zu erstellen, folgen Sie den Anweisungen in der AWS Service Catalog-Dokumentation. Wenn Sie die AWS CLI verwenden, lautet ein Beispielbefehl: `aws servicecatalog create-product --cli-input-json file://create-product-input.json` wobei die Datei `create-product-input.json` ist, die die Parameter für das Produkt übergibt. Ein Beispiel für diese Datei finden Sie im Abschnitt Zusätzliche Informationen. Weitere Informationen finden Sie in der AWS CLI-Dokumentation.	AWS Service Catalog

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie Einschränkungen an.	Wenden Sie Stack-Set-Einschränkungen auf das Portfolio an, um Produktbereitstellungsoptionen wie mehrere AWS-Konten, Regionen und Berechtigungen zu konfigurieren. Anweisungen finden Sie in der AWS Service Catalog-Dokumentation.	AWS Service Catalog
Fügen Sie -Berechtigungen hinzu.	Erteilen Sie Benutzern Berechtigungen, damit sie die Produkte im Portfolio starten können. Anweisungen zur Konsole finden Sie in der AWS Service Catalog-Dokumentation. Wenn Sie die AWS CLI verwenden, finden Sie hier einen Beispielbefehl: `aws servicecatalog associate-principal-with-portfolio \ --portfolio-id port-2s6abcdefwdh4 \ --principal-arn arn:aws:iam::444455556666:role/Admin \ --principal-type IAM` Weitere Informationen finden Sie in der AWS CLI-Dokumentation.	AWS Service Catalog, IAM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Produkt bereit.	Ein bereitgestelltes Produkt ist eine mit Ressourcen ausgestattete Instance eines Produkts. Durch die Bereitstellung eines Produkts basierend auf einer CloudFormation Vorlage werden ein CloudFormation Stack und die zugrunde liegenden Ressourcen gestartet. Stellen Sie das Produkt bereit, indem Sie auf die entsprechenden AWS-Regionen und -Konten basierend auf Stack-Set-Einschränkungen abzielen. In der AWS CLI finden Sie hier einen Beispielbefehl: `aws servicecatalog provision-product \ --product-id prod-abcdfz3syn2rg \ --provisioning-artifact-id pa-abc347 pcsccfm \ --provisioned-product-name "mytestpp name3"` Weitere Informationen finden Sie in der AWS CLI-Dokumentation.	AWS Service Catalog

Zugehörige Ressourcen

Referenzen

- Übersicht über AWS Service Catalog
- Verwenden von AWS CloudFormation StackSets

Tutorials und Videos

- AWS re:Invent 2019: Alles automatisieren: Optionen und bewährte Methoden (Video)

Zusätzliche Informationen

Wenn Sie den `create-product` Befehl verwenden, verweist der `cli-input-json` Parameter auf eine Datei, die Informationen wie Produkteigentümer, Support-E-Mail und CloudFormation Vorlagendetails angibt. Hier ist ein Beispiel für eine solche Datei:

```
{
   "Owner": "Test admin",
      "SupportDescription": "Testing",
         "Name": "SNS",
            "SupportEmail": "example@example.com",
            "ProductType": "CLOUD_FORMATION_TEMPLATE",
               "AcceptLanguage": "en",
                  "ProvisioningArtifactParameters": {
                     "Description": "SNS product",
                        "DisableTemplateValidation": true,
                           "Info": {
                              "LoadTemplateFromURL": "<url>"
                     },
                           "Name": "version 1"
}
```

Migrieren eines AWS-Mitgliedskontos von AWS Organizations zu AWS Control Tower

Erstellt von Bololfo Jr. Cerrada (AWS)

Umgebung: Produktion	Technologien: Management und Governance; Modernisierung	AWS-Services: AWS Organizations; AWS Control Tower

Übersicht

Dieses Muster beschreibt, wie Sie ein Amazon Web Services (AWS)-Konto von AWS Organizations, bei dem es sich um ein Mitgliedskonto handelt, das durch ein Verwaltungskonto geregelt wird, zu AWS Control Tower migrieren. Durch die Registrierung des Kontos bei AWS Control Tower können Sie präventive und detektivische Leitlinien und Funktionen nutzen, die Ihre Kontoverwaltung optimieren. Möglicherweise möchten Sie auch Ihr Mitgliedskonto migrieren, wenn Ihr AWS Organizations-Verwaltungskonto kompromittiert wurde, und Sie möchten Mitgliedskonten in eine neue Organisation verschieben, die von AWS Control Tower verwaltet wird.

AWS Control Tower bietet ein Framework, das die Funktionen mehrerer anderer AWS-Services, einschließlich AWS Organizations, kombiniert und integriert und eine konsistente Compliance und Governance in Ihrer Umgebung mit mehreren Konten gewährleistet. Mit AWS Control Tower können Sie eine Reihe vorgeschriebener Regeln und Definitionen befolgen, die die Funktionen von AWS Organizations erweitern. Sie können beispielsweise Integritätsschutz verwenden, um sicherzustellen, dass Sicherheitsprotokolle und die erforderlichen kontoübergreifenden Zugriffsberechtigungen erstellt und nicht geändert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Control Tower in Ihrer Zielorganisation in AWS Organizations eingerichtet (Anweisungen finden Sie unter Einrichten in der AWS Control Tower-Dokumentation)
- Administratoranmeldeinformationen für AWS Control Tower (Mitglied der AWSControlTowerAdminsGruppe)

- Administratoranmeldeinformationen für das AWS-Quellkonto

Einschränkungen

- Das Quellverwaltungskonto in AWS Organizations muss sich vom Zielverwaltungskonto in AWS Control Tower unterscheiden.

Produktversionen

- AWS Control Tower Version 2.3 (Februar 2020) oder höher (siehe Versionshinweise)

Architektur

Das folgende Diagramm veranschaulicht den Migrationsprozess und die Referenzarchitektur. Dieses Muster migriert das AWS-Konto von der Quellorganisation zu einer Zielorganisation, die von AWS Control Tower verwaltet wird.

Der Anmeldevorgang besteht aus folgenden Schritten:

1. Das Konto verlässt die Quellorganisation in AWS Organizations .
2. Das Konto wird zu einem eigenständigen Konto. Das bedeutet, dass es keiner Organisation gehört, sodass Governance und Fakturierung unabhängig von Kontoadministratoren verwaltet werden.
3. Die Zielorganisation sendet eine Einladung für das Konto, der Organisation beizutreten.
4. Das eigenständige Konto nimmt die Einladung an und wird Mitglied der Zielorganisation.
5. Das Konto ist bei AWS Control Tower registriert und in eine registrierte Organisationseinheit (OU) verschoben. (Es wird empfohlen, das AWS Control Tower-Dashboard zu überprüfen, um die Registrierung zu bestätigen.) Zu diesem Zeitpunkt werden alle Integritätsschutzmechanismen, die in der registrierten Organisationseinheit aktiviert sind, wirksam.

Tools

AWS-Services

- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer einzigen Entität (einer Organisation) konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Control Tower integriert die Funktionen anderer -Services, einschließlich AWS Organizations, AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) und AWS Service Catalog, um Sie bei der Durchsetzung und Verwaltung von Governance-Regeln für Sicherheit, Betrieb und Compliance in großem Umfang über alle Ihre Organisationen und Konten in der AWS Cloud hinweg zu unterstützen.

Epics

Entfernen des Mitgliedskontos aus der Quellorganisation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass das Mitgliedskonto als eigenständiges Konto ausgeführt werden kann.	Vergewissern Sie sich, dass das Mitgliedskonto, das die Quellorganisation verlassen wird, über die Informationen verfügt, die für den Betrieb als eigenständiges Konto erforderlich sind. Wenn das Mitgliedskonto beispielsweise keine Fakturierungsdaten hat, kann es nicht als eigenständiges Konto betrieben werden, da AWS die Zahlungsinformationen verwendet, um kostenpflichtige AWS-Aktivitäten zu berechnen, die auftreten, während das Konto nicht an eine Organisation angefügt ist. Wenn Sie das Mitgliedskonto mithilfe der AWS Organizations-Konsole, API oder AWS Command Line Interface (CLI)-Befehle erstellt haben,	Kontoadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden die für eigenstän dige Konten erforderlichen Informationen in der Regel nicht automatisch erfasst. Um diese Informationen hinzuzufügen, melden Sie sich beim Konto an und geben Sie einen Support-Plan, Kontaktinformationen und eine Zahlungsweise an. Weitere Informationen darüber, was Sie wissen müssen, bevor Sie ein Konto aus einer Organisation entfernen, finden Sie unter Vor dem Entfernen eines Kontos aus der Organisation in der AWS Organizations-Doku mentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie das Mitglieds konto aus seiner Quellorga nisation.	Folgen Sie den Anweisung en in der AWS Organizat ions-Dokumentation, um ein Mitgliedskonto aus einer Organisation zu entfernen . Sie können sich beim Verwaltungskonto der Organisation anmelden und das Mitgliedskonto entfernen oder sich beim Mitgliedskonto anmelden und die Organisat ion verlassen. Wenn Sie keine Anmeldein formationen auf Administr atorebene haben, um das Konto zu entfernen oder zu verlassen, bitten Sie den Administrator Ihrer Organisat ion um Hilfe. Wenn dem Mitgliedskonto ein Support-Plan, Kontaktin formationen oder Zahlungsi nformationen fehlen, werden Sie aufgefordert, diese Informationen anzugeben und zu überprüfen. Wenn Sie die Organisat ion verlassen, werden Sie zur Seite Erste Schritte der AWS Organizations-Kons ole weitergeleitet, auf der Sie Einladungen für Ihr Konto zum	Administrator des Verwaltun gskontos oder des Kontos

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beitritt zu anderen Organisationen anzeigen können. Wichtig: Zu diesem Zeitpunkt ist Ihr Konto ein eigenständiges Konto. Wenn Sie Workloads ausführen, die nicht durch das kostenlose Kontingent von AWS abgedeckt sind, werden Ihnen die Zahlungs- und Abrechnungsinformationen in Rechnung gestellt, die Sie für das Konto angegeben haben.	
Stellen Sie sicher, dass das Mitgliedskonto nicht mehr Teil der Quellorganisation ist.	In der AWS Organizations-Konsole sollten Sie die Schaltfläche Organisation verlassen nicht mehr sehen. Stattdessen sollten Sie ausstehende Einladungen von anderen Organisationen sehen, falls vorhanden.	Kontoadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die IAM-Rollen, die Zugriff auf Ihr Konto gewähren, aus der Organisation, die Sie verlassen haben.	Wenn Sie das Konto aus der Quellorganisation entfernen, werden von AWS Organizations oder Administratoren erstellte AWS Identity and Access Management (IAM)-Rollen nicht automatisch gelöscht. Um den Zugriff über das Verwaltungskonto der Quellorganisation zu beenden, müssen Sie die IAM-Rollen manuell löschen. Weitere Informationen finden Sie unter Löschen von Rollen oder Instance-Profilen in der IAM-Dokumentation. Wenn ein Mitgliedskonto eine Organisation verlässt, werden alle Tags gelöscht, die dem Konto angefügt wurden. Eigenständige Konten unterstützen keine Tags.	Kontoadministrator

Laden Sie das Konto ein, der neuen Organisation mit AWS Control Tower beizutreten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei AWS Control Tower an.	Melden Sie sich als Administrator bei der AWS Control Tower-Konsole an. Derzeit gibt es keine direkte Möglichkeit, ein AWS-Konto von einer Quellorganisation	AWS Control Tower-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in eine Organisation in einer Organisationseinheit zu verschieben, die von AWS Control Tower verwaltet wird. Sie können jedoch die AWS Control Tower-Governance auf ein vorhandenes AWS-Konto erweitern, wenn Sie es bei einer Organisationseinhe it registrieren, die bereits von AWS Control Tower geregelt wird. Aus diesem Grund müssen Sie sich für diesen Schritt bei AWS Control Tower anmelden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Mitgliedskonto ein.	1. Melden Sie sich bei der AWS Organizations-Konsole an und navigieren Sie zur Seite AWS-Konten. 2. Wählen Sie auf der Seite AWS-Konto hinzufügen die Option Ein vorhandenes AWS-Konto einladen aus. 3. Geben Sie die Kontoinformationen an, einschließlich der 12-stelligen Kontonummer (ohne Bindestriche) sowie der optionalen Beschreibung und Tags, und wählen Sie dann Einladung senden aus. Wichtig: Stellen Sie sicher, dass keine Anwendungen oder Netzwerkkonnektivität von der Kontoübertragung betroffen sind. Diese Aktion sendet eine Einladungs-E-Mail mit einem Link zum Mitgliedskonto. Wenn der Kontoadministrator dem Link folgt und die Einladung annimmt, wird das Mitgliedskonto auf der Seite AWS-Konten angezeigt. Weitere Informationen finden Sie unter Einladen eines AWS-Kontos zu Ihrer	AWS Control Tower-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Organisation in der AWS Organizations-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Anwendungen und Konnektivität.	Wenn das Mitgliedskonto in der neuen Organisation registriert wurde, wird es in der Organisationseinheit innerhalb eines Stammverzeichnisses angezeigt. Sie wird auch in der AWS Control Tower-Konsole angezeigt, die als nicht bei Konten registriert gekennzeichnet ist, da sie noch nicht bei der registrierten Organisationseinheit von AWS Control Tower registriert wurde. Überprüfen Sie Folgendes: • Überprüfen Sie das AWS Control Tower-Dashboard, um festzustellen, ob Verstöße gegen den Integritätsschutz vorliegen. • Überprüfen Sie die Netzwerkkonnektivität (VPN oder AWS Direct Connect), um sicherzustellen, dass sie nicht von der Übertragung betroffen war. • (Anwendungseigentümer) Testen Sie die Anwendungen, die diesem Konto zugeordnet sind, um sicherzustellen, dass sie wie erwartet ausgeführt werden und dass die Abhängigkeiten von der Kontoüber	AWS Control Tower-Administrator, Administrator des Mitgliedskontos, Anwendungseigentümer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tragung nicht betroffen waren.	

Vorbereiten des Kontos für die Registrierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Integritätsschutz und beheben Sie Verstöße.	Überprüfen Sie die Leitlinien, die in der Ziel-OU definiert sind, insbesondere die präventiven Leitlinien, und beheben Sie alle Verstöße. Eine Reihe obligatorischer, präventiver Integritätsschutz ist standardmäßig aktiviert, wenn Sie Ihre Landing Zone von AWS Control Tower einrichten. Diese können nicht deaktiviert werden. Sie müssen diese obligatorischen Leitlinien überprüfen und das Mitgliedskonto korrigieren (manuell oder mithilfe eines Skripts), bevor Sie das Konto registrieren. Hinweis: Präventive Integritätsschutzmaßnahmen halten registrierte Konten von AWS Control Tower konform und verhindern Richtlinienverstöße. Jeder Verstoß gegen präventive Leitlinien kann sich auf die Registrierung	AWS Control Tower-Administrator, Mitgliedskontoadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auswirken. Detektivische Integritätsschutzverstöße werden nach erfolgreicher Registrierung im AWS Control Tower-Dashboard angezeigt , falls sie erkannt werden. Sie wirken sich nicht auf den Registrierungsprozess aus. Weitere Informationen finden Sie unter Guardrails in AWS Control Tower in der AWS-Dokumentation.	
Überprüfen Sie nach der Behebung von Integritä tsschutzverstößen, ob Verbindungsprobleme vorliegen.	In einigen Fällen müssen Sie möglicherweise bestimmte Ports schließen oder Services deaktivieren, um Integritä tsschutzverstöße zu beheben. Stellen Sie sicher, dass Anwendungen, die diese Ports und Services verwenden, korrigiert werden, bevor Sie das Konto registrieren.	Anwendungsbesitzer

Registrieren des Kontos bei AWS Control Tower

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der AWS Control Tower-Konsole an.	Verwenden Sie Anmeldein formationen mit Administr atorberechtigungen für AWS Control Tower. Verwenden Sie nicht die Anmeldein formationen des Root-Benu tzers (Verwaltungskonto), um	AWS Control Tower-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein AWS Organizations-Konto zu registrieren. Dadurch wird eine Fehlermeldung angezeigt .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie das Konto.	1. Wählen Sie auf der Seite Account Factory in AWS Control Tower Konto registrieren aus. 2. Geben Sie die Details ein, einschließlich der E-Mail-Adresse, die dem Konto zugeordnet ist, das Sie registrieren möchten, des Anzeigenamens, der in AWS Control Tower angezeigt wird, der E-Mail-Adresse des IAM Identity Center, des Vor- und Nachnamens des Kontoinhabers und der Organisationseinheit, in der Sie das Konto registrieren möchten. Die E-Mail-Adresse des IAM Identity Center ist Ihre bevorzugte Benutzer-E-Mail-Adresse. Sie können dieselbe E-Mail-Adresse wie die Konto-E-Mail verwenden. 3. Wählen Sie Enroll account (Konto anmelden). Weitere Informationen finden Sie unter Registrieren eines vorhandenen Kontos in der AWS Control Tower-Dokumentation.	AWS Control Tower-Administrator

Überprüfen des Kontos nach der Registrierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das Konto.	Wählen Sie in AWS Control Tower Konten aus. Das soeben registrierte Konto hat den anfänglichen Status Registrieren. Wenn die Registrierung abgeschlossen ist, ändert sich ihr Status in Registriert.	AWS Control Tower-Administrator, Mitgliedskontoadministrator
Überprüfen Sie, ob die Integritätsschutzrichtlinie verletzt wurde.	In der Organisationseinheit definierte Guardrails gelten automatisch für das registrierte Mitgliedskonto. Überwachen Sie das AWS Control Tower-Dashboard auf Verstöße und beheben Sie sie entsprechend. Weitere Informationen finden Sie unter Guardrails in AWS Control Tower in der AWS-Dokumentation.	AWS Control Tower-Administrator, Mitgliedskontoadministrator

Fehlerbehebung

Problem	Lösung
Sie erhalten die Fehlermeldung: Ein unbekannter Fehler ist aufgetreten. Versuchen Sie es später erneut oder wenden Sie sich an den AWS Support.	Dieser Fehler tritt auf, wenn Sie Root-Benutzer-Anmeldeinformationen (Verwaltungskonto) in AWS Control Tower verwenden, um ein neues Konto zu registrieren. AWS Service Catalog kann das Account Factory-Portfolio oder -Produkt nicht dem Root-Benutzer zuordnen, was zu der Fehlermeldung führt. Um diesen

Problem	Lösung
	Fehler zu beheben, verwenden Sie Anmeldeinformationen für Nicht-Root-Benutzer (Administrator), um das neue Konto zu registrieren. Weitere Informationen zum Zuweisen von administrativem Zugriff zu einem Administratorbenutzer finden Sie unter Erste Schritte in der AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Dokumentation.
Auf der Seite AWS Control Tower-Aktivitäten wird die Aktion Katastrophale Abweichung abrufen angezeigt.	Diese Aktion spiegelt eine Abweichungsprüfung des Services wider und weist nicht auf Probleme mit der AWS Control Tower-Einrichtung hin. Es ist keine Aktion erforderlich.

Zugehörige Ressourcen

Dokumentation

- Terminologie und Konzepte von AWS Organizations (Dokumentation von AWS Organizations)
- Was ist AWS Control Tower? (Dokumentation zu AWS Control Tower)
- Entfernen eines Mitgliedskontos aus Ihrer Organisation (Dokumentation zu AWS Organizations)
- Erstellen eines Administratorkontos in AWS Control Tower (Dokumentation zu AWS Control Tower)

Tutorials und Videos

- AWS Control Tower-Workshop (Workshop im Selbststudium)
- Was ist AWS Control Tower? (Video)
- Bereitstellen von Benutzern in AWS Control Tower (Video)
- Aktivieren von AWS Control Tower für bestehende Organisationen (Video)

Überwachen der Verwendung eines freigegebenen Amazon Machine Image über mehrere AWS-Konten hinweg

Erstellt von Naveen Suthar (AWS) und Sandeep Gawande (AWS)

Code-Repository: cross-account-ami-auditing-terraform-samples	Umgebung: PoC oder Pilotprojekt	Technologien: Management und Governance DevOps; Serverless; Betrieb
AWS-Services: Amazon DynamoDB ;AWS Lambda; Amazon EventBridge		

Übersicht

Amazon Machine Images (AMIs)werden verwendet, um Amazon Elastic Compute Cloud (Amazon EC2)-Instances in Ihrer Amazon Web Services (AWS)-Umgebung zu erstellen. Sie können AMIs in einem separaten, zentralisierten AWS-Konto erstellen, das in diesem Muster als Erstellerkonto bezeichnet wird. Anschließend können Sie das AMI für mehrere AWS-Konten freigeben, die sich in derselben AWS-Region befinden, die in diesem Muster als Konsumentenkonten bezeichnet werden. Die Verwaltung von AMIs von einem einzigen Konto aus bietet Skalierbarkeit und vereinfacht die Verwaltung. In den Konsumentenkonten können Sie auf das freigegebene AMI in Amazon EC2 Auto Scaling-Startvorlagen und Amazon Elastic Kubernetes Service (Amazon EKS)-Knotengruppen verweisen.

Wenn ein freigegebenes AMI veraltet ist, abgemeldet ist oder nicht freigegeben ist, können AWS-Services, die auf das AMI in den Konsumentenkonten verweisen, dieses AMI nicht verwenden, um neue Instances zu starten. Jedes Auto-Scaling-Ereignis oder jeder Neustart derselben Instance schlägt fehl. Dies kann zu Problemen in der Produktionsumgebung führen, z. B. zu Ausfallzeiten von Anwendungen oder Leistungseinbußen. Wenn AMI-Freigabe- und -Nutzungsereignisse in mehreren AWS-Konten auftreten, kann es schwierig sein, diese Aktivität zu überwachen.

Dieses Muster hilft Ihnen dabei, die gemeinsame AMI-Nutzung und den Status für alle Konten in derselben Region zu überwachen. Es verwendet Serverless-AWS-Services wie Amazon EventBridge, Amazon DynamoDB , AWS Lambda und Amazon Simple Email Service (Amazon SES). Sie stellen die Infrastruktur als Code (IaC) mithilfe von HashiCorp Terraform bereit. Diese Lösung

bietet Warnungen, wenn ein Service in einem Konsumentenkonto auf ein abgemeldetes oder nicht freigegebenes AMI verweist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei oder mehrere aktive AWS-Konten: ein Erstellerkonto und ein oder mehrere Verbraucherkonten
- Ein oder mehrere AMIs, die vom Erstellerkonto für ein Verbraucherkonto freigegeben werden
- Terraform-CLI, installiert (Terraform-Dokumentation)
- Terraform-AWS-Anbieter, konfiguriert (Terraform-Dokumentation)
- (Optional, aber empfohlen) Terraform-Backend, konfiguriert (Terraform-Dokumentation)
- Git, installiert

Einschränkungen

- Dieses Muster überwacht AMIs, die für bestimmte Konten freigegeben wurden, mithilfe der Konto-ID. Dieses Muster überwacht keine AMIs, die mithilfe der Organisations-ID für eine Organisation freigegeben wurden.
- AMIs können nur für Konten innerhalb derselben AWS-Region freigegeben werden. Dieses Muster überwacht AMIs innerhalb einer einzelnen Zielregion. Um die Verwendung von AMIs in mehreren Regionen zu überwachen, stellen Sie diese Lösung in jeder Region bereit.
- Dieses Muster überwacht keine AMIs, die vor der Bereitstellung dieser Lösung gemeinsam genutzt wurden. Wenn Sie zuvor freigegebene AMIs überwachen möchten, können Sie die Freigabe des AMI aufheben und es dann erneut mit den Konsumentenkonten teilen.

Produktversionen

- Terraform Version 1.2.0 oder höher
- Terraform AWS Provider Version 4.20 oder höher

Architektur

Zieltechnologie-Stack

Die folgenden Ressourcen werden als IaC über Terraform bereitgestellt:

- Amazon-DynamoDB-Tabellen
- Amazon- EventBridge Regeln
- AWS Identity and Access Management (IAM)-Rolle
- Funktionen von AWS Lambda
- Amazon SES

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Ein AMI im Erstellerkonto wird für ein Konsumentenkonto in derselben AWS-Region freigegeben.
2. Wenn das AMI freigegeben wird, erfasst eine Amazon- EventBridge Regel im Erstellerkonto das `ModifyImageAttribute` Ereignis und initiiert eine Lambda-Funktion im Erstellerkonto.
3. Die Lambda-Funktion speichert Daten im Zusammenhang mit dem AMI in einer DynamoDB-Tabelle im Erstellerkonto.
4. Wenn ein AWS-Service im Konsumentenkonto das freigegebene AMI verwendet, um eine Amazon EC2-Instance zu starten, oder wenn das freigegebene AMI einer Startvorlage zugeordnet ist, erfasst eine - EventBridge Regel im Konsumentenkonto die Verwendung des freigegebenen AMI.
5. Die EventBridge Regel initiiert eine Lambda-Funktion im Konsumentenkonto. Die Lambda-Funktion bewirkt Folgendes:
   a. Die Lambda-Funktion aktualisiert die AMI-bezogenen Daten in einer DynamoDB-Tabelle im Konsumentenkonto.
   b. Die Lambda-Funktion übernimmt eine IAM-Rolle im Erstellerkonto und aktualisiert die DynamoDB-Tabelle im Erstellerkonto. In der `Mapping` Tabelle wird ein Element erstellt, das die Instance-ID oder Startvorlagen-ID der jeweiligen AMI-ID zuordnet.
6. Das AMI, das im Erstellerkonto zentral verwaltet wird, ist veraltet, wird abgemeldet oder die Freigabe wird aufgehoben.
7. Die EventBridge Regel im Erstellerkonto erfasst das `DeregisterImage` Ereignis `ModifyImageAttribute` oder mit der `remove` Aktion und initiiert die Lambda-Funktion.

8. Die Lambda-Funktion überprüft die DynamoDB-Tabelle, um festzustellen, ob das AMI in einem der Konsumentenkonten verwendet wird. Wenn dem AMI in der `Mapping` Tabelle keine Instance-IDs oder Startvorlagen-IDs zugeordnet sind, ist der Vorgang abgeschlossen.
9. Wenn Instance-IDs oder Startvorlagen-IDs mit dem AMI in der `Mapping` Tabelle verknüpft sind, verwendet die Lambda-Funktion Amazon SES, um eine E-Mail-Benachrichtigung an die konfigurierten Abonnenten zu senden.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Email Service (Amazon SES) hilft Ihnen, E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domänen zu senden und zu empfangen.

Andere Tools

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit dem Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.
- Python ist eine universelle Computer-Programmiersprache.

Code-Repository

Der Code für dieses Muster ist im GitHub cross-account-ami-monitoring-terraform-samples-Repository verfügbar.

Bewährte Methoden

- Folgen Sie den bewährten Methoden für die Arbeit mit AWS Lambda-Funktionen .
- Folgen Sie den bewährten Methoden für die Erstellung von AMIs.
- Befolgen Sie beim Erstellen der IAM-Rolle das Prinzip der geringsten Berechtigung und gewähren Sie die Mindestberechtigungen, die zum Ausführen einer Aufgabe erforderlich sind. Weitere Informationen finden Sie unter Gewähren von geringsten Berechtigungen und Bewährte Methoden für die Sicherheit in der IAM-Dokumentation.
- Richten Sie Überwachung und Warnungen für die AWS Lambda-Funktionen ein. Weitere Informationen finden Sie unter Überwachung und Fehlerbehebung bei Lambda-Funktionen.

Sekunden

Anpassen der Terraform-Konfigurationsdateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die benannten AWS CLI-Profile.	Erstellen Sie für das Ersteller konto und jedes Konsument enkonto ein AWS Command Line Interface (AWS CLI)-benanntes Profil. Anweisung en finden Sie unter Einrichten der AWS CLI im AWS Getting Started Resources Center.	DevOps Techniker
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein. Dadurch wird das cross-account-ami-monitorin g-terraform-samples-Reposito ry mithilfe von GitHub SSH geklont. `git clone git@githu b.com:aws-samples/ cross-account-ami-`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`monitoring-terraform-samples.git`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Datei provider.tf.	1. Geben Sie den folgenden Befehl ein, um in den `terraform` Ordner im geklonten Repository zu navigieren. `cd cross-account-ami-monitoring/terraform` 2. Öffnen Sie die `provider.tf` Datei. 3. Aktualisieren Sie die Terraform-AWS-Provider-Konfigurationen für das Erstellerkonto und das Verbraucherkonto wie folgt: • `alias`Geben Sie für einen Namen für die Anbieterkonfiguration ein. • Geben Sie für die AWS-Zielregion ein`region`, in der Sie diese Lösung bereitstellen möchten. • Geben Sie für das `profile`benannte AWS CLI-Profil für den Zugriff auf das Konto ein. 4. Wenn Sie mehr als ein Konsumentenkonto konfigurieren, erstellen Sie ein Profil für jedes zusätzliche Konsumentenkonto.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Speichern und schließen Sie die Datei `provider.tf` . Weitere Informationen zur Konfiguration der Anbieter finden Sie unter Konfigurationen mehrerer Anbieter in der Terraform-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Datei terraform.tfvars.	1. Öffnen Sie die `terraform.tfvars` Datei. 2. Konfigurieren Sie im `account_email_mapping` Parameter wie folgt Warnungen für das Ersteller konto und das Verbrauch erkonto: • `account`Geben Sie für die Konto-ID ein. • Geben Sie für die E-Mail-Adresse ein`email`, an die Sie Warnungen senden möchten. Sie können für jedes Konto nur eine E-Mail-Adresse eingeben. 3. Wenn Sie mehr als ein Konsumentenkonto konfigurieren, geben Sie ein Konto und eine E-Mail-Adresse für jedes zusätzliche Konsumentenkonto ein. 4. Speichern und schließen Sie die Datei `terraform.tfvars` .	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Datei main.tf.	Führen Sie diese Schritte nur aus, wenn Sie diese Lösung für mehr als ein Konsument enkonto bereitstellen. Wenn Sie diese Lösung nur für ein Konsumentenkonto bereitste llen, ist keine Änderung dieser Datei erforderlich. 1. Öffnen Sie die `main.tf` Datei. 2. Erstellen Sie für jedes zusätzliche Verbrauch erkonto ein neues Modul, das auf dem `consumer_account_A` Modul in der Vorlage basiert. Für jedes Konsumentenkonto sollte der Wert für mit dem Alias übereinstimmen`provider`, den Sie in die `provider.tf` Datei eingegeben haben. 3. Speichern und schließen Sie die Datei `main.tf`.	DevOps Techniker

Bereitstellen der Lösung mithilfe von Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	Geben Sie in der Terraform-CLI die folgenden Befehle ein, um die AWS-Ressourcen in	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den Ersteller- und Verbrauch erkonten bereitzustellen:
	1. Geben Sie den folgenden Befehl ein, um Terraform zu initialisieren.
	`terraform init`
	2. Geben Sie den folgenden Befehl ein, um die Terraform-Konfigurationen zu validieren.
	`terraform validate`
	3. Geben Sie den folgenden Befehl ein, um einen Terraform-Ausführungsplan zu erstellen.
	`terraform plan`
	4. Überprüfen Sie die Konfigurationsänderungen im Terraform-Plan und bestätigen Sie, dass Sie diese Änderungen implementieren möchten.
	5. Geben Sie den folgenden Befehl ein, um die Ressourcen bereitzustellen.
	`terraform apply`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Identität der E-Mail-Adresse.	Als Sie den Terraform-Plan bereitgestellt haben, hat Terraform eine E-Mail-Adressidentität für jedes Konsumentenkonto in Amazon SES erstellt. Bevor Benachrichtigungen an diese E-Mail-Adresse gesendet werden können, müssen Sie die E-Mail-Adresse verifizieren. Anweisungen finden Sie unter Verifizieren einer E-Mail-Adressenidentität in der Amazon SESDokumentation.	Allgemeines AWS

Validieren der Ressourcenbereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung im Erstellerkonto.	1. Melden Sie sich beim Erstellerkonto an. 2. Vergewissern Sie sich in der Navigationsleiste, dass die Zielregion angezeigt wird. Wenn Sie sich in einer anderen Region befinden, wählen Sie den Namen der aktuell angezeigten Region und dann die Zielregion aus. 3. Öffnen Sie die DynamoDB-Konsole unter https://console.aws.amazon.com/dynamodb/.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Navigationsbereich Tables (Tabellen) aus. 5. Überprüfen Sie in der Tabellenliste, ob die `AmiShare` Tabelle vorhanden ist. 6. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda. 7. Wählen Sie im Navigationsbereich Funktionen aus. 8. Überprüfen Sie in der Liste der Funktionen, ob die `ami-share` Funktion vorhanden ist. 9. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iamv2/. 10. Wählen Sie im Navigationsbereich Rollen aus. 11. Überprüfen Sie in der Rollenliste, ob die `external-ddb-role` Rolle vorhanden ist. 12. Öffnen Sie die - EventBridge Konsole unter https://console.aws.amazon.com/events/. 13. Wählen Sie im Navigationsbereich Regeln aus. 14. Überprüfen Sie in der Liste der Regeln, ob die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`modify_image_attribute_event` Regel vorhanden ist. 15. Öffnen Sie die Amazon SES-Konsole unter https://console.aws.amazon.com/ses/. 16. Wählen Sie im Navigationsbereich Verifizierte Identitäten aus. 17. Überprüfen Sie in der Liste der Identitäten, ob für jedes Konsumentenkonto eine E-Mail-Adressenidentität registriert und verifiziert wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung im Konsumentenkonto.	1. Melden Sie sich beim Konsumentenkonto an. 2. Vergewissern Sie sich in der Navigationsleiste, dass die Zielregion angezeigt wird. Wenn Sie sich in einer anderen Region befinden, wählen Sie den Namen der aktuell angezeigten Region und dann die Zielregion aus. 3. Öffnen Sie die DynamoDB-Konsole unter https://console.aws.amazon.com/dynamodb/. 4. Wählen Sie im Navigationsbereich Tables (Tabellen) aus. 5. Überprüfen Sie in der Tabellenliste, ob die `Mapping` Tabelle vorhanden ist. 6. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda. 7. Wählen Sie im Navigationsbereich Funktionen aus. 8. Überprüfen Sie in der Liste der Funktionen, ob die `ami-deregister-function` Funktionen `ami-usage-function` und vorhanden sind.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Öffnen Sie die - EventBridge Konsole unter https://console.aws.amazon.com/events/. 10. Wählen Sie im Navigationsbereich Regeln aus. 11. Überprüfen Sie in der Liste der Regeln, ob die `ami_deregister_events` Regeln `ami_usage_events` und vorhanden sind.	

Validieren der Überwachung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AMI im Erstellerkonto.	1. Erstellen Sie im Ersteller konto ein privates AMI. Anweisungen finden Sie unter Erstellen eines AMI aus einer Amazon EC2-Instance. 2. Teilen Sie das neue AMI mit einem der Konsument enkonten. Anweisungen finden Sie unter Freigeben eines AMI für bestimmte AWS-Konten.	DevOps Techniker
Verwenden Sie das AMI im Konsumentenkonto.	Verwenden Sie im Konsument enkonto das freigegebene AMI, um eine EC2-Instance oder Startvorlage zu erstellen	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	. Anweisungen finden Sie unter Wie starte ich eine EC2-Instance von einem benutzerdefinierten AMI (AWS re:Post Knowledge Center) oder So erstellen Sie eine Startvorlage (Dokumentation zu Amazon EC2 Auto Scaling).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Überwachung und Warnungen.	1. Melden Sie sich beim Erstellerkonto an. 2. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. 3. Wählen Sie im Navigationsbereich die Option AMIs. 4. Wählen Sie das AMI in der Liste und dann Aktionen, AMI-Berechtigungen bearbeiten aus. 5. Wählen Sie im Abschnitt Freigegebene Konten das Konsumentenkonto aus und wählen Sie dann Ausgewählte entfernen aus. 6. Wählen Sie Änderungen speichern aus. 7. Überprüfen Sie, ob die Ziel-E-Mail-Adresse, die Sie für das Konsumentenkonto definiert haben, eine Benachrichtigung erhält, dass die Freigabe für das AMI abgebrochen wurde.	DevOps Techniker

(Optional) Beenden der Überwachung freigegebener AMIs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Ressourcen.	1. Geben Sie den folgenden Befehl ein, um die durch dieses Muster bereitgestellten Ressourcen zu entfernen und die Überwachung freigegebener AMIs zu beenden. `terraform destroy` 2. Bestätigen Sie den `destroy` Befehl, indem Sie eingeben `yes`.	DevOps Techniker

Fehlerbehebung

Problem	Lösung
Ich habe keine E-Mail-Warnung erhalten.	Es kann mehrere Gründe geben, warum die Amazon SES-E-Mail nicht gesendet wurde. Überprüfen Sie, ob Folgendes der Fall ist: 1. Verwenden Sie im Abschnitt Clarics das Epic Validate resource deployment, um zu bestätigen, dass die Infrastruktur in allen AWS-Konten ordnungsgemäß bereitgestellt wurde. 2. Validieren Sie die Lambda-Funktionsereignisse in Amazon CloudWatch Logs. Anweisungen finden Sie unter Verwenden der CloudWatch Konsole in der Lambda-Dokumentation. Vergewissern Sie sich, dass es

Problem	Lösung
	keine Berechtigungsprobleme gibt, z. B. eine explizite Zugriffsverweigerung in identitätsbasierten oder ressourcenbasierten Richtlinien. Weitere Informationen finden Sie unter Logik zur Richtlinienbewertung in der IAM-Dokumentation. 3. Überprüfen Sie in Amazon SES, ob der Status der E-Mail-Adressenidentität Verifiziert lautet. Weitere Informationen finden Sie unter Verifizieren einer E-Mail-Adressenidentität.

Zugehörige Ressourcen

AWS-Dokumentation

- Erstellen von Lambda-Funktionen mit Python (Lambda-Dokumentation)
- Erstellen eines AMI (Amazon EC2-Dokumentation)
- Freigeben eines AMI für bestimmte AWS-Konten (Amazon EC2-Dokumentation)
- Abmelden Ihres AMI (Amazon EC2Dokumentation)

Terraform-Dokumentation

- Installieren von Terraform
- Terraform-Backend-Konfiguration
- Terraform-AWS-Anbieter
- Terraform-Binär-Download

Einrichten von Warnungen für programmgesteuerte Kontoschließungen in AWS Organizations

Erstellt von Richard Milner-Watts (AWS), Debojit Bhadra (AWS) und Manav Yadav (AWS)

Code-Repository: AWS Account microSD Notifier	Umgebung: Produktion	Technologien: Management und Governance
AWS-Services: AWS CloudTrail; Amazon EventBridge; AWS Lambda ; AWS Organizations ; Amazon SNS		

Übersicht

Mit der CloseAccount API für AWS Organizations können Sie Mitgliedskonten innerhalb einer Organisation programmgesteuert schließen, ohne sich mit Root-Anmeldeinformationen beim Konto anmelden zu müssen. Die RemoveAccountFromOrganization API ruft ein Konto aus einer Organisation in AWS Organizations ab, sodass es zu einem eigenständigen Konto wird.

Diese APIs erhöhen möglicherweise die Anzahl der Operatoren, die ein AWS-Konto schließen oder entfernen können. Alle Benutzer, die über AWS Identity and Access Management (IAM) im AWS Organizations-Verwaltungskonto Zugriff auf die Organisation haben, können diese APIs aufrufen, sodass der Zugriff nicht auf den Besitzer der Stamm-E-Mail des Kontos mit einem zugehörigen Multi-Faktor-Authentifizierung (MFA)-Gerät beschränkt ist.

Dieses Muster implementiert Warnungen beim Aufrufen der `RemoveAccountFromOrganization` APIs `CloseAccount` und , sodass Sie diese Aktivitäten überwachen können. Für Warnungen verwendet es ein Amazon Simple Notification Service (Amazon SNS)-Thema. Sie können Slack-Benachrichtigungen auch über einen Webhook einrichten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Eine Organisation in AWS Organizations
- Zugriff auf das Organisationsverwaltungskonto unter dem Stammverzeichnis der Organisation, um die erforderlichen Ressourcen zu erstellen

Einschränkungen

- Wie in der AWS Organizations-API-Referenz beschrieben, ermöglicht die `CloseAccount` API, dass nur 10 Prozent der aktiven Mitgliedskonten innerhalb eines fortlaufenden Zeitraums von 30 Tagen geschlossen werden.
- Wenn ein AWS-Konto geschlossen wird, wird sein Status in SUSPENDED geändert. Für 90 Tage nach diesem Statusübergang kann der AWS Support das Konto wieder eröffnen. Nach 90 Tagen wird das Konto dauerhaft gelöscht.
- Benutzer, die Zugriff auf das AWS Organizations-Verwaltungskonto und die APIs haben, verfügen möglicherweise auch über Berechtigungen zum Deaktivieren dieser Warnungen. Wenn das Hauptproblem böswilliges Verhalten statt versehentliches Löschen ist, sollten Sie die durch dieses Muster erstellten Ressourcen mit einer IAM-Berechtigungsgrenze schützen.
- Die API ruft `CloseAccount` und auf, die in der Region USA Ost (Nord-Virginia) () verarbeitet `RemoveAccountFromOrganization` werden`us-east-1`. Daher müssen Sie diese Lösung in bereitstellen`us-east-1`, um die Ereignisse zu beobachten.

Architektur

Zieltechnologie-Stack

- AWS Organizations
- AWS CloudTrail
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Zielarchitektur

Das folgende Diagramm zeigt die Lösungsarchitektur für dieses Muster.

1. AWS Organizations verarbeitet eine - `CloseAccount` oder `-RemoveAccountFromOrganization`Anforderung.
2. Amazon EventBridge ist in AWS integriert CloudTrail , um diese Ereignisse an den Standard-Event-Bus zu übermitteln.
3. Eine benutzerdefinierte Amazon- EventBridge Regel entspricht den AWS Organizations-Anforderungen und -Aufrufen einer AWS Lambda-Funktion.
4. Die Lambda-Funktion übermittelt eine Nachricht an ein SNS-Thema, das Benutzer für E-Mail-Warnungen oder Weiterverarbeitung abonnieren können.
5. Wenn Slack-Benachrichtigungen aktiviert sind, übermittelt die Lambda-Funktion eine Nachricht an einen Slack-Webhook.

Tools

AWS-Services

- AWS CloudFormation bietet eine Möglichkeit, eine Sammlung verwandter AWS- und Drittanbieterressourcen zu modellieren, sie schnell und konsistent bereitzustellen und während ihres gesamten Lebenszyklus zu verwalten, indem Infrastruktur als Code behandelt wird.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge empfängt ein Ereignis, einen Indikator für eine Änderung der Umgebung, und wendet eine Regel an, um das Ereignis an ein Ziel weiterzuleiten. Regeln ordnen Ereignisse Zielen zu, die entweder auf der Struktur des Ereignisses, einem so genannten Ereignismuster, oder nach einem Zeitplan basieren.
- AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch, von einigen Anfragen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die tatsächlich konsumierte Zeit. Es werden keine Gebühren berechnet, solange Ihr Code nicht ausgeführt wird.
- AWS Organizations unterstützt Sie bei der zentralen Verwaltung und Steuerung Ihrer Umgebung, wenn Sie Ihre AWS-Ressourcen vergrößern und skalieren. Mit AWS Organizations können Sie programmgesteuert neue AWS-Konten erstellen und Ressourcen zuweisen, Konten gruppieren, um Ihre Workflows zu organisieren, Richtlinien für die Verwaltung auf Konten oder Gruppen anwenden und die Abrechnung vereinfachen, indem Sie eine einzige Zahlungsweise für alle Ihre Konten verwenden.

- AWS CloudTrail überwacht und zeichnet Kontoaktivitäten in Ihrer gesamten AWS-Infrastruktur auf und gibt Ihnen die Kontrolle über Speicher-, Analyse- und Abhilfemaßnahmen.
- Amazon Simple Notification Service (Amazon SNS) ist ein vollständig verwalteter Messaging-Service für die Kommunikation application-to-application (A2A) und application-to-person (A2P).

Andere Tools

- Die AWS Lambda Powertools for Python-Bibliothek besteht aus einer Reihe von Dienstprogrammen, die Funktionen zur Nachverfolgung, Protokollierung, Metriken und Ereignisbehandlung für Lambda-Funktionen bereitstellen.

Code

Der Code für dieses Muster befindet sich im GitHub AWS Account Closer Notifier-Repository.

Die Lösung enthält eine CloudFormation Vorlage, die die Architektur für dieses Muster bereitstellt. Es verwendet die AWS Lambda Powertools for Python-Bibliothek, um Protokollierung und Nachverfolgung bereitzustellen.

Sekunden

Bereitstellen der Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für den Lösungs-Stack.	Die CloudFormation Vorlage für dieses Muster befindet sich im Hauptzweig des GitHub Repositorys . Es stellt die IAM-Rollen, - EventBridge Regeln, Lambda-Funktionen und das SNS-Thema bereit. So starten Sie die Vorlage: 1. Klonen Sie das GitHub Repository, um eine Kopie	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Lösungscodes zu erhalten. 2. Öffnen Sie die AWS-Management konsole für das AWS Organizations-Verwaltungskonto. 3. Wählen Sie die Region USA Ost (Nord-Virginia) (`us-east-1`) und öffnen Sie dann die CloudFormation - Konsole . 4. Erstellen Sie den Stack, indem Sie die `account-closure-notifier.yml` Vorlage verwenden und die folgenden Werte angeben: • Stackname: `aws-account-closure-notifier-stack` • `ResourcePrefix` -Parameter: `aws-account-closure-notifier` • `SlackNotification` Parameter: Wenn Slack-Benachrichtigungen erforderlich sind, ändern Sie diese Einstellung in `true`. • `SlackWebhookEndpoint` Parameter: Wenn Slack-Benachrichti	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gungen erforderlich sind, geben Sie die Webhook-URL an. Weitere Informationen zum Starten eines CloudFormation Stacks finden Sie in der AWS-Dokumentation.	
Stellen Sie sicher, dass die Lösung erfolgreich gestartet wurde.	1. Warten Sie, bis der CloudFormation Stack den Status CREATE_COMPLETE erreicht hat. 2. Öffnen Sie die -EventBridge Konsole in `us-east-1` . 3. Stellen Sie sicher, dass eine neue Regel mit dem Namen erstellt wurde`aws-account-closure-notifier-event-rule` .	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das SNS-Thema.	(Optional) Wenn Sie das SNS-Thema abonnieren möchten: 1. Öffnen Sie die Amazon SNS-Konsole in `us-east-1` und suchen Sie das Thema mit dem Namen `aws-account-closure-notifier-sns-topic` . 2. Wählen Sie den Themennamen und dann Abonnement erstellen aus. 3. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. 4. Geben Sie für Endpunkt die E-Mail-Adresse an, die die Benachrichtigung erhalten soll, und wählen Sie dann Abonnement erstellen aus. 5. Überprüfen Sie Ihren E-Mail-Posteingang auf eine Nachricht von AWS Notifications. Verwenden Sie den Link in dieser E-Mail, um das Abonnement zu bestätigen. Weitere Informationen zum Einrichten von SNS-Benachrichtigungen finden Sie in der Amazon SNS-Dokumentation.	AWS-Administrator

Überprüfen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie ein Testereignis an den Standard-Event-Bus.	Das GitHub Repository enthält ein Beispielereignis, das Sie zum Testen an den EventBridge Standard-Event Bus senden können. Die EventBridge Regel reagiert auch auf Ereignisse, die die benutzerdefinierte Ereignisquelle verwenden `account.closure.notifier` . Hinweis: Sie können die CloudTrail Ereignisquelle nicht verwenden, um dieses Ereignis zu senden, da es nicht möglich ist, ein Ereignis als AWS-Service zu senden. So senden Sie ein Testereignis: 1. Öffnen Sie die -EventBridge Konsole in `us-east-1` . 2. Wählen Sie im Navigationsbereich unter Buses die Option Event Buses und dann den Standard-Event Bus aus. 3. Wählen Sie Ereignisse senden aus. 4. Geben Sie für Ereignisquelle ein `account.closure.notifier` .	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Geben Sie für Detailtyp `AWS API Call via CloudTrail` ein. 6. Kopieren Sie für Ereignisdetails den Inhalt von `tests/dummy-event.json` aus dem GitHub Repository in das Textfeld. 7. Wählen Sie Senden, um den Benachrichtigungsworkflow zu initiieren.	
Stellen Sie sicher, dass die E-Mail-Benachrichtigung empfangen wurde.	Überprüfen Sie das Postfach, das das SNS-Thema abonniert hat, auf Benachrichtigungen. Sie sollten eine E-Mail mit Details zum Konto erhalten, das geschlossen wurde, und zum Prinzipal, der den API-Aufruf ausgeführt hat.	AWS-Administrator
Überprüfen Sie, ob die Slack-Benachrichtigung empfangen wurde.	(Optional) Wenn Sie bei der Bereitstellung der CloudFormation Vorlage eine Webhook-URL für den `SlackWebhookEndpoint` Parameter angegeben haben, überprüfen Sie den Slack-Kanal, der dem Webhook zugeordnet ist. Es sollte eine Nachricht mit Details zum Konto, das geschlossen wurde, und zum Prinzipal, der den API-Aufruf ausgeführt hat, angezeigt werden.	AWS-Administrator

Zugehörige Ressourcen

- CloseAccount Aktion (API-Referenz für AWS Organizations)
- RemoveAccountFromOrganization Aktion (API-Referenz für AWS Organizations)
- AWS Lambda Powertools für Python

Mehr Muster

- Automatisieren der AWS-Ressourcenbewertung
- Automatisieren der Portfolio- und Produktbereitstellung von AWS Service Catalog mithilfe von AWS CDK
- Automatisches Anfügen einer von AWS verwalteten Richtlinie für Systems Manager an EC2-Instance-Profile mithilfe von Cloud Custodian und AWS CDK
- Automatisches Verschlüsseln vorhandener und neuer Amazon-EBS-Volumes
- Zentralisierte Protokollierung und Sicherheitsleitplanken für mehrere Konten
- EC2-Instances beim Start auf obligatorische Tags überprüfen
- Erstellen einer RACI- oder RASCI-Matrix für ein Cloud-Betriebsmodell
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2-Instances
- Erstellen Sie benutzerdefinierte AWS Config-Regeln mithilfe von AWS CloudFormation Guard-Richtlinien
- Automatisches Erstellen von Tag-basierten CloudWatch Amazon-Dashboards
- Löschen ungenutzter Amazon Elastic Block Store (Amazon EBS)-Volumes mithilfe von AWS Config und AWS Systems Manager
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform
- Bereitstellen von Code in mehreren AWS-Regionen mithilfe von AWS CodePipeline, AWS CodeCommitund AWS CodeBuild
- Exportieren Sie einen Bericht über AWS IAM Identity Center-Identitäten und deren Zuweisungen mithilfe von PowerShell
- Generieren einer AWS- CloudFormation Vorlage mit verwalteten AWS Config-Regeln mithilfe vonoSphere
- Gewähren Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Starten eines CodeBuild Projekts über AWS-Konten hinweg mithilfe von Step Functions und einer Lambda-Proxy-Funktion
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- IAM-Root-Benutzeraktivitäten überwachen

- ???
- Aufbewahren von routbarem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze, die keine Workload sind
- Registrieren mehrerer AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES
- Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern
- Senden von Benachrichtigungen für eine Datenbank-Instance von Amazon RDS für SQL Server mithilfe eines On-Premises-SMTP-Servers und Database Mail
- Einrichten eines Grafana-Überwachungs-Dashboards für AWS ParallelCluster
- Automatisches Markieren von Transit Gateway-Anhängen mit AWS Organizations
- Verwenden Sie Bol Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren
- Visualisieren von IAM-Anmeldeinformationsberichten für alle AWS-Konten mit Amazon QuickSight

Nachrichtenübermittlung und Kommunikation

Themen

Automatisieren Sie die RabbitMQ-Konfiguration in Amazon MQ

Erstellt von Yogesh Bhatia (AWS) und Afroz Khan (AWS)

Umgebung: PoC oder Pilot	Technologien: Nachricht enübermittlung und Kommunikation DevOps; Infrastruktur	AWS-Dienste: Amazon MQ; AWS CloudFormation

Übersicht

Amazon MQ ist ein verwalteter Message Broker-Service, der Kompatibilität mit vielen gängigen Message Brokern bietet. Die Verwendung von Amazon MQ mit RabbitMQ bietet einen robusten RabbitMQ-Cluster, der in der Amazon Web Services (AWS) -Cloud mit mehreren Brokern und Konfigurationsoptionen verwaltet wird. Amazon MQ bietet eine hochverfügbare, sichere und skalierbare Infrastruktur und kann problemlos eine große Anzahl von Nachrichten pro Sekunde verarbeiten. Mehrere Anwendungen können die Infrastruktur mit unterschiedlichen virtuellen Hosts, Warteschlangen und Exchanges nutzen. Die Verwaltung dieser Konfigurationsoptionen oder die manuelle Erstellung der Infrastruktur kann jedoch Zeit und Mühe erfordern. Dieses Muster beschreibt eine Möglichkeit, Konfigurationen für RabbitMQ in einem Schritt über eine einzige Datei zu verwalten. Sie können den mit diesem Muster bereitgestellten Code in jedes Continuous Integration (CI) -Tool wie Jenkins oder Bamboo einbetten.

Du kannst dieses Muster verwenden, um jeden RabbitMQ-Cluster zu konfigurieren. Alles, was es benötigt, ist Konnektivität zum Cluster. Obwohl es viele andere Möglichkeiten gibt, RabbitMQ-Konfigurationen zu verwalten, erstellt diese Lösung ganze Anwendungskonfigurationen in einem Schritt, sodass Sie Warteschlangen und andere Details einfach verwalten können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde so installiert und konfiguriert, dass sie auf Ihr AWS-Konto verweist (Anweisungen finden Sie in der AWS-CLI-Dokumentation)
- Ansible ist installiert, sodass Sie Playbooks ausführen können, um die Konfiguration zu erstellen
- rabbitmqadmin ist installiert (Anweisungen finden Sie in der RabbitMQ-Dokumentation)

- Ein RabbitMQ-Cluster in Amazon MQ, erstellt mit gesunden Amazon-Metriken CloudWatch

Zusätzliche Anforderungen

- Stellen Sie sicher, dass Sie die Konfigurationen für virtuelle Hosts und Benutzer separat und nicht als Teil von JSON erstellen.
- Stellen Sie sicher, dass das Konfigurations-JSON Teil des Repositorys ist und versionsgesteuert ist.
- Die Version der rabbitmqadmin-CLI muss mit der Version des RabbitMQ-Servers identisch sein, daher ist es am besten, die CLI von der RabbitMQ-Konsole herunterzuladen.
- Stellen Sie im Rahmen der Pipeline sicher, dass die JSON-Syntax vor jedem Lauf validiert wird.

Produktversionen

- AWS-CLI Version 2.0
- Ansible Version 2.9.13
- rabbitmqadmin Version 3.9.13 (muss mit der RabbitMQ-Serverversion identisch sein)

Architektur

Quelltechnologie-Stack

- Ein RabbitMQ-Cluster, der auf einer vorhandenen lokalen virtuellen Maschine (VM) oder einem Kubernetes-Cluster (vor Ort oder in der Cloud) ausgeführt wird

Zieltechnologie-Stack

- Automatisierte RabbitMQ-Konfigurationen auf Amazon MQ für RabbitMQ

Zielarchitektur

Es gibt viele Möglichkeiten, RabbitMQ zu konfigurieren. Dieses Muster verwendet die Importkonfigurationsfunktion, bei der eine einzelne JSON-Datei alle Konfigurationen enthält. Diese Datei wendet alle Einstellungen an und kann von einem Versionskontrollsystem wie Bitbucket oder Git verwaltet werden. Dieses Muster verwendet Ansible, um die Konfiguration über die rabbitmqadmin-CLI zu implementieren.

Tools

Tools

- rabbitmqadmin ist ein Befehlszeilentool für die HTTP-basierte RabbitMQ-API. Es wird zur Verwaltung und Überwachung von RabbitMQ-Knoten und -Clustern verwendet.
- Ansible ist ein Open-Source-Tool zur Automatisierung von Anwendungen und IT-Infrastruktur.
- Mit AWS CLI können Sie mithilfe von Befehlen in einer Befehlszeilen-Shell mit AWS-Services interagieren.

AWS-Services

- Amazon MQ ist ein verwalteter Message Broker-Service, der es einfach macht, Message Broker in der Cloud einzurichten und zu betreiben.
- AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Infrastruktur einzurichten und die Cloud-Bereitstellung mit Infrastruktur als Code zu beschleunigen.

Code

Die in diesem Muster verwendete JSON-Konfigurationsdatei und ein Beispiel für ein Ansible-Playbook sind im Anhang enthalten.

Epen

Erstellen Sie Ihre AWS-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen RabbitMQ-Cluster auf AWS.	Wenn Sie noch keinen RabbitMQ-Cluster haben, können Sie AWS verwenden , um den Stack CloudFormation auf AWS zu erstellen . Oder Sie können das Cloudformation-Modul in	AWS CloudFormation, Ansible

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ansible verwenden, um den Stack zu erstellen. Bei letzterem Ansatz können Sie Ansible für beide Aufgaben verwenden: zum Erstellen der RabbitMQ-Infrastruktur und zum Verwalten von Konfigurationen.	

Erstellen Sie die Konfiguration von Amazon MQ für RabbitMQ

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Eigenschaftendatei.	Laden Sie die JSON-Konfigurationsdatei (`rabbitmqconfig.json`) im Anhang herunter oder exportieren Sie sie aus der RabbitMQ-Konsole. Ändern Sie sie, um Warteschlangen, Austauschvorgänge und Bindungen zu konfigurieren. Diese Konfigurationsdatei zeigt Folgendes: - Erzeugt zwei Warteschlangen: `sample-queue1` und `sample-queue2` - Erzeugt zwei Börsen: `sample-exchange1` und `sample-exchange2` - Implementiert die Bindung zwischen den Warteschlangen und den Börsen	JSON

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Diese Konfigurationen werden gemäß den Anforderungen von rabbitmqadmin unter dem virtuellen Root-Host (/) ausgeführt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Details der Amazon MQ for RabbitMQ-Infrastruktur ab.	Rufen Sie die folgenden Details für die RabbitMQ-Infrastruktur auf AWS ab: • Broker-Name • RabbitMQ-Host • RabbitMQ-Benutzername (der Administratorbenutzer, der bei der Clustererstellung erstellt wurde) • RabbitMQ-Passwort Sie können die AWS-Manag ementkonsole oder die AWS-CLI verwenden, um diese Informationen abzurufen. Diese Details ermöglichen es dem Ansible-Playbook, eine Verbindung zu Ihrem AWS-Konto herzustellen und den RabbitMQ-Cluster zum Ausführen von Befehlen zu verwenden. Wichtig: Der Computer, auf dem das Ansible-Playbook ausgeführt wird, muss auf Ihr AWS-Konto zugreifen können, und die AWS-CLI muss bereits konfiguriert sein, wie im Abschnitt Vorausset zungen beschrieben.	AWS-CLI, Amazon MQ

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Datei hosts_var.	Erstellen Sie die `hosts_var` Datei für Ansible und stellen Sie sicher, dass alle Variablen in der Datei definiert sind. Erwägen Sie, Ansible Vault zum Speichern des Passworts zu verwenden. Sie können die `hosts_var` Datei wie folgt konfigurieren (ersetzen Sie die Sternchen durch Ihre Informationen):
	`RABBITMQ_HOST: "**********.mq.us-east-2.amazonaws.com"`
	`RABBITMQ_VHOST: "/"`
	`RABBITMQ_USERNAME: "admin"`
	`RABBITMQ_PASSWORD: "*******"`
		Ansible

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Ansible-P laybook.	Ein Beispiel-Playbook finden Sie `ansible-rabbit-config.yaml` im Anhang. Laden Sie diese Datei herunter und speichern Sie sie. Das Ansible-Playbook importiert und verwaltet alle RabbitMQ-Konfigura tionen, wie Warteschlangen, Exchanges und Bindungen, die Anwendungen benötigen. Folgen Sie den bewährten Methoden für Ansible-P laybooks, z. B. zum Sichern von Passwörtern. Verwenden Sie Ansible Vault für die Passwortverschlüsselung und rufen Sie das RabbitMQ-Passwort aus der verschlüs selten Datei ab.	Ansible

Bereitstellen der Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Playbook aus.	Führen Sie das Ansible-Playbook aus, das Sie im vorherigen Epos erstellt haben. `ansible-playbook ansible-rabbit-con fig.yaml`	RabbitMQ, Amazon MQ, Ansible

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können die neuen Konfigurationen auf der RabbitMQ-Konsole überprüfen.	

Zugehörige Ressourcen

- Migration von RabbitMQ zu Amazon MQ (AWS-Blogbeitrag)
- Management-Befehlszeilentool (RabbitMQ-Dokumentation)
- Einen CloudFormation AWS-Stack erstellen oder löschen (Ansible-Dokumentation)
- Migration nachrichtengesteuerter Anwendungen zu Amazon MQ für RabbitMQ (AWS-Blogbeitrag)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verbessern Sie die Anrufqualität auf den Workstations von Kundendienstmitarbeitern in Amazon Connect-Kontaktzentren

Erstellt von Ernest Ozdoba (AWS)

Umgebung: Produktion	Technologien: Messaging und Kommunikation; Endbenutzer-Computing	AWS-Services: Amazon Connect

Übersicht

Probleme mit der Anrufqualität sind einige der schwierigsten Probleme, die in Kontaktzentren behoben werden können. Um Probleme mit der Sprachqualität und komplexe Verfahren zur Fehlerbehebung zu vermeiden, müssen Sie die Arbeitsumgebung und die Workstation-Einstellungen Ihrer Kundendienstmitarbeiter optimieren. Dieses Muster beschreibt Techniken zur Optimierung der Sprachqualität für Kundendienstmitarbeiterarbeitsplätze in Amazon Connect-Kontaktzentren. Es bietet Empfehlungen in den folgenden Bereichen:

- Anpassungen der Arbeitsumgebung. Die Umgebung von Kundendienstmitarbeitern wirkt sich nicht darauf aus, wie die Stimme über das Netzwerk übertragen wird, aber sie haben Auswirkungen auf die Anrufqualität.
- Einstellungen für die Kundendienstmitarbeiter-Workstation. Hardware- und Netzwerkkonfigurationen für Kontaktcenter-Workstations haben erhebliche Auswirkungen auf die Anrufqualität.
- Browsereinstellungen. Kundendienstmitarbeiter verwenden einen Webbrowser, um auf die Website des Amazon Connect Contact Control Panel (CCP) zuzugreifen und mit Kunden zu kommunizieren, sodass sich die Browsereinstellungen auf die Anrufqualität auswirken können.

Die folgenden Komponenten können sich auch auf die Anrufqualität auswirken, sie fallen jedoch außerhalb des Bereichs der Workstation und sind in diesem Muster nicht abgedeckt:

- Datenverkehr fließt über AWS Direct Connect, ein Full-Tunnel-VPN oder ein Split-Tunnel-VPN zur Amazon Web Services (AWS)-Cloud
- Netzwerkbedingungen bei der Arbeit im oder außerhalb des Unternehmens

- Public Switched Phone Network (PSTN)-Konnektivität
- Das Gerät und der Telefonanbieter des Kunden
- Einrichtung der virtuellen Desktop-Infrastruktur (VDI)

Weitere Informationen zu diesen Bereichen finden Sie unter Häufige Probleme mit dem Contact Control Panel (CCP) und Verwenden des Endpoint Test Utility in der Amazon Connect-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Headsets und Workstations müssen den im Amazon Connect Administratorhandbuch angegebenen Anforderungen entsprechen.

Einschränkungen

- Die Optimierungstechniken in diesem Muster gelten für die Sprachqualität des Softphones. Sie gelten nicht, wenn Sie das Amazon Connect CCP im Festnetztelefonmodus konfigurieren. Sie können jedoch den Festnetztelefonmodus verwenden, wenn Ihre Softphone-Einrichtung keine akzeptable Sprachqualität für den Anruf bietet.

Produktversionen

- Informationen zu unterstützten Browsern und Versionen finden Sie im Amazon Connect Administratorhandbuch.

Architektur

Dieses Muster ist architekturunabhängig, da es auf die Einstellungen der Kundendienstmitarbeiter-Workstation abzielt. Wie das folgende Diagramm zeigt, ist der Sprachpfad vom Kundendienstmitarbeiter zum Kunden vom Headset, Browser, Betriebssystem, Workstation-Hardware und Netzwerk des Kundendienstmitarbeiters betroffen.

In Amazon Connect-Kontaktzentren wird die Audiokonnektivität des Benutzers mit WebRTC hergestellt. Sprache wird mit dem interaktiven Opus-Audiocodec kodiert und während der Übertragung mit dem Secure Real-Time Transport Protocol (SRTP) verschlüsselt. Andere Netzwerkarchitekturen sind möglich, darunter VPN-, private WAN/LAN- und ISP-Netzwerke.

Tools

- Amazon Connect Endpoint Test Utility – Dieses Dienstprogramm überprüft die Netzwerkkonnektivität und die Browsereinstellungen.
- Browser-Konfigurationseditoren für WebRTC-Einstellungen:
  - Für Firefox: about:config
  - Für Chrome: Chrome://Flags
- CCP Log Parser – Dieses Tool hilft Ihnen bei der Analyse von CCP-Protokollen zu Fehlerbehebungszwecken.

Polen

Anpassen der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reduzieren Sie Hintergrundrauschen.	Vermeiden Sie verrauschte Umgebungen. Wenn dies nicht möglich ist, optimieren Sie die Umgebung mit den folgenden Tipps zur Soundsicherheit: • Reduzieren Sie das Rauschen, indem Sie Sound-dissipierende Oberflächen wie z. B. Trichter, Trichter und weiche Trichter verwenden. • Blockieren Sie das Rauschen, indem Sie	Kundendienstmitarbeiter, Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Barrieren zwischen den Tischen setzen. • Stellen Sie sich eine aktive Rauschunterdrückun gslösung (ANC) vor, z. B. einen White-Noise-Genera tor, um die Sicherheit zu erhöhen und sicherzus tellen, oder verwenden Sie Headsets mit Rauschunt erdrückung. • Vermeiden Sie Echo bei Ihren Anrufen. Große, leere Leerzeichen können Echoeffekte verursachen oder Rauschen verstärke n. Das Bedecken von Oberflächen, die unzustell bare Signale auslösen können, trägt dazu bei, Echos zu reduzieren.	

Optimieren der Einstellungen für die Workstation von Kundendienstmitarbeitern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie das richtige Headset aus.	• Wenn die Umgebung verrauscht ist, wählen Sie ein Stereo-Headset aus. Wenn Sie den Ton an beide Trichter weiterlei ten, können Kundendie nstmitarbeiter den Kunden besser konzentrieren und	Kundendienstmitarbeiter, Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hören, und das Gesamtrau schen wird reduziert, da es weniger wahrscheinlich ist, dass Kundendienstmitarb eiter ihre Stimme erhöhen. • Vermeiden Sie es, Lautsprecher oder integrier tes Computeraudio zu verwenden. Verwenden Sie für optimale Qualität ein kabelgebundenes Headset, das speziell für die Verwendung im Kontaktzentrum vorgesehe n ist. WLAN-Headsets sind praktisch, aber sie können aufgrund von Störungen und Transcodierung eine Quelle für zusätzliche Audioverz ögerung und eine geringere Audioqualität sein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie das Headset wie vorgesehen.	• Aktivieren Sie die aktiven Funktionen zur Rauschunt erdrückung und zur Sprachverbesserung Ihres Headsets, falls diese verfügbar sind. Suchen Sie nach Einstellungen wie ANC oder ANR. Anweisung en zum Aktivieren dieser Einstellungen finden Sie im Benutzerhandbuch für Ihr Headset. • Passen Sie Ihr Mikrofon so an, dass Sie direkt darin sprechen können. Die beste Position für Ihr Mikrofon liegt direkt unter Ihrem Quad. Die korrekte Platzierung kann einen Unterschied von 10 Dezibeln (dB) im Soundlevel bewirken. Die meisten Headsets ermöglich en es Ihnen, den Mikrofona rm (Boom) zu rotieren oder zu schieben. Daher ist es wichtig, ihn an der richtigen Stelle zu halten, wenn Sie sprechen. • Einige Headsets sind mit mehreren Mikrofonen und erweiterten Funktionen wie Sprachhörer ausgestattet, mit denen Sprache ohne Kabel erfasst werden kann.	Kundendienstmitarbeiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um sicherzustellen, dass Sie das Hauptmikrofon wie vom Hersteller vorgesehen verwenden, lesen Sie das Benutzerhandbuch für Ihr Gerät.	
Überprüfen Sie die Workstation-Ressourcen.	Stellen Sie sicher, dass die Computer Ihrer Kundendienstmitarbeiter leistungsfähig sind. Wenn sie Anwendungen von Drittanbietern verwenden, die -Ressourcen verbrauchen, erfüllen ihre Computer möglicherweise nicht die Mindesthardwareanforderungen für die Ausführung von CCP. Wenn Kundendienstmitarbeiter Probleme mit der Anrufqualität haben, stellen Sie sicher, dass sie über genügend Rechenleistung (CPU), Festplattenspeicher, Netzwerkbandbreite und Arbeitsspeicher für CCP verfügen. Kundendienstmitarbeiter sollten alle unnötigen Anwendungen und Registerkarten schließen, um die CCP-Leistung und die Anrufqualität zu verbessern.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Soundeinstellungen des Betriebssystems.	Die Standardeinstellungen für Mikrofonstufe und Boost funktionieren normalerweise in Ordnung. Wenn Sie feststellen, dass die ausgehende Stimme still ist oder das Mikrofon zu stark annimmt, kann es hilfreich sein, diese Einstellungen anzupassen. Mikrofoneinstellungen finden Sie in der Systemtonkonfiguration Ihres Computers (Ton, Eingabe unter MacOS, Mikrofoneigenschaften unter Windows). Sie können über Systemtools oder Anwendungen von Drittanbietern auf erweiterte Einstellungen zugreifen, die sich auf die Sprachqualität auswirken können. Hier sind einige der Einstellungen, die Sie überprüfen können: • Sample rate – Dieser Wert bestimmt, wie oft der Sound pro Sekunde untersucht wird. Die Standardeinstellung ist normalerweise 44 oder 48 Kilohertz (kHz). Der optimale Wert für Amazon Connect ist 48 kHz. Sie können Ihre Browsereinstellungen verwenden, um den Standardwert zu	Agent, Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	überschreiben. Weitere Informationen finden Sie im Abschnitt zur Fehlerbeh ebung im Amazon Connect-Administratorhandbuch. • Gewinn – Dieser Wert bestimmt, wie stark das Mikrofon den Ton amplizier t. Wenn Sie den Gewinn erhöhen, nimmt Ihr Mikrofon möglicherweise mehr Hintergrundrauschen auf. • Bit-Tiefe – Dieser digitale Auflösungswert beschreibt, wie viele Stufen von Sound Telefonie erkannt werden. Je höher die Bittiefe, desto gleichmäßiger hört die Stimme. Viele herkömmliche Telefonnetze verwenden jedoch den Telefonie-Code-Modulationsstandard (PCM), der nur eine 8-Bit-Auflösung unterstützt. • Offener Schwellenwert – Dies ist der minimale Tondruck, den ein Mikrofon aufnimmt. Wenn Sie Probleme mit der Sprachqualität haben, versuchen Sie, diese Werte auf ihre Standardeinstellun gen wiederherzustellen, bevor	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie weitere Untersuchungen durchführen. Weitere Informationen zu diesen und anderen anpassbaren Einstellungen finden Sie im Gerätehan dbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie ein kabelgebundenes Netzwerk.	In der Regel hat ein kabelgebundenes Ethernet eine geringere Latenz, sodass es einfacher ist, die für die Sprachdatenübertragung erforderliche konsistente Übertragungsqualität bereitzustellen. Wir empfehlen mindestens 100 KB Bandbreite pro Aufruf. • Wenn Kundendienstmitarbeiter von zu Hause aus arbeiten, empfehlen wir eine kabelgebundene Verbindung über WLAN-Verbindungen. Es sollte nicht mehr als 150 Millisekunden dauern, bis der Kunde gehört wird. Sie können auf den Latenztest von Amazon Connect über das Amazon Connect Endpoint Test Utility zugreifen. Dieses Dienstprogramm misst jedoch die Verzögerung vom Browser zu Amazon Connect-Regionen, nicht zu Kunden. Die unidirektionale Verzögerungsempfehlung von 150 Millisekunden verhindert, dass Kundendienstmitarbeiter und Kunde miteinander sprechen. Der Wert wird von Anfang zu	Netzwerkadministrator, Kundendienstmitarbeiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ende gemessen, und jedes Element fügt eine Verzögerung hinzu, einschließlich des Teils des Anrufs zwischen der Amazon Connect-Region und dem Kunden. • Wenn Kundendienstmitarbeiter vom Büro aus arbeiten, ist Unternehmens-Wi-Fi akzeptabel, solange sich die Parameter im empfohlenen Bereich befinden und der Echtzeit-Transportprotokoll (RTP)-Datenverkehr priorisiert wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Hardwaret reiber.	Wenn Sie ein USB-Headset oder einen anderen Headset-Typ verwenden, das über eine eigene Firmware verfügt, empfehlen wir Ihnen, es mit der neuesten Version auf dem neuesten Stand zu halten. Einfache Headsets, die einen Hilfsport verwenden , verwenden das integrierte Audiogerät des Computers . Stellen Sie daher sicher, dass der Hardwaretreiber des Betriebssystems auf dem neuesten Stand ist. In seltenen Fällen kann eine Aktualisierung des Audiotrei bers zu Audioproblemen führen, und Sie müssen sie möglicherweise zurücksetzen. Weitere Informationen zum Ändern von Firmware- und Treiberversionen finden Sie im Gerätehandbuch.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vermeiden Sie USB-Hubs und -Dongles.	Wenn Sie Ihr Headset verbinden, vermeiden Sie zusätzliche Geräte wie Dongles, Porttypkonverter, Hubs und Erweiterungskabel. Diese Geräte können sich auf die Anrufqualität auswirken . Verbinden Sie Ihr Gerät stattdessen direkt mit dem Port auf Ihrem Computer.	Kundendienstmitarbeiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CCP-Protokolle.	Der CCP Log Parser bietet eine einfache Möglichkeit, Anwendungsprotokolle zu überprüfen. 1. Laden Sie die CCP-Protokolle nach einem Anruf herunter. 2. Öffnen Sie den CCP Log Parser . 3. Ziehen Sie die Protokolldatei per Drag-and-Drop, um das Protokoll zur Analyse hochzuladen. 4. Wenn das Protokoll analysiert wurde, wird standardmäßig die Registerkarte Snapshots und Protokolle ausgewählt. Wählen Sie die Registerkarte Metriken daneben, um die Erkenntnisse zu überprüfen. 5. Überprüfen Sie im Abschnitt WebRTC-Metriken – audio_input Folgendes: • Das Audiolevel-Diagramm, um zu sehen, ob Ihr empfangener Audiolevel über 0 liegt. Dies weist darauf hin, dass Audio von Ihrem Anrufer empfangen wurde.	Kundendienstmitarbeiter (erweiterte Fähigkeiten)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Das Paketdiagramm für alle verlorenen Pakete. Wenn dieses Diagramm signifikante Erhöhungen zeigt, wenden Sie sich an Ihr IT-Support-Team. 6. Überprüfen Sie im Abschnitt WebRTC-Metriken – audio_output Folgendes: • Das Audiolevel-Diagramm, um zu bestätigen, dass Audio von Ihrem Gerät gesendet wurde. • Das Paketdiagramm. Wenn Sie einen Anstieg des Paketverlusts feststellen, melden Sie ihn Ihrem IT-Support-Team. • Das Jitter-Puffer- und RTT-Diagramm. Werte für die Round Trip Time (RTT) über 300 wirken sich auf die Anruferfa hrung aus. Melden Sie diese Ihrem IT-Support-Team.	

Browsereinstellungen optimieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die WebRTC-Standardeinstellungen wieder her.	WebRTC muss aktiviert sein, um Softphones mit CCP zu tätigen. Wir empfehlen Ihnen, die Standardeinstellungen für WebRTC-bezogene Funktionen beizubehalten. • In Chrome können Sie Flags festlegen, indem Sie zu der URL Chrome://Flags navigieren. Geben Sie WebRTC in das Suchfeld ein, um Einstellungen zu finden, die das CCP beeinträchtigen können, und setzen Sie diese auf Standard . • Geben Sie in Firefox about:config in die Adresslei ste ein und geben Sie dann WebRTC in das Suchfeld auf der Konfigurationsseite ein. Nicht standardmäßige Einstellungen werden fett gedruckt und können in Standard geändert werden.	Administrator
Deaktivieren Sie Browserer weiterungen bei der Fehlerbeh ebung.	Einige Browsererweiterungen können sich auf die Anrufqual ität auswirken oder sogar verhindern, dass Anrufe ordnungsgemäß verbunden werden. Verwenden Sie das	Agent, Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Inkognitofenster oder den privaten Modus in Ihrem Browser und deaktivieren Sie alle Erweiterungen. Wenn das Problem dadurch behoben wird, überprüfen Sie Ihre Browsererweiterungen und suchen Sie nach verdächtigen Add-Ons, oder deaktivieren Sie sie einzeln.	
Überprüfen Sie die Browser-B eispielrate.	Vergewissern Sie sich, dass Ihre Mikrofoneingabe auf die optimale 48-kHz-Prüfrate eingestellt ist. Anweisung en finden Sie im Amazon Connect Administratorhandb uch.	Agent, Administrator

Zugehörige Ressourcen

Wenn Sie die Schritte in diesem Muster befolgt haben, aber immer noch Probleme mit der Anrufqualität haben, finden Sie Tipps zur Fehlerbehebung in den folgenden Ressourcen.

- Überprüfen Sie häufige Probleme mit dem Contact Control Panel (CCP).
- Überprüfen Sie die Verbindung mit dem Endpoint Test Utility .
- Folgen Sie bei anderen Problemen dem Leitfaden zur Fehlerbehebung.

Wenn Ihre Fehlerbehebung und Anpassungen das Anrufqualitätsproblem nicht lösen, liegt die Ursache möglicherweise außerhalb Ihrer Workstation. Wenden Sie sich zur weiteren Fehlerbehebung an Ihr IT-Support-Team.

Weitere Muster

- Zerlegen von Monolithen in Microservices mithilfe von CQRS und Event Sourcing
- Integrieren Sie Amazon API Gateway mit Amazon SQS, um asynchrone REST-APIs zu handhaben
- Registrieren mehrerer AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES
- Ausführen von nachrichtengesteuerten Workloads in großem Umfang mithilfe von AWS Fargate

Migration

Themen

Automatisieren Sie die Identifizierung und Planung von Migrationsstrategien mithilfe von AppScore

Umgebung: Produktion	Quelle: Alle Workloads	Ziel: AWS Cloud
R-Typ: N/A	Arbeitslast: Alle anderen Workloads	Technologien: Migration; Modernisierung; Web- und mobile Apps; SaaS
AWS-Services: AWS Application Discovery Service; AWS Migration Hub		

Übersicht

Lokale Anwendungen erfordern einen transformativen Ansatz, um die Vorteile der Amazon Web Services (AWS) Cloud voll auszuschöpfen. Die sieben gängigen Migrationsstrategien (7 Rs) bieten Ihnen Transformationsoptionen, die von technologischen Änderungen an lokalen Datenbankservern bis hin zur Neuerstellung einer Anwendung mithilfe einer cloudnativen Microservices-Architektur reichen.

Wenn Sie sich für das vollständige 7-Rs-Modell entscheiden, arbeiten Sie auf Anwendungs- und Geschäftsebene, anstatt nur die Server zu evaluieren und für die Migration vorzubereiten. Sie können Serverdaten zwar mithilfe von Tools wie AWS Migration Evaluator abrufen, andere Anwendungsinformationen werden jedoch häufig nicht aufgezeichnet (z. B. der Roadmap-Status, die erforderlichen Wiederherstellungszeitziele (RTO) und die Wiederherstellungspunktziele (Recovery Point Objective, RPO) oder Datenschutzanforderungen).

Dieses Muster beschreibt, wie Sie AppScorediese Herausforderungen mithilfe einer anwendungsorientierten Ansicht Ihres Portfolios vermeiden können. Dies beinhaltet eine empfohlene Transformationsroute zur AWS-Cloud für jede Anwendung im Vergleich zum vollständigen 7-Rs-Modell. AppScore hilft Ihnen dabei, Anwendungsinformationen zu erfassen, den idealen Transformationsweg zu bestimmen, die Risiken, die Komplexität und die Vorteile der Cloud-Einführung zu ermitteln und schnell die Migrationsumfänge, Verschiebungsgruppen und Zeitpläne zu definieren.

Dieses Muster wurde von AWS und AppScore Technology Limited, einem AWS-Partner, erstellt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Bestehende Anwendungen, die Sie in die AWS-Cloud migrieren möchten.
- Bestehende Serverinventarinformationen aus einem Tool wie AWS Migration Evaluator. Sie können diese Daten auch zu einem späteren Zeitpunkt Ihrer Migration importieren.
- Ein vorhandenes AppScore Konto mit Power-User-Rechten. Weitere Informationen zu AppScore Benutzerkonten finden Sie unter Wie weise ich Benutzern eine rollenbasierte Zugriffskontrolle (RBAC) zu? in der Dokumentation AppScore
- Ein Verständnis dafür, wie man RBAC-Rollen zuweist in. AppScore AppScore bietet drei Rollen als Fachexperte (KMU), die sich an den Fragen orientieren, die in der Bewertungsphase gestellt wurden. Das bedeutet, dass ein KMU nur Fragen beantwortet, die für sein Fachwissen und seine Rolle relevant sind. Weitere Informationen dazu finden Sie unter Wie weise ich Benutzern eine rollenbasierte Zugriffskontrolle (RBAC) zu? in der Dokumentation. AppScore
- Ein Verständnis AppScore der Empfehlungen, die auf den folgenden drei Kategorien von Anwendungsattributen basieren:
  - Risiko — Die geschäftliche Bedeutung der Anwendung, unabhängig davon, ob sie vertrauliche Daten enthält, Anforderungen an die Datenhoheit und die Anzahl der Anwendungsbenutzer oder Schnittstellen
  - Komplexität — Die Entwicklungssprache der Anwendung (COBOL hat beispielsweise eine höhere Punktzahl als .NET oder PHP), das Alter, die Benutzeroberfläche oder die Anzahl der Schnittstellen
  - Vorteil — Der Bedarf an Batch-Verarbeitung, das Anwendungsprofil, das Disaster-Recovery-Modell, die Nutzung der Entwicklungs- und Testumgebung
- Ein Verständnis AppScore der vier Phasen der iterativen Datenerfassung:
  - Beschilderung — Fragen, die mit Serverdaten kombiniert werden, um die 7-Rs-Bewertungen zu erstellen. Weitere Informationen finden Sie in der Dokumentation unter So werden Bewerbungen signalisiert und bewertet. AppScore
  - Bewertung — Fragen, bei denen das Risiko, der Nutzen und die Komplexität bewertet werden.
  - Bewertung des aktuellen Status — Fragen, die eine Bewertung des aktuellen Stands des Antrags ermöglichen.

- Transformation — Fragen, die die Anwendung für die future Staatsgestaltung umfassend bewerten.

Wichtig: Nur die Stufen Signposting und Scoring sind erforderlich, um Bewerbungspunkte und 7 Rs-Bewertungen zu erhalten und die Gruppenplanung zu ermöglichen. Nachdem Sie die Anträge und den Umfang der Formulare gruppiert haben, können Sie die Phasen „Bewertung des aktuellen Zustands“ und „Transformation“ abschließen, um sich einen detaillierteren Überblick über Ihre Bewerbung zu verschaffen.

Architektur

Das folgende Diagramm zeigt den AppScore Workflow, bei dem Anwendungs- und Serverdaten verwendet werden, um eine Empfehlung für Ihre Migrationsstrategie und Ihren Transformationsplan zu erstellen.

Tools

- AppScore— AppScore hilft Ihnen dabei, die Lücke zwischen Entdeckung und Migrationsimplementierung zu schließen, indem es eine anwendungsorientierte Ansicht Ihres Portfolios mit einer empfohlenen Route zur Cloud für jede Anwendung im Vergleich zum vollständigen 7-Rs-Modell bietet.
- AWS Migration Evaluator — AWS Migration Evaluator ist ein Service zur Migrationsbewertung, der Sie dabei unterstützt, ein aussagekräftiges Geschäftsszenario für Planung und Migration zu erstellen.

Epen

Erstellen und laden Sie die erste Anwendungsliste

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Liste der Bewerbungen vor.	Melden Sie sich mit Ihren Benutzeranmeldedaten beim AppScore Portal an. Laden Sie das `Import Template`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von der Anwendungsseite herunter und aktualisieren Sie es dann `Import Template` mit den nichttechnischen Attributen Ihrer Anwendung (z. B. Datenklassifizierung oder einer Liste von Attributen, die angepasst werden können). Weitere Informationen dazu finden Sie in der Dokumentation unter Wie ändere ich die AppScore Anwendungs- und Geschäftsfragebögen?. AppScore Hinweis: Sie können eine Anwendung auch manuell hinzufügen, indem Sie auf der Anwendungsseite die Option Neue Anwendung auswählen . Anschließend können Sie die nichttechnischen Attribute der Anwendung eingeben.	
Importieren Sie die Anwendungsdaten.	Wählen Sie auf der Anwendungsseite Anwendungen importieren aus, um Ihre Anwendungsdaten zu importieren.	Ingenieur für Migration

Erfassen Sie die Anwendungs- und Geschäftsdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfe und beantworte die Fragen zur Beschilderung und Bewertung.	Öffnen Sie die Seite Server und wählen Sie Server importieren. Wählen Sie die CSV-Datei aus, die Ihre Serverdaten enthält. Die Datei kann Attribute wie Name, Rechenzentrum, Betriebssystem, virtuell oder physisch, Anwendungsname, Rolle, Datenbanktechnologie, Umgebung, Anzahl und Auslastung der CPU-Kerne, RAM-Größe und -Auslastung, Festplattengröße und -auslastung, abgestimmter Maschinentyp sowie aktuelle und voraussichtliche monatliche Kosten enthalten. Bestätigen Sie die Spaltenzuweisung und wählen Sie Bestätigen und Importieren. Fehlende Informationen in den importierten Daten werden auf der Serverseite hervorgehoben. Sie können diese Lücken auf dieser Seite oder mithilfe der Option Massenbearbeitung beheben. Server sind der entsprechenden Anwendung zugeordnet. Wenn jedoch	Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	keine Anwendungen in vorhanden sind AppScore, werden sie automatisch erstellt und die Server werden dann zugeordnet. Sie können auch eine API-Verbindung verwenden, um die Daten mit AWS Migration Hub abzurufen. Weitere Informationen dazu finden Sie unter Wie importiere ich Server von AWS Migration Hub über die API? In der AppScore Dokumentation. Hinweis: Wenn Sie ein Discovery-Tool (z. B. AWS Migration Evaluator) verwendet haben, um die Leistung im Zeitverlauf zu erfassen, müssen Sie so schnell wie möglich einen frühen Extrakt der Serverdaten laden und die Daten aktualisieren, wenn die Leistungskennzahlen vollständig erfasst sind. AppScore verwendet die Servernamen, Betriebssystem- und Datenbankversionen, Rechenzentren und Umgebungen, um Ergebnisse und 7-Rs-Empfehlungen bereitzustellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ergebnisse der Anwendung.	Öffnen Sie die Bewerbungsseite, um die Punktzahl und die Bewertung Ihrer Bewerbungen mit 7 Rs einzusehen. Ihre aktuellen Betriebskosten werden ebenfalls berechnet. Diese Berechnungen werden aktualisiert, wenn neue Informationen auf die Seiten „Anwendungen“ oder „Server“ importiert werden.	Besitzer der App
Analysieren Sie einzelne Anwendungen.	Wählen Sie auf der Anwendungsseite eine Anwendung aus, um detaillierte Empfehlungen zu erhalten. Sie können den Application Assessment Report auswählen, um eine PDF- oder DOCX-Datei mit den detaillierten Bewertungsdaten für bestimmte Bewerbungen zu generieren.	Besitzer der App

Erstellen Sie den Migrationsplan

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Anwendungen für die Umzugsgruppe aus.	Öffnen Sie die Seite Planung, wählen Sie Group Builder und erstellen Sie dann Anwendungsverschiebungsgruppen gemäß Ihren Anforderungen.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Im Abschnitt Spalten können Sie der Anwendungsliste Attribute hinzufügen oder daraus entfernen. Sie können auch Anwendungsattribute im Bereich Filter verwenden , um bestimmte Anwendung en auszuwählen. Dazu gehört auch das Herausfiltern aller Anwendungen, die bereits Teil vorhandener Verschieb ungsgruppen sind.	
Erstellen Sie die Verschieb ungsgruppe.	Wählen Sie Ausgewählte Gruppe, geben Sie einen Namen für Ihre Move-Grup pe ein, wählen Sie die Anwendungen aus, die Sie in Ihre Move-Gruppe aufnehmen möchten, und klicken Sie dann auf Zur Gruppe hinzufügen.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie die Migration.	Auf der Seite „Umwandlungspläne“ finden Sie eine geschätzte Dauer, den Aufwand und die Kosten der Transformation für Ihre Transfergruppe. AppScore Die Transfergruppe wird automatisch dem allgemeinen Transformationszeitplan hinzugefügt. Hinweis: Sie können die Annahmen, die der Aufwandsschätzung zugrunde liegen, auf der Seite mit den Planungseinstellungen anpassen. Dies hilft, sie an die Anforderungen Ihres Unternehmens anzupassen. Weitere Informationen dazu finden Sie in der AppScore Dokumentation unter Wie konfiguriere ich die Planungseinstellungen?.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie den vollständigen Transformationsbericht.	Öffnen Sie die Group Manager-Seite und wählen Sie Create Application Transformation Report Doc. Wählen Sie die Verschiebegruppen aus und klicken Sie dann auf Exportieren. Dadurch wird eine DOCX-Datei generiert, die die Transformation zusammenfasst, einschließlich der Details für jede Move-Gruppe. Ein Beispiel für einen Bericht zur Anwendungstransformation finden Sie auf der Website unter Beispielbericht zur Anwendungstransformation. AppScore	Ingenieur für Migration

Zugehörige Ressourcen

- Was sind die 7 Rs einer Anwendungsmigration?
- Ein genauerer Blick auf AppScore
- AppScore im AWS Marketplace

Erstellen von AWS- CloudFormation Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python

Erstellt von Venkata Naveen Kopp (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Automation	Ziel: Datenbank in AWS Cloud
R-Typ: N/A	Workload: Microsoft	Technologien: Migration; Datenbanken

Übersicht

Dieses Muster beschreibt die Schritte zum automatischen Erstellen von AWS- CloudFormation Vorlagen für AWS Database Migration Service (AWS DMS) mit Microsoft Excel und Python.

Die Migration von Datenbanken mit AWS DMS beinhaltet häufig die Erstellung von AWS-CloudFormation Vorlagen zur Bereitstellung von AWS DMS-Aufgaben. Bisher erforderte das Erstellen von AWS- CloudFormation Vorlagen Kenntnisse der JSON- oder YAML-Programmiersprache. Mit diesem Tool benötigen Sie nur grundlegende Kenntnisse von Excel und wie Sie ein Python-Skript mit einem Terminal- oder Befehlsfenster ausführen.

Als Eingabe verwendet das Tool eine Excel-Arbeitsmappe, die die Namen der zu migrierenden Tabellen, Amazon-Ressourcennamen (ARNs) von AWS DMS-Endpunkten und AWS DMS-Replikations-Instances enthält. Das Tool generiert dann AWS- CloudFormation Vorlagen für die erforderlichen AWS DMS-Aufgaben.

Ausführliche Schritte und Hintergrundinformationen finden Sie im Blogbeitrag Erstellen von AWS-CloudFormation Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel im AWS Database-Blog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Microsoft Excel Version 2016 oder höher

- Python Version 2.7 oder höher
- Das xlrd Python-Modul (installiert an einer Eingabeaufforderung mit dem Befehl: pip install xlrd)
- AWS DMS-Quell- und Zielendpunkte und AWS DMS-Replikations-Instance

Einschränkungen

- Die Namen von Schemata, Tabellen und zugehörigen Spalten werden an den Zielendpunkten in Kleinbuchstaben umgewandelt.
- Dieses Tool berücksichtigt nicht die Erstellung von AWS DMS-Endpunkten und Replikations-Instances.
- Derzeit unterstützt das Tool nur ein Schema für jede AWS DMS-Aufgabe.

Architektur

Quelltechnologie-Stack

- Eine On-Premises-Datenbank
- Microsoft Excel

Zieltechnologie-Stack

- AWS- CloudFormation Vorlagen
- Eine Datenbank in der AWS Cloud

Architektur

Tools

- Pycharm IDE oder eine beliebige integrierte Entwicklungsumgebung (IDE), die Python Version 3.6 unterstützt
- Microsoft Office 2016 (für Microsoft Excel)

Polen

Konfigurieren des Netzwerks, der AWS DMS-Replikations-Instance und der Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beantragen Sie bei Bedarf eine Erhöhung des Servicekontingents.	Beantragen Sie bei Bedarf eine Erhöhung des Servicekontingents für die AWS DMS-Aufgaben.	Allgemeines AWS
Konfigurieren Sie die AWS-Region, Virtual Private Clouds (VPCs), CIDR-Bereiche, Availability Zones und Subnetze.		Allgemeines AWS
Konfigurieren Sie die AWS DMS-Replikations-Instance.	Die AWS DMS-Replikations-Instance kann sowohl eine Verbindung zu On-Premises- als auch zu AWS-Datenbanken herstellen.	Allgemeines AWS
Konfigurieren Sie AWS DMS-Endpunkte.	Konfigurieren Sie Endpunkte sowohl für die Quell- als auch für die Zieldatenbank.	Allgemeines AWS

Bereiten Sie die Telefonie für AWS DMS-Aufgaben und Tags vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Tabellenliste.	Listen Sie alle an der Migration beteiligten Tabellen auf.	Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Aufgaben vor.	Bereiten Sie das Excel-Kabel mithilfe der von Ihnen konfiguri erten Tabellenliste vor.	Allgemeines AWS, Microsoft Excel
Bereiten Sie die Tags vor.	Details zu den AWS-Resso urcen-Tags, die an die AWS DMS-Aufgaben angehängt werden sollen.	Allgemeines AWS, Microsoft Excel

Herunterladen und Ausführen des Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Tool zur Vorlagengenerierung aus dem GitHub Repository herunter und extrahieren Sie es.	GitHub -Repository: https://g ithub.com/aws-samples/dms-cloudformation-templates-gen erator/	
Führen Sie das Tool aus.	Folgen Sie den detaillierten Anweisungen im Blogbeitrag, der unter „Referenzen und Hilfe“ aufgeführt ist.	

Zugehörige Ressourcen

- Erstellen von AWS- CloudFormation Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel (Blogbeitrag)
- DMS CloudFormation Templates Generator (GitHub Repository)
- Python-Dokumentation
- xlrd-Beschreibung und Download
- AWS DMS-Dokumentation
- AWS- CloudFormation Dokumentation

Erste Schritte mit der automatisierten Portfolioerkennung

Erstellt von Pratik Chunawala (AWS) und Bololfo Jr. Cerrada (AWS)

Umgebung: Produktion	Quelle: On-Premises	Ziel: On-Premises
R-Typ: N/A	Workload: Alle anderen Workloads	Technologien: Migration

Übersicht

Die Bewertung des Portfolios und die Erfassung von Metadaten ist eine kritische Herausforderung bei der Migration von Anwendungen und Servern in die Amazon Web Services (AWS) Cloud, insbesondere bei großen Migrationen mit mehr als 300 Servern. Die Verwendung eines automatisierten Portfolioerkennungstools kann Ihnen helfen, Informationen über Ihre Anwendungen zu sammeln, z. B. die Anzahl der Benutzer, die Häufigkeit der Verwendung, Abhängigkeiten und Informationen über die Infrastruktur der Anwendung. Diese Informationen sind bei der Planung von Migrationswellen unerlässlich, damit Sie Anwendungen mit ähnlichen Eigenschaften ordnungsgemäß priorisieren und gruppieren können. Die Verwendung eines Erkennungstools optimiert die Kommunikation zwischen dem Portfolioteam und den Anwendungsbesitzern, da das Portfolioteam die Ergebnisse des Erkennungstools validieren kann, anstatt die Metadaten manuell zu erfassen. In diesem Muster werden die wichtigsten Überlegungen zur Auswahl eines automatisierten Erkennungstools sowie Informationen zur Bereitstellung und zum Testen eines Tools in Ihrer Umgebung erörtert.

Dieses Muster enthält eine Vorlage, die als Ausgangspunkt für die Erstellung Ihrer eigenen Checkliste für allgemeine Aktivitäten dient. Neben der Checkliste finden Sie eine Vorlage für eine RACI-Matrix (Verantwortlich, Rechenschaftspflicht, Konsultiert, Informiert). Sie können diese RACI-Matrix verwenden, um zu bestimmen, wer für jede Aufgabe in Ihrer Checkliste verantwortlich ist.

Polen

Auswählen eines Erkennungstools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie fest, ob ein Erkennungstool für Ihren Anwendungsfall geeignet ist.	Ein Erkennungstool ist möglicherweise nicht die beste Lösung für Ihren Anwendung sfall. Berücksichtigen Sie den Zeitaufwand für die Auswahl, Beschaffung, Vorbereitung und Bereitstellung eines Erkennungstools. Es kann 4–8 Wochen dauern, bis die Scan-Appliance für ein Agentless -Discovery-Tool in Ihrer -Umgebung eingerichtet oder Agenten auf allen im Umfang enthaltenen Workloads installiert ist. Nach der Bereitstellung müssen Sie 4–12 Wochen für das Erkennung stool einplanen, um Metadaten zu sammeln, indem Sie die Anwendungs-Workloads scannen und eine Anwendung s-Stack-Analyse durchführ en. Wenn Sie weniger als 100 Server migrieren, können Sie möglicherweise die Metadaten manuell erfassen und Abhängigkeiten schneller analysieren als die Zeit, die für die Bereitstellung und Erfassung von Metadaten mit einem automatisierten	Migrationsleiter, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erkennungstool erforderlich ist.	
Wählen Sie ein Erkennung stool aus.	Lesen Sie die Überlegungen zur Auswahl eines Tools zur automatisierten Erkennung im Abschnitt Zusätzliche Informationen. Bestimmen Sie die geeigneten Kriterien für die Auswahl eines Erkennung stools für Ihren Anwendung sfall und werten Sie dann jedes Tool anhand dieser Kriterien aus. Eine umfassend e Liste der Tools zur automatis ierten Erkennung finden Sie unter Tools zur Migration von Erkennungs-, Planungs- und Empfehlungen.	Migrationsleiter, Migration singenieur

Vorbereiten der Installation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Checkliste vor der Bereitstellung vor.	Erstellen Sie eine Checklist e der Aufgaben, die Sie erledigen müssen, bevor Sie das Tool bereitstellen. Ein Beispiel finden Sie unter Checkliste für die Vorabbere itstellung auf der Flexera-D okumentationswebsite.	Entwicklungsleiter, Migration singenieur, Migrationsleiter, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Netzwerkanforderungen vor.	Stellen Sie die Ports, Protokolle, IP-Adressen und das Routing bereit, die für die Ausführung und den Zugriff auf die Zielserver durch das Tool erforderlich sind. Weitere Informationen finden Sie im Installationshandbuch für Ihr Erkennungstool. Ein Beispiel finden Sie unter Bereitstellungsanforderungen auf der Flexera-Dokumentationswebsite.	Migrationsingenieur, Netzwerkadministrator, Cloud-Architekt
Bereiten Sie die Anforderungen an das Konto und die Anmeldeinformationen vor.	Identifizieren Sie die Anmeldeinformationen, die Sie für den Zugriff auf die Zielserver und die Installation aller Komponenten des Tools benötigen.	Cloud-Administrator, Allgemeines AWS, Migrationsingenieur, Migrationsleiter, Netzwerkadministrator, AWS-Administrator
Bereiten Sie die Appliances vor, auf denen Sie das Tool installieren werden.	Stellen Sie sicher, dass die Appliances, auf denen Sie die Toolkomponenten installieren, die Spezifikationen und Plattformanforderungen für das Tool erfüllen.	Migrationsingenieur, Migrationsleiter, Netzwerkadministrator
Bereiten Sie die Änderungsaufträge vor.	Bereiten Sie gemäß dem Änderungsmanagement-Prozess in Ihrer Organisation die erforderlichen Änderungsaufträge vor und stellen Sie sicher, dass diese Änderungsaufträge genehmigt sind.	Leiter der Erstellung, Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die Anforderungen an die Stakeholder.	Senden Sie die Checkliste und die Netzwerkanforderungen vor der Bereitstellung an die Stakeholder. Stakeholder sollten die erforderlichen Anforderungen überprüfen, bewerten und vorbereiten, bevor sie mit der Bereitstellung fortfahren.	Leiter der Erstellung, Leiter der Migration

Bereitstellen des Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Installationsprogramm herunter.	Laden Sie das Installationsprogramm oder das Image der virtuellen Maschine herunter. Images virtueller Maschinen werden in der Regel im Open Virtualization Format (OVF) geliefert.	Leiter der Erstellung, Leiter der Migration
Extrahieren Sie die Dateien.	Wenn Sie ein Installationsprogramm verwenden, müssen Sie das Installationsprogramm herunterladen und auf einem On-Premises-Server ausführen.	Leiter der Erstellung, Leiter der Migration
Stellen Sie das Tool auf den Servern bereit.	Stellen Sie das Erkennungstool auf den On-Premises-Zielservern wie folgt bereit: • Wenn es sich bei Ihrer Quelldatei um ein Image	Build-Verantwortlicher, Migrationsleiter, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einer virtuellen Maschine handelt, stellen Sie es in Ihrer Umgebung der virtuelle n Maschine bereit, z. B. VMware . • Wenn Ihre Quelldatei ein Installationsprogramm ist, führen Sie das Installat ionsprogramm aus, um das Tool zu installieren und einzurichten.	
Melden Sie sich beim Erkennungstool an.	Folgen Sie den Anweisung en auf dem Bildschirm und melden Sie sich an, um mit dem Tool zu beginnen.	Migrationsleiter, Entwicklu ngsleiter
Aktivieren Sie das Produkt.	Geben Sie Ihren Lizenzsch lüssel ein.	Leiter der Erstellung, Leiter der Migration
Konfigurieren Sie das Tool.	Geben Sie alle Anmeldein formationen ein, die für den Zugriff auf die Zielserve r erforderlich sind, z. B. Anmeldeinformationen für Windows, VMware, Simple Network Management Protocol (SNMP) und Secure Shell Protocol (SSH) oder Datenbanken.	Leiter der Erstellung, Leiter der Migration

Testen des Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie Testserver aus.	Identifizieren Sie einen kleinen Satz von Subnetzen oder IP-Adressen, die nicht zur Produktion gehören, mit denen Sie das Erkennungstool testen können. Auf diese Weise können Sie die Scans schnell validieren, Fehler schnell identifizieren und beheben und Ihre Tests von Produktio nsumgebungen isolieren.	Build-Verantwortlicher, Migrationsleiter, Netzwerka dministrator
Beginnen Sie mit dem Scannen der ausgewählten Testserver.	Geben Sie für ein Agentless-Discovery-Tool die Subnetze oder IP-Adressen für die ausgewählten Testserver in die Discovery-Tool-Konsole ein und starten Sie den Scan. Installieren Sie für ein agentenbasiertes Erkennung stool den Agenten auf den ausgewählten Testservern.	Build-Verantwortlicher, Migrationsleiter, Netzwerka dministrator
Überprüfen Sie die Scanergeb nisse.	Überprüfen Sie die Scanergeb nisse für die Testserver. Wenn Fehler gefunden werden, beheben Sie diese und beheben Sie sie. Dokumenti eren Sie die Fehler und Lösungen. Sie referenzieren diese Informationen in Zukunft und können diese Informati	Build-Verantwortlicher, Migrationsleiter, Netzwerka dministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen zu Ihrem Portfolio-Runbook hinzufügen.	
Scannen Sie die Testserver erneut.	Sobald der erneute Scan abgeschlossen ist, wiederhol en Sie den Scan, bis keine Fehler vorliegen.	Build-Verantwortlicher, Migrationsleiter, Netzwerka dministrator

Zugehörige Ressourcen

AWS-Ressourcen

- Leitfaden zur Bewertung des Anwendungsportfolios für die AWS Cloud-Migration
- Tools zur Migration von Erkennungs-, Planungs- und Empfehlungen

Bereitstellungsleitfäden für häufig ausgewählte Erkennungstools

- Bereitstellen der virtuellen RN150-Appliance (Flexera-Dokumentation)
- Gatherer-Installation (modelizeIT-Dokumentation)
- Installation des On-Premises-Analyseservers (modelizeIT-Dokumentation)

Zusätzliche Informationen

Überlegungen zur Auswahl eines automatisierten Erkennungstools

Jedes Erkennungstool hat Vorteile und Einschränkungen. Berücksichtigen Sie bei der Auswahl des geeigneten Tools für Ihren Anwendungsfall Folgendes:

- Wählen Sie ein Erkennungstool aus, das die meisten, wenn nicht alle Metadaten erfassen kann, die Sie benötigen, um Ihr Portfoliobewertungsziel zu erreichen.
- Identifizieren Sie alle Metadaten, die Sie manuell sammeln müssen, da das Tool sie nicht unterstützt.

- Stellen Sie den Stakeholdern die Anforderungen an das Erkennungstool zur Verfügung, damit sie das Tool auf der Grundlage ihrer internen Sicherheits- und Compliance-Anforderungen wie Server-, Netzwerk- und Anmeldeinformationsanforderungen überprüfen und bewerten können.
  - Erfordert das Tool, dass Sie einen Agenten im Umfang der Workload installieren?
  - Erfordert das Tool, dass Sie eine virtuelle Appliance in Ihrer Umgebung einrichten?
- Bestimmen Sie Ihre Anforderungen an die Datenresidenz. Einige Organisationen möchten ihre Daten nicht außerhalb ihrer Umgebung speichern. Um dies zu beheben, müssen Sie möglicherweise einige Komponenten des Tools in der On-Premises-Umgebung installieren.
- Stellen Sie sicher, dass das Tool das Betriebssystem (OS) und die Betriebssystemversion der im Umfang enthaltenen Workload unterstützt.
- Stellen Sie fest, ob Ihr Portfolio Mainframe-, Mittelbereichs- und Legacy-Server umfasst. Die meisten Erkennungstools können diese Workloads als Abhängigkeiten erkennen, aber einige Tools können möglicherweise keine Gerätedetails wie Auslastung und Serverabhängigkeiten abrufen. Device42 und modernizeIT-Erkennungstools unterstützen sowohl Mainframe- als auch Mittelbereichsserver.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS

Umgebung: PoC oder Pilotprojekt	Quelle: Cloudera-Workloads	Ziel: Öffentliche Cloud der Cloudera Data Platform (CDP)
R-Typ: N/A	Arbeitslast: Alle anderen Workloads	Technologien: Migration ; Große Datenmengen; Datenbanken; Analytik
AWS-Services: Amazon EC2; Amazon EKS; AWS Identity and Access Management; Amazon S3; Amazon RDS		

Übersicht

Dieses Muster beschreibt die allgemeinen Schritte für die Migration Ihrer lokalen Cloudera Distributed Hadoop (CDH), Hortonworks Data Platform (HDP) und Cloudera Data Platform (CDP) -Workloads zur CDP Public Cloud auf AWS. Wir empfehlen Ihnen, mit Cloudera Professional Services und einem Systemintegrator (SI) zusammenzuarbeiten, um diese Schritte umzusetzen.

Es gibt viele Gründe, warum Cloudera-Kunden ihre lokalen CDH-, HDP- und CDP-Workloads in die Cloud verlagern möchten. Zu den typischen Gründen gehören:

- Rationalisieren Sie die Einführung neuer Datenplattform-Paradigmen wie Data Lakehouse oder Data Mesh
- Erhöhen Sie die Agilität Ihres Unternehmens, demokratisieren Sie den Zugriff auf bestehende Datenbestände und deren Inferenz
- Senken Sie die Gesamtbetriebskosten (TCO)
- Verbessern Sie die Workload-Elastizität
- Ermöglichen Sie eine höhere Skalierbarkeit und reduzieren Sie den Zeitaufwand für die Bereitstellung von Datendiensten im Vergleich zu herkömmlichen Installationen vor Ort drastisch
- Legacy-Hardware außer Dienst stellen und Hardware-Aktualisierungszyklen deutlich reduzieren

- Nutzen Sie die pay-as-you-go Preisgestaltung, die mit dem Cloudera-Lizenzmodell (CCU) auf Cloudera-Workloads auf AWS ausgedehnt wird
- Nutzen Sie die Vorteile einer schnelleren Bereitstellung und einer verbesserten Integration mit Plattformen für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD)
- Verwenden Sie eine einzige einheitliche Plattform (CDP) für mehrere Workloads

Cloudera unterstützt alle wichtigen Workloads, einschließlich Machine Learning, Data Engineering, Data Warehouse, Operational Database, Stream Processing (CSP) sowie Datensicherheit und Governance. Cloudera bietet diese Workloads seit vielen Jahren vor Ort an, und Sie können diese Workloads in die AWS-Cloud migrieren, indem Sie CDP Public Cloud mit Workload Manager und Replication Manager verwenden.

Cloudera Shared Data Experience (SDX) bietet einen gemeinsamen Metadatenkatalog für diese Workloads, um eine konsistente Datenverwaltung und einen konsistenten Betrieb zu ermöglichen. SDX bietet außerdem umfassende, differenzierte Sicherheit zum Schutz vor Bedrohungen und eine einheitliche Steuerung für Prüf- und Suchfunktionen zur Einhaltung von Standards wie dem Payment Card Industry Data Security Standard (PCI DSS) und der DSGVO.

Die CDP-Migration auf einen Blick

Arbeitslast	Quell-Workload	CDH, HDP und CDP Private Cloud
	Quellumgebung	• Windows, Linux • Lokal, Colocation oder jede Umgebung außerhalb von AWS
	Ziel-Workload	CDP Public Cloud auf AWS
	Zielumgebung	• Bereitstellungsmodell: Kundenkonto • Betriebsmodell: Kunde/ClouderA-Steuerebene
	Migrationsstrategie (7Rs)	Rehosten, Neuplattformen oder Refactoring

Migration	Handelt es sich um ein Upgrade der Workload-Version?	Ja
	Dauer der Migration	• Bereitstellung: Ungefähr eine Woche, um ein Kundenkonto, eine vom Kunden verwaltete virtuelle private Cloud (VPC) und eine vom Kunden verwaltete CDP Public Cloud-Umgebung zu erstellen. • Migrationsdauer: 1—4 Monate, abhängig von der Komplexität und Größe der Arbeitslast.

Kosten	Kosten für die Ausführung des Workloads auf AWS	• Im Großen und Ganzen gehen die Kosten einer CDH-Workload-Migration zu AWS davon aus, dass Sie eine neue Umgebung auf AWS einrichten werden. Dazu gehören die Abrechnung von Zeit und Aufwand des Personals sowie die Bereitstellung von Rechenressourcen und die Lizenzierung von Software für die neue Umgebung. • Das Cloud-basierte Preismodell von Cloudera bietet Ihnen die Flexibili tät, die Vorteile von Bursting- und automatischen Skalierungsfunktionen zu nutzen. Weitere Informati onen finden Sie unter CDP Public Cloud-Servicetarife auf der Cloudera-Website. • Cloudera Enterprise Data Hub basiert auf Amazon Elastic Compute Cloud (Amazon EC2) und bildet traditionelle Cluster eng ab. Data Hub kann angepasst werden, was sich jedoch auf die Kosten auswirken wird. • CDP Public Cloud Data Warehouse, Cloudera Machine Learning und Cloudera Data Engineering (CDE) sind containerbasiert

		und können so konfiguriert werden, dass sie automatisch skalieren.
	Systemanforderungen	Weitere Informationen finden Sie im Abschnitt Voraussetzungen.
Infrastrukturvereinbarungen und Rahmenbedingungen	SLA	Weitere Informationen finden Sie unter Cloudera Service Level Agreement für CDP Public Cloud.
	DR	Weitere Informationen finden Sie in der Cloudera-Dokumentation unter Disaster Recovery.
	Lizenz- und Betriebsmodell (für AWS-Zielkonto)	Modell „Bring Your Own License“ (BYOL)
Compliance	Anforderungen an Sicherheit	Weitere Informationen finden Sie in der Cloudera-Dokumentation im Überblick über die Cloudera-Sicherheit.
	Andere Compliance-Zertifizierungen	Informationen zur Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO) und zum CDP Trust Center finden Sie auf der Cloudera-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS-Kontoanforderungen, einschließlich Konten, Ressourcen, Services und Berechtigungen, z. B. Einrichtung von Rollen und Richtlinien für AWS Identity and Access Management (IAM)

- Voraussetzungen für die Bereitstellung von CDP über die Cloudera-Website

Die Migration erfordert die folgenden Rollen und Fachkenntnisse:

Rolle	Fähigkeiten und Verantwortlichkeiten
Führung im Bereich Migration	Sorgt für die Unterstützung der Geschäfts leitung, die Zusammenarbeit, Planung, Implementierung und Bewertung im Team
Cloudera KMU	Fachkenntnisse in den Bereichen CDH-, HDP- und CDP-Administration, Systemadministration und Architektur
AWS-Architekt	Kenntnisse in AWS-Services, Netzwerken, Sicherheit und Architekturen

Architektur

Der Aufbau der geeigneten Architektur ist ein entscheidender Schritt, um sicherzustellen, dass Migration und Leistung Ihren Erwartungen entsprechen. Damit Ihre Migrationsbemühungen die Annahmen dieses Playbooks erfüllen, muss Ihre Zieldatenumgebung in der AWS-Cloud, entweder auf gehosteten Virtual Private Cloud (VPC) -Instances oder CDP, in Bezug auf Betriebssystem- und Softwareversionen sowie wichtige Maschinenspezifikationen Ihrer Quellumgebung entsprechen.

Das folgende Diagramm (mit freundlicher Genehmigung aus dem Cloudera Shared Data Experience-Datenblatt wiedergegeben) zeigt die Infrastrukturkomponenten für die CDP-Umgebung und wie die Stufen oder Infrastrukturkomponenten interagieren.

Die Architektur umfasst die folgenden CDP-Komponenten:

- Data Hub ist ein Dienst zum Starten und Verwalten von Workload-Clustern, der von Cloudera Runtime unterstützt wird. Sie können die Clusterdefinitionen in Data Hub verwenden, um Workload-Cluster für benutzerdefinierte Anwendungsfälle bereitzustellen und auf sie zuzugreifen und benutzerdefinierte Clusterkonfigurationen zu definieren. Weitere Informationen finden Sie auf der Cloudera-Website.

- Data Flow and Streaming befasst sich mit den wichtigsten Herausforderungen, mit denen Unternehmen bei der Übertragung von Daten konfrontiert sind. Es verwaltet Folgendes:
  - Verarbeitung von Echtzeit-Datenstreaming mit hohem Volumen und großem Umfang
  - Verfolgung der Herkunft und Herkunft von Streaming-Daten
  - Verwaltung und Überwachung von Edge-Anwendungen und Streaming-Quellen

  Weitere Informationen finden Sie unter Cloudera DataFlow und CSP auf der Cloudera-Website.
- Data Engineering umfasst Datenintegration, Datenqualität und Datenverwaltung, die Unternehmen beim Aufbau und der Pflege von Daten-Pipelines und Workflows unterstützen. Weitere Informationen finden Sie auf der Cloudera-Website. Erfahren Sie mehr über die Unterstützung für Spot-Instances, um Kosteneinsparungen bei AWS for Cloudera Data Engineering-Workloads zu ermöglichen.
- Mit Data Warehouse können Sie unabhängige Data Warehouses und Data Marts einrichten, die automatisch skaliert werden, um den Workload-Anforderungen gerecht zu werden. Dieser Service bietet isolierte Recheninstanzen und automatisierte Optimierung für jedes Data Warehouse und jeden Data Mart und hilft Ihnen, Kosten zu sparen und gleichzeitig SLAs einzuhalten. Weitere Informationen finden Sie auf der Cloudera-Website. Erfahren Sie mehr über Kostenmanagement und auto-scaling für Cloudera Data Warehouse auf AWS.
- Die Betriebsdatenbank in CDP bietet eine zuverlässige und flexible Grundlage für skalierbare Hochleistungsanwendungen. Sie bietet eine jederzeit verfügbare, skalierbare Echtzeitdatenbank, die traditionelle strukturierte Daten zusammen mit neuen, unstrukturierten Daten auf einer einheitlichen Betriebs- und Warehousing-Plattform bereitstellt. Weitere Informationen finden Sie auf der Cloudera-Website.
- Machine Learning ist eine Cloud-native Plattform für maschinelles Lernen, die Self-Service-Funktionen für Datenwissenschaft und Datentechnik zu einem einzigen, portablen Service innerhalb einer Unternehmensdatencloud zusammenführt. Sie ermöglicht den skalierbaren Einsatz von maschinellem Lernen und künstlicher Intelligenz (KI) für Daten an jedem beliebigen Ort. Weitere Informationen finden Sie auf der Cloudera-Website.

CDP auf AWS

Das folgende Diagramm (mit freundlicher Genehmigung der Cloudera-Website angepasst) zeigt die High-Level-Architektur von CDP auf AWS. CDP implementiert ein eigenes Sicherheitsmodell, um sowohl Konten als auch den Datenfluss zu verwalten. Diese werden mithilfe von kontenübergreifenden Rollen in IAM integriert.

Die CDP-Steuerebene befindet sich in einem Cloudera-Master-Konto in einer eigenen VPC. Jedes Kundenkonto hat sein eigenes Unterkonto und eine eigene VPC. Kontoübergreifende IAM-Rollen und SSL-Technologien leiten den Verwaltungsdatenverkehr zur und von der Steuerungsebene an Kundenservices weiter, die sich in öffentlichen Subnetzen befinden, die über das Internet routbar sind, innerhalb jeder Kunden-VPC. Auf der VPC des Kunden bietet die Cloudera Shared Data Experience (SDX) unternehmensweite Sicherheit mit einheitlicher Governance und Compliance, sodass Sie schneller Erkenntnisse aus Ihren Daten gewinnen können. SDX ist eine Designphilosophie, die in alle Cloudera-Produkte integriert ist. Weitere Informationen zu SDX und der CDP Public Cloud-Netzwerkarchitektur für AWS finden Sie in der Cloudera-Dokumentation.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Automatisierung und Tools

- Für zusätzliche Tools können Sie Cloudera Backup Data Recovery (BDR), AWS Snowball und AWS Snowmobile verwenden, um Daten von lokalen CDH, HDP und CDP auf AWS-gehostete CDP zu migrieren.
- Für neue Bereitstellungen empfehlen wir, die AWS-Partnerlösung für CDP zu verwenden.

Epics

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Binden Sie das Cloudera-Team ein.	Cloudera verfolgt ein standardisiertes Kooperationsmodell mit seinen Kunden und kann mit Ihrem Systemintegrator (SI) zusammenarbeiten, um denselben Ansatz zu fördern. Wenden Sie sich an das Cloudera-Kundenteam, damit es Ihnen mit Rat und Tat zur Seite steht und Ihnen die notwendigen technischen Ressourcen für den Start des Projekts zur Verfügung stellt. Durch die Kontaktaufnahme mit dem Cloudera-Team wird sichergestellt, dass sich alle erforderlichen Teams auf die Migration vorbereiten können, wenn der Termin näher rückt. Sie können sich an Cloudera Professional Services wenden, um Ihre Cloudera-Implementierung schnell, zu geringeren Kosten und mit Spitzenleistung von der Pilotphase zur Produktion zu überführen. Eine vollständige Liste der Angebote finden Sie auf der Cloudera-Website.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CDP Public Cloud-Umgebung auf AWS für Ihre VPC.	Arbeiten Sie mit Cloudera Professional Services oder Ihrem SI zusammen, um CDP Public Cloud in einer VPC auf AWS zu planen und bereitzustellen.	Cloud-Architekt, Cloudera SME

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Priorisieren und bewerten Sie die zu migrierenden Workloads.	Bewerten Sie alle Ihre lokalen Workloads, um herauszufinden, welche Workloads am einfachsten zu migrieren sind. Anwendungen, die nicht geschäftskritisch sind, sollten am besten zuerst verschoben werden, da sie nur minimale Auswirkungen auf Ihre Kunden haben werden. Speichern Sie die geschäftskritischen Workloads zum Schluss, nachdem Sie andere Workloads erfolgreich migriert haben. Hinweis: Transiente Workloads (CDP Data Engineering) lassen sich einfacher migrieren als persistente Workloads (CDP Data Warehouse). Es ist auch wichtig, bei der Migration das Datenvolumen und die Standorte zu berücksichtigen. Zu den Herausforderungen können die kontinuierliche Replikation von Daten aus einer lokalen Umgebung in die Cloud und die Änderung der Datenerfassungspipelines gehören, um Daten direkt in die Cloud zu importieren.	Leitung der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erörtern Sie Aktivitäten zur Migration von CDH, HDP, CDP und Legacy-An wendungen.	Erwägen Sie mit Cloudera Workload Manager die folgenden Aktivitäten und beginnen Sie mit der Planung: • Daten und Workloads zum Kopieren in Ihre AWS-Umgebung • Cloud-fähige Daten • Laute Nachbarn, die Ressourcen verbrauch en und anderen Mietern Probleme bereiten • Elastische Workloads • Kleine Cluster mit hohem Betriebsaufwand	Leitung der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfüllen Sie die Anforderungen und Empfehlungen von Cloudera Replication Manager.	Arbeiten Sie mit Cloudera Professional Services und Ihrem SI zusammen, um die Migration von Workloads in Ihre CDP Public Cloud-Umgebung auf AWS vorzubereiten. Wenn Sie die folgenden Anforderungen und Empfehlungen kennen, können Sie häufig auftretende Probleme während und nach der Installation des Replication Manager-Service vermeiden. • Überprüfen Sie anhand der Begleitdokumente zu Replication Manager, ob Sie die Umgebungs- und Systemanforderungen erfüllen. Weitere Informationen finden Sie unter Supportmatrix für CDP Public Cloud Replication Manager auf der Cloudera-Website. • Sie benötigen keinen Root-Zugriff auf die Knoten, auf denen die Replication Manager App und die Data Lifecycle Manager (DLM) -Engine installiert werden. • Installieren Sie Apache Hive während der Erstinstallation von Replication Manager,	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sofern Sie nicht sicher sind, dass Sie die Hive-Replikation in future nicht mehr verwenden werden. Wenn Sie Hive installieren möchten, nachdem Sie HDFS-Replikationsrichtlinien in Replication Manager erstellt haben, müssen Sie alle HDFS-Replikationsrichtlinien löschen und anschließend neu erstellen, nachdem Sie Hive hinzugefügt haben. • In Replication Manager verwendete Cluster müssen symmetrische Konfigurationen haben. Jeder Cluster in einer Replikationsbeziehung muss in Bezug auf Sicherheit (Kerberos), Benutzerverwaltung (LDAP/AD) und Knox Proxy exakt gleich konfiguriert sein. Clusterdienste wie Hadoop Distributed File System (HDFS), Apache Hive, Apache Knox, Apache Ranger und Apache Atlas können unterschiedliche Konfigurationen für Hochverfügbarkeit (HA) haben. Quell- und Zielcluster können beispielsweise	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	separate HA- und Nicht-HA-Konfigurationen haben.	

CDP zu AWS migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie den ersten Workload für Entwicklungs-/Testumgebungen mithilfe von Cloudera Workload Manager.	Ihr SI kann Ihnen helfen, Ihren ersten Workload in die AWS-Cloud zu migrieren. Dabei sollte es sich um eine Anwendung handeln, die nicht kundenorientiert oder geschäftskritisch ist. Ideale Kandidaten für die Dev/Test-Migration sind Anwendungen mit Daten, die die Cloud problemlos aufnehmen kann, wie z. B. CDP Data Engineering-Workloads. Dabei handelt es sich um eine vorübergehende Arbeitslast, auf die in der Regel weniger Benutzer zugreifen, im Vergleich zu einer dauerhaften Arbeitslast wie einer CDP Data Warehouse-Arbeitslast, auf die viele Benutzer ununterbrochenen Zugriff benötigen könnten. Data Engineering-Workloads sind nicht dauerhaft, wodurch die Auswirkungen auf das Geschäft minimiert werden,	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	falls etwas schief geht. Diese Aufgaben können jedoch für die Produktionsbericht erstattung von entscheidender Bedeutung sein. Priorisieren Sie daher zunächst Datenvera rbeitungs-Workloads mit geringen Auswirkungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wiederholen Sie die Migrationsschritte nach Bedarf.	Cloudera Workload Manager hilft bei der Identifizierung von Workloads, die sich am besten für die Cloud eignen. Er bietet Kennzahlen wie Cloud-Leistungsbewertungen, Größen-/Kapazitätspläne für die Zielumgebung und Replikationspläne. Die besten Kandidaten für eine Migration sind saisonale Workloads, Ad-hoc-Berichte und zeitweilige Jobs, die nicht viele Ressourcen verbrauchen. Cloudera Replication Manager verschiebt Daten von lokalen Standorten in die Cloud und von der Cloud in lokale Umgebungen. Optimieren Sie mithilfe von Workload Manager proaktiv Workloads, Anwendungen, Leistung und Infrastrukturkapazität für Data Warehousing, Data Engineering und maschinelles Lernen. Eine vollständige Anleitung zur Modernisierung eines Data Warehouse finden Sie auf der Cloudera-Website.	Cloudera SME

Zugehörige Ressourcen

Cloudera-Dokumentation:

- Registrierung klassischer Cluster bei CDP, Cloudera Manager und Replication Manager:
  - Management-Konsole
  - Replication Manager: Hive-Replikation
- Sentry-Replikation
- Sentry-Berechtigungen
- Checkliste für die Planung von Data Hub-Clustern
- Workload Manager-Architektur
- Anforderungen für Replication Manager
- Beobachtbarkeit der Cloudera-Datenplattform
- AWS-Anforderungen

AWS-Dokumentation:

- Cloud-Datenmigration

Starten Sie den AWS Replication Agent automatisch neu, ohne SELinux nach dem Neustart eines RHEL-Quellservers zu deaktivieren

Erstellt von Anil Kunapareddy (AWS), Shanmugam Shanker (AWS) und Venkatramana Chintha (AWS)

Umgebung: Produktion	Technologien: Migration; Betriebssysteme	Workload: Open-Source
AWS-Services: AWS Application Migration Service		

Übersicht

AWS Application Migration Service vereinfacht, beschleunigt und automatisiert die Migration Ihres Red Hat Enterprise Linux (RHEL)-Workloads in die Amazon Web Services (AWS) Cloud. Um Quellserver zum Application Migration Service hinzuzufügen, installieren Sie den AWS Replication Agent auf den Servern.

Application Migration Service bietet asynchrone Replikation auf Blockebene in Echtzeit. Das bedeutet, dass Sie den normalen IT-Betrieb während des gesamten Replikationsprozesses fortsetzen können. Für diese IT-Operationen müssen Sie möglicherweise Ihren RHEL-Quellserver während der Migration neu starten oder neu starten. In diesem Fall wird der AWS Replication Agent nicht automatisch neu gestartet und Ihre Datenreplikation wird beendet. In der Regel können Sie Security-Enhanced Linux (SELinux) auf den deaktivierten oder permissive nModus setzen, um AWS Replication Agent automatisch neu zu starten. Die Sicherheitsrichtlinien Ihrer Organisation verbieten jedoch möglicherweise die Deaktivierung von SELinux und Sie müssen Ihre Dateien möglicherweise auch umbenennen.

Dieses Muster beschreibt, wie Sie den AWS Replication Agent automatisch neu starten, ohne SELinux zu deaktivieren, wenn Ihr RHEL-Quellserver während einer Migration neu gestartet oder neu gestartet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein On-Premises-RHEL-Workload, den Sie in die AWS Cloud migrieren möchten.
- Application Migration Service wurde von der Application Migration Service-Konsole initialisiert. Die Initialisierung ist nur erforderlich, wenn Sie diesen Service zum ersten Mal verwenden. Anweisungen finden Sie in der Dokumentation zum Application Migration Service .
- Eine vorhandene AWS Identity and Access Management (IAM)-Richtlinie für Application Migration Service. Weitere Informationen finden Sie in der Dokumentation zum Application Migration Service .

Versionen

- RHEL Version 7 oder höher

Tools

AWS-Services

- AWS Application Migration Service ist eine hoch automatisierte lift-and-shift (Hostwechsel-)Lösung, die die Kosten für die Migration von Anwendungen zu AWS vereinfacht, beschleunigt und senkt.

Linux-Befehle

Die folgende Tabelle enthält eine Liste der Linux-Befehle, die Sie auf Ihrem RHEL-Quellserver ausführen werden. Diese werden auch in den Epics und Geschichteen für dieses Muster beschrieben.

Befehl	Beschreibung
`#systemctl –version`	Identifiziert die Systemversion.
`#systemctl list-units --type=service`	Listet alle aktiven Services auf, die auf dem RHEL-Server verfügbar sind.

`#systemctl list-units --type=service | grep running`	Listet alle Services auf, die derzeit auf dem RHEL-Server ausgeführt werden.
`#systemctl list-units --type=service | grep failed`	Listet alle Services auf, die nach dem Neustart oder Neustart des RHEL-Servers nicht geladen werden konnten.
`restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Ändert den Kontext in `aws-replication-service` .
`yum install policycoreutils*`	Installiert die Richtlinienkernprogramme, die für den Betrieb des SELinux-Systems erforderlich sind.
`ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Durchsucht das Audit-Protokoll und erstellt ein Modul für Richtlinien.
`semodule -i my-modprobe.pp`	Aktiviert die Richtlinie.
`cat my-modprobe.te`	Zeigt den Inhalt der `my-modprobe.te` Datei an.
`semodule -l | grep my-modprobe`	Prüft, ob die Richtlinie in das SELinux-Modul geladen wurde.

Polen

Installieren Sie den AWS Replication Agent und starten Sie den RHEL-Quellserver neu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Migration Service-Benutzer mit einem Zugriffsschlüssel und einem geheimen Zugriffsschlüssel.	Um den AWS Replication Agent zu installieren, müssen Sie einen Application Migration Service-Benutzer mit den erforderlichen AWS-Anmeldeinformationen erstellen. Anweisungen finden	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie in der Dokumentation zum Application Migration Service .	
Installieren Sie den AWS Replication Agent.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Migration Service-Konsole unter https://console.aws.amazon.com/mgn/home. 2. Konfigurieren Sie die Replikationseinstellungen, indem Sie den Anweisungen in der Application Migration Service-Dokumentation folgen. 3. Installieren Sie den AWS Replication Agent, indem Sie den Anweisungen in der Application Migration Service-Dokumentation folgen. 4. Wählen Sie auf der Seite Quellserver den RHEL-Quellserver und dann Replikation aus, um die erste Replikation zu starten. Weitere Informationen finden Sie in der Application Migration Service-Dokumentation.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den RHEL-Quellserver neu oder starten Sie ihn neu.	Starten Sie Ihren RHEL-Quellserver neu oder starten Sie ihn neu, wenn der Status der Datenreplikation im Migrations-Dashboard auf Zustand anzeigt.	Migrationsingenieur
Überprüfen Sie den Status der Datenreplikation.	Warten Sie eine Stunde und überprüfen Sie dann den Status der Datenreplikation im Migrations-Dashboard erneut. Er sollte sich im Status „Verharrt“ befinden.	Migrationsingenieur

Überprüfen des AWS Replication Agent-Status auf dem RHEL-Quellserver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Systemversion.	Öffnen Sie die Befehlszeilenschnittstelle für Ihren RHEL-Quellserver und führen Sie den folgenden Befehl aus, um die Systemversion zu identifizieren: `#systemctl –version`	Migrationsingenieur
Listet alle aktiven Services auf.	Um alle aktiven Services aufzulisten, die auf dem RHEL-Server verfügbar sind, führen Sie den Befehl aus: `#systemctl list-units --type=service`	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Listet alle laufenden Services auf.	Um alle Services aufzulisten, die derzeit auf dem RHEL-Server ausgeführt werden, verwenden Sie den Befehl : `#systemctl list-units --type=service | grep running`	Migrationsingenieur
Listen Sie alle Services auf, die nicht geladen werden konnten.	Um alle Services aufzulisten, die nach dem Neustart oder Neustart des RHEL-Servers nicht geladen werden konnten, führen Sie den Befehl aus: `#systemctl list-units --type=service | grep failed`	Migrationsingenieur

Erstellen und Ausführen des SELinux-Moduls

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie den Sicherheitskontext.	Führen Sie in der Befehlszeilenschnittstelle für Ihren RHEL-Quellserver den folgenden Befehl aus, um den Sicherheitskontext in den AWS-Replikationsservice zu ändern: `restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Core-Dienstprogramme.	Führen Sie den Befehl aus, um die Core-Dienstprogramme zu installieren, die für den Betrieb des SELinux-Systems und seiner Richtlinien erforderlich sind: `yum install policycoreutils*`	Migrationsingenieur
Durchsuchen Sie das Audit-Protokoll und erstellen Sie ein Modul für Richtlinien.	Führen Sie den Befehl aus: `ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Migrationsingenieur
Zeigen Sie den Inhalt der my-modprobe-te Datei an.	Die `my-modprobe.te` Datei wird mit dem Befehl audit2allow generiert. Sie enthält die SELinux-Domains, das Richtlinienquellverzeichnis und die Unterverzeichnisse und gibt die Zugriffsvektorregeln und Übergänge an, die den Domains zugeordnet sind. Führen Sie den Befehl aus, um den Inhalt der Datei anzuzeigen: `cat my modprobe.te`	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Richtlinie.	Um das Modul einzufügen und das Richtlinienpaket aktiv zu machen, führen Sie den Befehl aus: `semodule -i my-modpro be.pp`	Migrationsingenieur
Überprüfen Sie, ob das Modul geladen wurde.	Führen Sie den Befehl aus: `semodule -l | grep my-modprobe` Nachdem das SELinux-M odul geladen wurde, müssen Sie SELinux während Ihrer Migration nicht mehr auf deaktivierten oder permissive nModus setzen.	Migrationsingenieur
Starten Sie den RHEL-Quel lserver neu oder starten Sie ihn neu und überprüfen Sie den Status der Datenrepl ikation.	Öffnen Sie die AWS Migration Service-Konsole, navigiere n Sie zu Fortschritt der Datenreplikation und starten Sie dann Ihren RHEL-Quel lserver neu oder starten Sie ihn neu. Die Datenrepl ikation sollte jetzt automatisch fortgesetzt werden, nachdem der RHEL-Quellserver neu gestartet wurde.	Migrationsingenieur

Zugehörige Ressourcen

- Dokumentation zum Application Migration Service

- Technische Trainingsmaterialien
- Fehlerbehebung bei AWS Replication Agent-Problemen
- Richtlinien für Application Migration Service

Re-Architekt

Themen

- Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren einer Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB mithilfe von AWS DMS und AWS SCT
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe eines Oracle-Bystanders und AWS DMS
- Migrieren von Oracle Database zu Amazon RDS for PostgreSQL mithilfe von Oracle GoldenGate
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mit AWS DMS und AWS SCT
- Migrieren von Daten aus einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren von SAP ASE zu Amazon RDS for SQL Server mit AWS DMS
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mit AWS DMS
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie eine lokale Vertica-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren älterer Anwendungen von Oracle Pro*C zu ECPG
- Migrieren von virtuell generierten Spalten von Oracle zu PostgreSQL
- Einrichten der Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL – kompatibel
- Validieren von Datenbankobjekten nach der Migration von Oracle zu Amazon Aurora PostgreSQL

Konvertieren des Datentyps VARCHAR2(1) für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL

Erstellt von Bolesh Damera (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: Amazon Aurora PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Softwareentwicklung und -tests; Speicher und Backup; Datenbanken
AWS-Services: Amazon Aurora; AWS DMS; Amazon RDS; AWS SCT		

Übersicht

Während einer Migration von Amazon Relational Database Service (Amazon RDS) für Oracle zu Amazon Aurora PostgreSQL – kompatible Edition kann es bei der Validierung der Migration in Amazon Web Services (AWS) Database Migration Service (AWS DMS) zu Datenkonflikten kommen. Um diese Nichtübereinstimmung zu vermeiden, können Sie den Datentyp VARCHAR2(1) in den booleschen Datentyp konvertieren.

Der Datentyp VARCHAR2 speichert Textzeichenfolgen variabler Länge, und VARCHAR2(1) gibt an, dass die Zeichenfolge 1 Zeichen oder 1 Byte lang ist. Weitere Informationen zu VARCHAR2 finden Sie unter In Oracle integrierte Datentypen (Oracle-Dokumentation).

In diesem Muster sind die VARCHAR2(1)-Daten in der Spalte der Beispiel-Quelldatentabelle entweder ein Y fürJa oder N für Nein. Dieses Muster enthält Anweisungen zur Verwendung von AWS DMS und AWS Schema Conversion Tool (AWS SCT), um diesen Datentyp von den Y- und N-Werten in VARCHAR2(1) in wahre oder falsche Werte in Boolean zu konvertieren.

Zielgruppe

Dieses Muster wird für diejenigen empfohlen, die Erfahrung mit der Migration von Oracle-Datenbanken zu Aurora PostgreSQL haben – kompatibel mit AWS DMS. Halten Sie sich bei

Abschluss der Migration an die Empfehlungen unter Konvertieren von Oracle zu Amazon RDS für PostgreSQL oder Amazon Aurora PostgreSQL (AWS-SCT-Dokumentation).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vergewissern Sie sich, dass Ihre Umgebung für Aurora vorbereitet ist, einschließlich der Einrichtung von Anmeldeinformationen, Berechtigungen und einer Sicherheitsgruppe. Weitere Informationen finden Sie unter Einrichten Ihrer Umgebung für Amazon Aurora (Aurora-Dokumentation).
- Eine Quelldatenbank von Amazon RDS für Oracle, die eine Tabellenspalte mit VARCHAR2(1)-Daten enthält.
- Eine Amazon Aurora PostgreSQL-kompatible Zieldatenbank-Instance. Weitere Informationen finden Sie unter Erstellen eines Datenbank-Clusters und Herstellen einer Verbindung mit einer Datenbank in einem Aurora-PostgreSQL-Datenbank-Cluster (Aurora-Dokumentation).

Produktversionen

- Amazon RDS für Oracle Version 12.1.0.2 oder höher.
- AWS DMS Version 3.1.4 oder höher. Weitere Informationen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS (AWS-DMS-Dokumentation). Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden.
- AWS Schema Conversion Tool (AWS SCT) Version 1.0.632 oder höher. Wir empfehlen Ihnen, die neueste Version von AWS SCT für die umfassendste Versions- und Funktionsunterstützung zu verwenden.
- Aurora unterstützt die PostgreSQL-Versionen, die unter Database Engine Versions for Aurora PostgreSQL -Compatible (Aurora-Dokumentation) aufgeführt sind.

Architektur

Quelltechnologie-Stack

Datenbank-Instance von Amazon RDS für Oracle

Zieltechnologie-Stack

Amazon Aurora PostgreSQL – Kompatible Datenbank-Instance

Quell- und Zielarchitektur

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Andere -Services

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht. In diesem Muster verwenden Sie dieses Tool, um eine Verbindung mit der Datenbank-Instance von Amazon RDS für Oracle herzustellen und die Daten abzufragen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können. In diesem Muster verwenden Sie dieses Tool, um eine Verbindung mit der Aurora-Datenbank-Instance herzustellen und die Daten abzufragen.

Polen

Vorbereiten der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Bericht zur Datenbankmigration.	1. Erstellen Sie in AWS SCT einen Bewertungsbericht zur Datenbankmigration . Weitere Informationen finden Sie unter Erstellen von Migrationsbewertungsberichten. 2. Überprüfen und führen Sie die Maßnahmen im Bewertungsbericht der Migration aus. Weitere Informationen finden Sie unter Bewertungsbericht-Aktionselemente.	DBA, Entwickler
Deaktivieren Sie Fremdschlüsseleinschränkungen in der Zieldatenbank.	In PostgreSQL werden Fremdschlüssel mithilfe von Auslösern implementiert. Während der Volllastphase lädt AWS DMS jede Tabelle einzeln. Wir empfehlen dringend, Fremdschlüsseleinschränkungen während eines Volllastvorgangs mit einer der folgenden Methoden zu deaktivieren: • Deaktivieren Sie vorübergehend alle Auslöser aus der Instance und beenden	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den vollständigen Ladevorgang. • Verwenden Sie den `session_replicatio n_role` -Parameter in PostgreSQL. Wenn das Deaktivieren von Fremdschlüsseleinschränkung en nicht möglich ist, erstellen Sie eine AWS DMS-Migra tionsaufgabe für die Primärdat en, die für die übergeordnete Tabelle und die untergeor dnete Tabelle spezifisch ist.	

Deaktivieren Sie die Primärsch lüssel und eindeutigen Schlüssel in der Zieldaten bank.	Deaktivieren Sie mit den folgenden Befehlen die Primärschlüssel und Einschränkungen für die Zieldatenbank. Dies trägt dazu bei, die Leistung der ersten Ladeaufgabe zu verbessern.
	
	`ALTER TABLE <table> DISABLE PRIMARY KEY;`
	
	`ALTER TABLE <table> DISABLE CONSTRAINT <constraint_name>;`
		DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erste Ladeaufgabe.	Erstellen Sie in AWS DMS die Migrationsaufgabe für den ersten Ladevorga ng. Anweisungen finden Sie unter Erstellen einer Aufgabe. Wählen Sie für die Migrationsmethode Migrieren vorhandener Daten aus. Diese Migrationsmethode wird `Full Load` in der -API aufgerufe n. Starten Sie diese Aufgabe noch nicht.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Aufgabeneinstellungen für die erste Ladeaufgabe.	Bearbeiten Sie die Aufgabeneinstellungen, um eine Datenvalidierung hinzuzufügen. Diese Validierungseinstellungen müssen in einer JSON-Datei erstellt werden. Anweisungen und Beispiele finden Sie unter Angeben von Aufgabeneinstellungen. Fügen Sie die folgenden Validierungen hinzu: • Um zu überprüfen, ob die VARCHAR2(1)-Daten in der Zieldatenbank genau in boolesche Werte konvertiert wurden, fügen Sie den Code im Datenvalidierungsskript im Abschnitt Zusätzliche Informationen dieses Musters hinzu. Das Validierungsskript konvertiert die booleschen Werte 1 in Y und 0 in N in der Zieltabelle und vergleicht dann die Werte in der Zieltabelle mit der Quelltabelle. Um den Rest der Datenmigration zu überprüfen, aktivieren Sie die Datenvalidierung in der Aufgabe. Weitere Informationen finden Sie unter Einstellu	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ngen für Datenvalidierungsa ufgaben.	
Erstellen Sie die laufende Replikationsaufgabe.	Erstellen Sie in AWS DMS die Migrationsaufgabe, die die Zieldatenbank mit der Quelldatenbank synchron hält. Anweisungen finden Sie unter Erstellen einer Aufgabe. Wählen Sie für die Migration smethode Nur Datenände rungen replizieren aus. Starten Sie diese Aufgabe noch nicht.	DBA

Testen der Migrationsaufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Beispieldaten für Tests.	Erstellen Sie in der Quelldate nbank zu Testzwecken eine Beispieltabelle mit Daten.	Developer
Vergewissern Sie sich, dass es keine widersprüchlichen Aktivitäten gibt.	Verwenden Sie die `pg_stat_activity` , um nach Aktivitäten auf dem Server zu suchen, die sich auf die Migration auswirken könnten. Weitere Informati onen finden Sie unter Der Statistikkollektor (PostgreSQL-Dokumentation).	AWS-Administrator
Starten Sie die AWS DMS-Migrationsaufgaben.	Starten Sie in der AWS DMS-Konsole auf der Seite Dashboard die ersten Lade-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und laufenden Replikati onsaufgaben, die Sie im vorherigen Epi erstellt haben.	
Überwachen Sie die Aufgaben und den Tabellenladestatus.	Überwachen Sie während der Migration den Aufgabens tatus und die Tabelle mit dem Status . Wenn der erste Ladevorgang abgeschlo ssen ist, gehen Sie auf der Registerkarte Tabellens tatistiken wie folgt vor: • Der Ladestatus sollte Tabelle abgeschlossen lauten. • Der Validierungsstatus sollte Validiert sein.	AWS-Administrator
Überprüfen Sie die Migration sergebnisse.	Fragen Sie mit pgAdmin die Tabelle in der Zieldatenbank ab. Eine erfolgreiche Abfrage zeigt an, dass die Daten erfolgreich migriert wurden.	Developer
Fügen Sie Primärschlüssel und Fremdschlüssel in der Zieldatenbank hinzu.	Erstellen Sie den Primärsch lüssel und den Fremdschl üssel in der Zieldatenbank. Weitere Informationen finden Sie unter ALTER TABLE (PostgreSQL-Website).	DBA
Bereinigen Sie die Testdaten.	Bereinigen Sie in den Quell- und Zieldatenbanken Daten, die für Einheitentests erstellt wurden.	Developer

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Migration ab.	Wiederholen Sie die vorherige Ausgabe, Testen der Migration saufgaben unter Verwendun g der echten Quelldaten. Dadurch werden die Daten von der Quelle zur Zieldaten bank migriert.	Developer
Überprüfen Sie, ob die Quell- und Zieldatenbanken synchron sind.	Überprüfen Sie, ob die Quell- und Zieldatenbanken synchron sind. Weitere Informationen und Anweisungen finden Sie unter AWS DMS-Daten validierung.	Developer
Halten Sie die Quelldatenbank an.	Halten Sie die Datenbank von Amazon RDS für Oracle an. Anweisungen finden Sie unter Temporäres Anhalten einer Amazon RDS-DB-Instance. Wenn Sie die Quelldatenbank beenden, werden das erste Laden und die laufenden Replikationsaufgaben in AWS DMS automatisch gestoppt. Zum Stoppen dieser Aufgaben sind keine zusätzlichen Maßnahmen erforderlich.	Developer

Zugehörige Ressourcen

AWS-Referenzen

- Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mit AWS DMS und AWS SCT (AWS Prescriptive Guidance)
- Konvertieren von Oracle in Amazon RDS für PostgreSQL oder Amazon Aurora PostgreSQL (AWS-SCT-Dokumentation)
- Funktionsweise von AWS DMS (AWS-DMS-Dokumentation)

Andere Referenzen

- Boolescher Datentyp (PostgreSQL-Dokumentation)
- In Oracle integrierte Datentypen (Oracle-Dokumentation)
- pgAdmin (pgAdmin-Website)
- SQL Developer (Oracle-Website)

Tutorial und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- Einführung in AWS DMS (Video)
- Grundlegendes zu Amazon RDS (Video)

Zusätzliche Informationen

Datenvalidierungsskript

Das folgende Datenvalidierungsskript konvertiert 1 in Y und 0 in N . Dies hilft der AWS DMS-Aufgabe dabei, die Tabellenvalidierung erfolgreich abzuschließen und zu bestehen.

```
{
"rule-type": "validation",
"rule-id": "5",
"rule-name": "5",
"rule-target": "column",
"object-locator": {
"schema-name": "ADMIN",
"table-name": "TEMP_CHRA_BOOL",
"column-name": "GRADE"
},
```

```
"rule-action": "override-validation-function",
"target-function": "case grade when '1' then 'Y' else 'N' end"
        }
```

Die -`case`Anweisung im Skript führt die Validierung durch. Wenn die Validierung fehlschlägt, fügt AWS DMS einen Datensatz in die Tabelle public.awsdms_validation_failures_v1 in der Zieldatenbank-Instance ein. Dieser Datensatz enthält den Tabellennamen, die Fehlerzeit und Details zu den nicht übereinstimmenden Werten in den Quell- und Zieltabellen.

Wenn Sie dieses Datenvalidierungsskript nicht zur AWS DMS-Aufgabe hinzufügen und die Daten in die Zieltabelle eingefügt werden, zeigt die AWS DMS-Aufgabe den Validierungsstatus als Nicht übereinstimmende Datensätze an.

Während der AWS SCT-Konvertierung ändert die AWS DMS-Migrationsaufgabe den Datentyp des VARCHAR2(1)-Datentyps in Boolean und fügt der `''N0''` Spalte eine Primärschlüsseleinschränkung hinzu.

Erstellen von Anwendungsbenutzern und -rollen in Aurora PostgreSQL – kompatibel

Erstellt von Abhishek Verma (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Beliebige Datenbank	Ziel: PostgreSQL-Datenbank
R-Typ: Neuarchitektur	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS; Amazon Aurora		

Übersicht

Wenn Sie zu Amazon Aurora PostgreSQL -kompatible Edition migrieren, müssen die Datenbankbenutzer und -rollen, die in der Quelldatenbank vorhanden sind, in der Aurora PostgreSQL -kompatiblen Datenbank erstellt werden. Sie können die Benutzer und Rollen in Aurora PostgreSQL – kompatibel erstellen, indem Sie zwei verschiedene Ansätze verwenden:

- Verwenden Sie ähnliche Benutzer und Rollen im Ziel wie in der Quelldatenbank. Bei diesem Ansatz werden die Datendefinitionssprachen (DDLs) für Benutzer und Rollen aus der Quelldatenbank extrahiert. Anschließend werden sie transformiert und auf die Aurora-PostgreSQL-kompatible Zieldatenbank angewendet. Der Blogbeitrag Verwenden von SQL zum Zuordnen von Benutzern, Rollen und Erteilungen von Oracle zu PostgreSQL behandelt beispielsweise die Extraktion aus einer Oracle-Quelldatenbank-Engine.
- Verwenden Sie standardisierte Benutzer und Rollen, die häufig während der Entwicklung, Verwaltung und Ausführung anderer verwandter Vorgänge in der Datenbank verwendet werden. Dazu gehören schreibgeschützte, Lese-/Schreib-, Entwicklungs-, Verwaltungs- und Bereitstellungsvorgänge, die von den jeweiligen Benutzern ausgeführt werden.

Dieses Muster enthält die Erteilungen, die für die Erstellung von Benutzern und Rollen in Aurora PostgreSQL erforderlich sind – kompatibel für den standardisierten Benutzer- und Rollenansatz. Die Schritte zur Erstellung von Benutzern und Rollen sind auf die Sicherheitsrichtlinie der Gewährung der

geringsten Berechtigungen für die Datenbankbenutzer abgestimmt. In der folgenden Tabelle sind die Benutzer, ihre entsprechenden Rollen und ihre Details zur Datenbank aufgeführt.

Benutzer	Rollen	Zweck
`APP_read`	`APP_RO`	Wird für den schreibge schützten Zugriff auf das Schema verwendet `APP`
`APP_WRITE`	`APP_RW`	Wird für Schreib- und Lesevorgänge im Schema verwendet `APP`
`APP_dev_user`	`APP_DEV`	Wird für den Entwicklu ngszweck im Schema `APP_DEV`mit schreibge schütztem Zugriff auf das Schema verwendet `APP`
`Admin_User`	`rds_superuser`	Wird zum Ausführen von Administratoroperationen in der Datenbank verwendet
`APP`	`APP_DEP`	Wird zum Erstellen der Objekte unter dem `APP` Schema und für die Bereitste llung von Objekten im `APP` Schema verwendet

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto
- Eine PostgreSQL-Datenbank, eine Datenbank von Amazon Aurora PostgreSQL -kompatible Edition oder eine Datenbank von Amazon Relational Database Service (Amazon RDS) für PostgreSQL

Produktversionen

- Alle Versionen von PostgreSQL

Architektur

Quelltechnologie-Stack

- Jede Datenbank

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL – kompatibel

Zielarchitektur

Das folgende Diagramm zeigt Benutzerrollen und die Schemaarchitektur in der Aurora-PostgreSQL-kompatiblen Datenbank.

Automatisierung und Skalierung

Dieses Muster enthält die Benutzer, Rollen und das Schemaerstellungsskript, das Sie mehrmals ausführen können, ohne dass dies Auswirkungen auf bestehende Benutzer der Quell- oder Zieldatenbank hat.

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.

Andere -Services

- psql ist ein Terminal-basiertes Frontend-Tool, das bei jeder PostgreSQL-Datenbankinstallation installiert wird. Es verfügt über eine Befehlszeilenschnittstelle zum Ausführen von SQL-, PL-PGSQL- und Betriebssystembefehlen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.

Polen

Erstellen der Benutzer und Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Bereitstellungsbenutzer.	Der Bereitstellungsbenutzer APP wird verwendet, um die Datenbankobjekte während Bereitstellungen zu erstellen und zu ändern. Verwenden Sie die folgenden Skripts, um die Bereitstellungsbenutzerrolle APP_DEP im Schema zu erstellenAPP. Überprüfen Sie die Zugriffsrechte, um sicherzustellen, dass dieser Benutzer nur über die Berechtigung zum Erstellen von Objekten im erforderlichen Schema verfügtAPP. 1. Stellen Sie eine Verbindung mit dem Administratorbenutzer her und erstellen Sie das Schema. `CREATE SCHEMA APP;` 2. Erstellen Sie den Benutzer.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>CREATE USER APP WITH
	 PASSWORD <password
	> ;</pre>
	3. Erstellen Sie die -Rolle.
	<pre>CREATE ROLE APP_DEP ;
	GRANT all on schema
	 APP to APP_DEP ;
	GRANT USAGE ON SCHEMA
	 APP to APP_DEP ;
	GRANT connect on
	 database <db_name>
	 to APP_DEP ;
	GRANT APP_DEP to APP;</pre>
	4. Um die Berechtigungen zu testen, stellen Sie eine Verbindung zu her APP und erstellen Sie die Tabellen.
	<pre>set search_path to
	 APP;
	SET
	CREATE TABLE test(id
	 integer) ;
	CREATE TABLE</pre>
	5. Überprüfen Sie die Berechtigungen.
	<pre>select schemaname ,
	 tablename , tableowne
	r from pg_tables
	 where tablename like
	 'test' ;
	schemaname
	
		tablename |
		 tableowner</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`APP | test | APP`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den schreibge schützten Benutzer.	Der schreibgeschützte Benutzer `APP_read` wird für die Ausführung der schreibge schützten Operation im Schema verwendet`APP`. Verwenden Sie die folgenden Skripts, um den schreibge schützten Benutzer zu erstellen. Überprüfen Sie die Zugriffsrechte, um sicherzus tellen, dass dieser Benutzer nur über die Berechtigung verfügt, die Objekte im Schema zu lesen `APP` und Lesezugriff für alle neuen Objekte, die im Schema erstellt wurden, automatisch zu gewähren`APP`.
	
	1. Erstellen Sie den Benutzer `APP_read`.
	
	`create user APP_read ; alter user APP_read with password 'your_password' ;`
	
	2. Erstellen Sie die -Rolle.
	
	`CREATE ROLE APP_ro ; GRANT SELECT ON ALL TABLES IN SCHEMA APP TO APP_RO ; GRANT USAGE ON SCHEMA APP TO APP_RO`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>GRANT CONNECT ON
	 DATABASE testdb TO
	 APP_RO ;
	GRANT APP_RO TO
	 APP_read;</pre>
	3. Um die Berechtigungen zu testen, melden Sie sich mit dem -APP_readBenutzer an.
	<pre>set search_path to
	 APP ;
	create table test1(id
	 integer) ;
	ERROR: permission
	 denied for schema APP
	LINE 1: create table
	 test1(id integer) ;
	insert into test
	 values (34) ;
	ERROR: permission
	 denied for table test
	 SQL state: 42501
	select from test
	no rows selected</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Lese-/Schreibbenutzer.	Der Lese-/Schreibbenutzer `APP_WRITE` wird verwendet, um Lese- und Schreibvorgänge für das Schema durchzuführen`APP`. Verwenden Sie die folgenden Skripts, um den Lese-/Schreibbenutzer zu erstellen und ihm die `APP_RW` Rolle zu gewähren. Überprüfen Sie die Zugriffsrechte, um sicherzustellen, dass dieser Benutzer nur Lese- und Schreibrechte für die Objekte im Schema hat APP und dass er automatisch Lese- und Schreibzugriff für jedes neue Objekt gewährt, das im Schema erstellt wurde`APP`.
	
	1. Erstellen Sie den Benutzer.
	
	`CREATE USER APP_WRITE ; alter user APP_WRITE with password 'your_password' ;`
	
	2. Erstellen Sie die -Rolle.
	
	`CREATE ROLE APP_RW; GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA APP TO APP_RW ;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>GRANT CONNECT ON
	 DATABASE postgres to
	 APP_RW ;
	GRANT USAGE ON SCHEMA
	 APP to APP_RW ;
	ALTER DEFAULT
	 PRIVILEGES IN SCHEMA
	 APP
	GRANT SELECT, INSERT,
	 UPDATE, DELETE ON
	 TABLES TO APP_RW ;
	GRANT APP_RW to
	 APP_WRITE</pre>	

	3. Um die Berechtigungen zu testen, melden Sie sich mit dem -APP_WRITE Benutzer an.
	
	<pre>SET SEARCH_PATH to
	 APP;
	CREATE TABLE
	 test1(id integer) ;
	ERROR: permission
	 denied for schema APP
	LINE 1: create table
	 test1(id integer) ;
	SELECT * FROM test ;
	id
	---- 	
	12
	INSERT INTO test
	 values (31) ;
	INSERT 0 1</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Admin-Benutzer.	Der Admin-Benutzer `Admin_User` wird verwendet, um Admin-Operationen in der Datenbank durchzuführen. Beispiele für diese Operationen sind `CREATE ROLE` und `CREATE DATABASE`. `Admin_User` verwendet die integrierte Rolle, `rds_superuser` um Admin-Operationen für die Datenbank durchzuführen. Verwenden Sie die folgenden Skripts, um die Berechtigung für den Administratorbenutzer `Admin_User` in der Datenbank zu erstellen und zu testen. 1. Erstellen Sie den Benutzer und gewähren Sie ihm die Rolle . `create user Admin_User WITH PASSWORD ‘Your password’ ALTER user Admin_user CREATEDB; ALTER user Admin_user CREATEROLE;` 2. Um die Berechtigung zu testen, melden Sie sich vom `Admin_User` Benutzer aus an.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SELECT * FROM APP.test ; id ---- 31 CREATE ROLE TEST ; CREATE DATABASE test123 ;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Entwicklungsbenutzer.	Der Entwicklungsbenutzer `APP_dev_user` hat die Berechtigung, die Objekte in seinem lokalen Schema zu erstellen `APP_DEV` und den Zugriff im Schema zu lesen`APP`. Verwenden Sie die folgenden Skripts, um die Berechtigungen des Benutzers `APP_dev_user` in der Datenbank zu erstellen und zu testen.
	1. Erstellen Sie den Benutzer.
	`CREATE USER APP1_dev_user with password 'your password';`
	2. Erstellen Sie das `APP_DEV` Schema für die `App_dev_user` .
	`CREATE SCHEMA APP1_DEV ;`
	3. Erstellen Sie die `APP_DEV`-Rolle.
	`CREATE ROLE APP1_DEV ;`
	`GRANT APP1_RO to APP1_DEV ;`
	`GRANT SELECT ON ALL TABLES IN SCHEMA APP1_DEV to APP1_dev_user`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>GRANT USAGE, CREATE
	 ON SCHEMA APP1_DEV to
	 APP1_DEV_USER
	GRANT APP1_DEV to
	 APP1_DEV_USER ;</pre>
	4. Um die Berechtigungen zu testen, melden Sie sich über an`APP_dev_user` .
	<pre>CREATE TABLE APP1_dev.
	test1(id integer) ;
	CREATE TABLE
	INSERT into APP1_dev.
	test1 (select * from
	 APP1.test);
	INSERT 0 1
	CREATE TABLE APP1.test
	4 (id int) ;
	ERROR: permissio
	n denied for schema
	 APP1
	LINE 1: create table
	 APP1.test4 (id
	 int) ;</pre>	

Zugehörige Ressourcen

PostgreSQL-Dokumentation

- ROLLE ERSTELLEN
- BENUTZER ERSTELLEN
- Vordefinierte Rollen

Zusätzliche Informationen

PostgreSQL 14-Erweiterung

PostgreSQL 14 bietet eine Reihe vordefinierter Rollen, die Zugriff auf bestimmte häufig benötigte, privilegierte Funktionen und Informationen gewähren. Administratoren (einschließlich Rollen, die über die -`CREATE ROLE`Berechtigung verfügen) können diese Rollen oder andere Rollen in ihrer Umgebung Benutzern gewähren und ihnen Zugriff auf die angegebenen Funktionen und Informationen gewähren.

Administratoren können Benutzern mit dem `GRANT` Befehl Zugriff auf diese Rollen gewähren. Um beispielsweise die `pg_signal_backend` Rolle zu erteilen`Admin_User`, können Sie den folgenden Befehl ausführen.

```
GRANT pg_signal_backend TO Admin_User;
```

Die `pg_signal_backend` Rolle soll es Administratoren ermöglichen, vertrauenswürdige Rollen ohne Endbenutzer zu aktivieren, um Signale an andere Backends zu senden. Weitere Informationen finden Sie unter PostgreSQL 14-Erweiterung.

Feinabstimmung des Zugriffs

In einigen Fällen kann es erforderlich sein, den Benutzern einen detaillierteren Zugriff zu gewähren (z. B. tabellenbasierten Zugriff oder spaltenbasierten Zugriff). In solchen Fällen können zusätzliche Rollen erstellt werden, um diesen Benutzern diese Berechtigungen zu gewähren. Weitere Informationen finden Sie unter PostgreSQL Grants.

Emulieren von Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank

Erstellt von HariKrishna Boorgadda (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: Aurora PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Modernisierung; Datenbanken
AWS-Services: Amazon Aurora		

Übersicht

Bewährte Methoden für die Notfallwiederherstellung (DR) von Unternehmen bestehen im Wesentlichen aus dem Entwerfen und Implementieren fehlertoleranter Hard- und Softwaresysteme, die eine Katastrophe überstehen (Geschäftsfortsetzung) und den normalen Betrieb (Geschäftsfortsetzung) mit minimalem Eingriff und idealerweise ohne Datenverlust fortsetzen können. Der Aufbau fehlertoleranter Umgebungen zur Erfüllung der DR-Ziele von Unternehmen kann teuer und zeitaufwändig sein und erfordert ein starkes Engagement des Unternehmens.

Oracle Database bietet drei verschiedene DR-Ansätze, die im Vergleich zu jedem anderen Ansatz zum Schutz von Oracle-Daten das höchste Datenschutz- und Verfügbarkeitsniveau bieten.

- Oracle Zero Data loss Recovery-Appliance
- Oracle Active Data Guard
- Oracle GoldenGate

Dieses Muster bietet eine Möglichkeit, die Oracle GoldenGate DR mithilfe einer globalen Amazon Aurora-Datenbank zu emulieren. Die Referenzarchitektur verwendet Oracle GoldenGate für DR in drei AWS-Regionen. Das Muster führt durch den Plattformwechsel der Quellarchitektur auf die cloudnative globale Aurora-Datenbank, die auf der Amazon Aurora PostgreSQL – kompatiblen Edition basiert.

Globale Aurora-Datenbanken sind für Anwendungen mit globaler Präsenz konzipiert. Eine einzelne Aurora-Datenbank erstreckt sich über mehrere AWS-Regionen mit bis zu fünf sekundären Regionen. Globale Aurora-Datenbanken bieten die folgenden Funktionen:

- Replikation auf physischer Speicherebene
- Globale Lesevorgänge mit niedriger Latenz
- Schnelle Notfallwiederherstellung nach regionsweiten Ausfällen
- Schnelle regionsübergreifende Migrationen
- Niedrige Replikationsverzögerung über Regionen hinweg
- Auswirkungen auf die ittle-to-no Leistung Ihrer Datenbank

Weitere Informationen zu den Features und Vorteilen der globalen Aurora-Datenbank finden Sie unter Verwenden von globalen Amazon-Aurora-Datenbanken. Weitere Informationen zu ungeplanten und verwalteten Failovers finden Sie unter Verwenden von Failover in einer globalen Amazon-Aurora-Datenbank.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Java Database Connectivity (JDBC)-PostgreSQL-Treiber für die Anwendungskonnektivität
- Eine globale Aurora-Datenbank, die auf Amazon Aurora PostgreSQL basiert – Kompatible Edition
- Eine Oracle Real Application Clusters (RAC)-Datenbank, die auf die globale Aurora-Datenbank migriert wurde, die auf Aurora PostgreSQL basiert – kompatibel

Einschränkungen von globalen Aurora-Datenbanken

- Globale Aurora-Datenbanken sind nicht in allen AWS-Regionen verfügbar. Eine Liste der unterstützten Regionen finden Sie unter Globale Aurora-Datenbanken mit Aurora PostgreSQL .
- Informationen zu Funktionen, die nicht unterstützt werden, und anderen Einschränkungen von globalen Aurora-Datenbanken finden Sie unter Einschränkungen von globalen Amazon Aurora-Datenbanken.

Produktversionen

- Amazon Aurora PostgreSQL – Kompatible Edition Version 10.14 oder höher

Architektur

Quelltechnologie-Stack

- Oracle RAC-Datenbank mit vier Knoten
- Oracle GoldenGate

Quellarchitektur

Das folgende Diagramm zeigt drei Cluster mit Oracle RAC mit vier Knoten in verschiedenen AWS-Regionen, die mit Oracle repliziert wurden GoldenGate.

Zieltechnologie-Stack

- Eine globale Amazon-Aurora-Datenbank mit drei Clustern, die auf Aurora PostgreSQL basiert – kompatibel, mit einem Cluster in der primären Region, zwei Clustern in verschiedenen sekundären Regionen

Zielarchitektur

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- Globale Amazon Aurora-Datenbanken umfassen mehrere AWS-Regionen und bieten globale Lesevorgänge mit niedriger Latenz sowie eine schnelle Wiederherstellung nach einem seltenen Ausfall, der sich auf eine gesamte AWS-Region auswirken könnte.

Polen

Regionen mit Reader-DB-Instances hinzufügen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen oder mehrere sekundäre Aurora-Cluster an.	Wählen Sie in der AWS-Managementkonsole Amazon Aurora aus. Wählen Sie den primären Cluster, Aktionen und Region hinzufügen aus der Dropdown-Liste aus.	DBA
Wählen Sie die Instance-Klasse aus.	Sie können die Instance-Klasse des sekundäre n Clusters ändern. Wir empfehlen jedoch, sie genauso zu halten wie die primäre Cluster-Instance-K lasse.	DBA
Fügen Sie die dritte Region hinzu.	Wiederholen Sie die Schritte in diesem Epic, um einen Cluster in der dritten Region hinzuzufü gen.	DBA

Failover der globalen Aurora-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie den primären Cluster aus der globalen Aurora-Datenbank.	1. Wählen Sie auf der Seite Datenbanken den primären Cluster aus. 2. Wählen Sie Aus global entfernen, um ein Failover	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf einen sekundären Cluster durchzuführen.	
Konfigurieren Sie Ihre Anwendung neu, um den Schreibdatenverkehr an den gerade hochgestuften Cluster weiterzuleiten.	Ändern Sie den Endpunkt in der Anwendung mit dem des neu hochgestuften Clusters.	DBA
Beenden Sie die Ausgabe von Schreibvorgängen an den nicht verfügbaren Cluster.	Halten Sie die Anwendung und alle DML-Aktivitäten (Data Manipulation Language) für den Cluster an, den Sie entfernt haben.	DBA
Erstellen Sie eine neue globale Aurora-Datenbank.	Jetzt können Sie eine globale Aurora-Datenbank mit dem neu hochgestuften Cluster als primärem Cluster erstellen.	DBA

Starten des primären Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den primären Cluster aus, der aus der globalen Datenbank gestartet werden soll.	Wählen Sie in der Amazon-Aurora-Konsole in der Einrichtung der globalen Datenbank den primären Cluster aus.	DBA
Starten Sie den Cluster.	Wählen Sie in der Dropdownliste Aktionen die Option Starten aus. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Aktualisieren Sie den Bildschirm, um den	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Status anzuzeigen, oder überprüfen Sie die Spalte Status auf den aktuellen Status des Clusters, nachdem der Vorgang abgeschlossen ist.	

Bereinigen der Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die verbleibenden sekundären Cluster.	Nachdem das Failover-Pilot abgeschlossen ist, entfernen Sie die sekundären Cluster aus der globalen Datenbank.	DBA
Löschen Sie den primären Cluster.	Entfernen Sie den Cluster.	DBA

Zugehörige Ressourcen

- Verwenden von Amazon Aurora Global Databases
- Aurora PostgreSQL Notfallwiederherstellungslösungen mit Amazon Aurora Global Database (Blogbeitrag)

Inkrementelle Migration von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL mit Oracle SQL Developer und AWS SCT

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle; Open-Source	Technologien: Migration; Datenbanken; Modernisierung
AWS-Services: Amazon EC2; Amazon RDS		

Übersicht

Viele Migrationsstrategien und -ansätze werden in mehreren Phasen ausgeführt, die von einigen Wochen bis zu mehreren Monaten dauern können. Während dieser Zeit kann es aufgrund von Patches oder Upgrades in den Oracle-DB-Quell-Instances, die Sie zu PostgreSQL-DB-Instances migrieren möchten, zu Verzögerungen kommen. Um diese Situation zu vermeiden, empfehlen wir Ihnen, den verbleibenden Oracle-Datenbankcode inkrementell zu PostgreSQL-Datenbankcode zu migrieren.

Dieses Muster bietet eine Strategie für die inkrementelle Migration ohne Ausfallzeiten für eine Oracle-DB-Instance mit mehreren Terabyte, für die nach der ersten Migration eine hohe Anzahl von Transaktionen durchgeführt wurde und die in eine PostgreSQL-Datenbank migriert werden müssen. Sie können den step-by-step Ansatz dieses Musters verwenden, um eine Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance inkrementell zu einer Amazon RDS for PostgreSQL-DB-Instance zu migrieren, ohne sich bei der Amazon Web Services (AWS)-Managementkonsole anzumelden.

Das Muster verwendet Oracle SQL Developer, um die Unterschiede zwischen zwei Schemata in der Oracle-Quelldatenbank zu ermitteln. Anschließend verwenden Sie AWS Schema Conversion Tool (AWS SCT), um die Datenbankschemaobjekte von Amazon RDS für Oracle in Datenbankschemaobjekte von Amazon RDS für PostgreSQL zu konvertieren. Anschließend können Sie ein Python-Skript in der Windows-Eingabeaufforderung ausführen, um AWS SCT-Objekte für die inkrementellen Änderungen an den Quelldatenbankobjekten zu erstellen.

Hinweis: Bevor Sie Ihre Produktions-Workloads migrieren, empfehlen wir Ihnen, einen Machbarkeitsnachweis (PoC) für den Ansatz dieses Musters in einer Test- oder Nicht-Produktionsumgebung durchzuführen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine vorhandene DB-Instance von Amazon RDS für Oracle.
- Eine vorhandene DB-Instance von Amazon RDS für PostgreSQL.
- AWS SCT, installiert und konfiguriert mit JDBC-Treibern für Oracle- und PostgreSQL-Datenbank-Engines. Weitere Informationen dazu finden Sie unter Installieren von AWS SCT und Installieren der erforderlichen Datenbanktreiber in der AWS SCT-Dokumentation.
- Oracle SQL Developer, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Oracle SQL Developer-Dokumentation.
- Die `incremental-migration-sct-sql.zip` Datei (angefügt), die auf Ihren lokalen Computer heruntergeladen wurde.

Einschränkungen

- Die Mindestanforderungen für Ihre Quell-DB-Instance von Amazon RDS für Oracle sind:
  - Oracle-Versionen 10.2 und höher (für Versionen 10.x), 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c für die Editionen Enterprise, Standard, Standard One und Standard Two
- Die Mindestanforderungen für Ihre Ziel-DB-Instance von Amazon RDS für PostgreSQL sind:
  - PostgreSQL-Versionen 9.4 und höher (für Versionen 9.x), 10.x und 11.x
- Dieses Muster verwendet Oracle SQL Developer. Ihre Ergebnisse können variieren, wenn Sie andere Tools verwenden, um Schemaunterschiede zu finden und zu exportieren.
- Die von Oracle SQL Developer generierten SQL-Skripts können Transformationsfehler auslösen, was bedeutet, dass Sie eine manuelle Migration durchführen müssen.

- Wenn die AWS SCT-Quell- und Zieltestverbindungen fehlschlagen, stellen Sie sicher, dass Sie die JDBC-Treiberversionen und eingehenden Regeln für die Virtual Private Cloud (VPC)-Sicherheitsgruppe so konfigurieren, dass sie eingehenden Datenverkehr akzeptieren.

Produktversionen

- Amazon RDS for Oracle DB-Instance Version 12.1.0.2 (Version 10.2 und höher)
- Amazon RDS for PostgreSQL DB-Instance Version 11.5 (Version 9.4 und höher)
- Oracle SQL Developer Version 19.1 und höher
- AWS SCT Version 1.0.632 und höher

Architektur

Quelltechnologie-Stack

- DB-Instance von Amazon RDS für Oracle

Zieltechnologie-Stack

- DB-Instance von Amazon RDS für PostgreSQL

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Migration einer DB-Instance von Amazon RDS für Oracle zu einer DB-Instance von Amazon RDS für PostgreSQL.

Das Diagramm zeigt den folgenden Migrationsworkflow:

1. Öffnen Sie Oracle SQL Developer und stellen Sie eine Verbindung zu den Quell- und Zieldatenbanken her.
2. Generieren Sie einen Differenzbericht und dann die SQL-Skriptdatei für die Schemadifferenzobjekte. Weitere Informationen zu Differenzberichten finden Sie unter Detaillierte Differenzberichte in der Oracle-Dokumentation.
3. Konfigurieren Sie AWS SCT und führen Sie den Python-Code aus.
4. Die SQL-Skriptdatei konvertiert von Oracle zu PostgreSQL .
5. Führen Sie die SQL-Skriptdatei auf der PostgreSQL-DB-Ziel-Instance aus.

Automatisierung und Skalierung

Sie können diese Migration automatisieren, indem Sie Ihrem Python-Skript zusätzliche Parameter und sicherheitsbezogene Änderungen für mehrere Funktionen in einem einzigen Programm hinzufügen.

Tools

- AWS SCT – AWS Schema Conversion Tool (AWS SCT) konvertiert Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere.
- Oracle SQL Developer – Oracle SQL Developer ist eine integrierte Entwicklungsumgebung (IDE), die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht.

Code

Die `incremental-migration-sct-sql.zip` Datei (angefügt) enthält den vollständigen Quellcode für dieses Muster.

Polen

Erstellen der SQL-Skriptdatei für die Schemaunterschiede der Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Database Diff in Oracle SQL Developer aus.	1. Melden Sie sich bei Ihrer Oracle-DB-Quell-Instance an, wählen Sie Tools und dann Database Diff aus. 2. Wählen Sie Ihre Quelldatenbank unter Quellverbindung aus. 3. Wählen Sie die aktualisierte oder gepatchte Quelldate	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nbank in Destination Connection aus. 4. Konfigurieren Sie die verbleibenden Optionen entsprechend Ihren Anforderungen, wählen Sie Weiter und dann Fertig stellen, um den Differenz bericht zu generieren.	
Generieren Sie die SQL-Skrip tdatei.	Wählen Sie Skript generiere n, um die Unterschiede in den SQL-Dateien zu generieren. Dadurch wird die SQL-Skrip tdatei generiert, die AWS SCT verwendet, um Ihre Datenbank von Oracle in PostgreSQL zu konvertieren.	DBA

Verwenden des Python-Skripts zum Erstellen der Ziel-DB-Objekte in AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS SCT mit der Windows-Eingabeauf forderung.	1. Kopieren Sie die `AWSSchemaConversionToolBatch.jar` Datei aus Ihrem vorinstal lierten AWS SCT-Ordne r und fügen Sie sie in Ihr Arbeitsverzeichnis ein. 2. Stellen Sie den Python-Code aus der `run_aws_sct_sql.py` Datei aus	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	dem `incremental-migration-sct-sql.zip` Ordner (angefügt) bereit. Dadurch werden XML-Dateien und Sct-Dateien im `projects` Verzeichnis mit den Konfigurationsdetails Ihrer Quell- und Zieldatenbankumgebung erstellt. Außerdem wird die SQL-Skriptdatei gelesen, die Sie in Oracle SQL Developer generiert haben. Schließlich werden .sql-Dateiobjekte im `output` Verzeichnis erstellt.
	3. Konfigurieren Sie die Konfigurationsdetails der Quell- und Zielumgebung in der `database_migration.txt` Datei im folgenden Format:
	`#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`
	
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`.rds.amazonaws.com ,ORCL,orcl,orcl123 4,orcl,1521,ORCL,P OSTGRESQL,mypgdbin stance.cokmvis0v46 q.us-east-1.rds.am azonaws.com,pguser ,pgpassword,pgdb,5432` 4. Ändern Sie die AWS SCT-Konfigurationsparameter entsprechend Ihren Anforderungen und kopieren Sie dann die SQL-Skriptdatei in Ihr Arbeitsverzeichnis im `input` Unterverzeichnis.	
Führen Sie das Python-Skript aus.	1. Führen Sie das Python-Skript mit dem folgenden Befehl aus: `$ python run_aws_sct_sql.py database_migration .txt` 2. Dadurch wird die SQL-Datei für DB-Objekte erstellt. Nicht konvertierte Codes mit Transformationsfehlern können manuell konvertiert werden.	DBA
Erstellen der Objekte in Amazon RDS für PostgreSQL	Führen Sie die SQL-Dateien aus und erstellen Sie Objekte in Ihrer DB-Instance von Amazon RDS für PostgreSQL.	DBA

Zugehörige Ressourcen

- Oracle auf Amazon RDS
- PostgreSQL auf Amazon RDS
- Verwenden der AWS SCT-Benutzeroberfläche
- Verwenden von Oracle als Quelle für AWS SCT

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Laden Sie BLOB-Dateien in TEXT, indem Sie die Dateikodierung in Aurora PostgreSQL-kompatibel verwenden

Erstellt von Bhanu Ganesh Gudivada (AWS) und Jeevan Shetty (AWS)

Umgebung: Produktion	Quelle: Lokale Oracle-Datenbank	Ziel: Aurora PostgreSQL-kompatibel
R-Typ: Re-Architect	Arbeitslast: Oracle; Open Source	Technologien: Migration; Datenbanken
AWS-Dienste: Amazon Aurora		

Übersicht

Während der Migration gibt es häufig Fälle, in denen Sie unstrukturierte und strukturierte Daten verarbeiten müssen, die aus Dateien in einem lokalen Dateisystem geladen wurden. Die Daten können sich auch in einem Zeichensatz befinden, der sich vom Zeichensatz der Datenbank unterscheidet.

Diese Dateien enthalten die folgenden Datentypen:

- Metadaten — Diese Daten beschreiben die Dateistruktur.
- Semistrukturierte Daten — Dies sind Textzeichenfolgen in einem bestimmten Format wie JSON oder XML. Möglicherweise können Sie Aussagen zu solchen Daten treffen, z. B. „beginnt immer mit '<'“ oder „enthält keine Zeilenumbruchzeichen“.
- Volltext — Diese Daten enthalten normalerweise alle Arten von Zeichen, einschließlich Zeilenumbruch- und Anführungszeichen. Sie können auch aus Multibyte-Zeichen in UTF-8 bestehen.
- Binärdaten — Diese Daten können Bytes oder Kombinationen von Bytes enthalten, einschließlich Nullen und Markierungen. end-of-file

Das Laden einer Mischung dieser Datentypen kann eine Herausforderung sein.

Das Muster kann mit lokalen Oracle-Datenbanken, Oracle-Datenbanken, die sich auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der Amazon Web Services (AWS) Cloud befinden, und

Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken verwendet werden. Als Beispiel verwendet dieses Muster Amazon Aurora PostgreSQL-Compatible Edition.

In Oracle Database können Sie mithilfe eines `BFILE` (binären Datei-) Zeigers, des `DBMS_LOB` Pakets und der Oracle-Systemfunktionen Daten aus einer Datei laden und mit Zeichenkodierung in CLOB konvertieren. Da PostgreSQL den BLOB-Datentyp bei der Migration zu einer Amazon Aurora PostgreSQL-Compatible Edition-Datenbank nicht unterstützt, müssen diese Funktionen in PostgreSQL-kompatible Skripten konvertiert werden.

Dieses Muster bietet zwei Ansätze für das Laden einer Datei in eine einzelne Datenbankspalte in einer Amazon Aurora PostgreSQL-kompatiblen Datenbank:

- Ansatz 1 — Sie importieren Daten aus Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket, indem Sie die `table_import_from_s3` Funktion der `aws_s3` Erweiterung mit der Kodierungsoption verwenden.
- Ansatz 2 — Sie kodieren außerhalb der Datenbank hexadezimal und dekodieren dann, um sie innerhalb der Datenbank anzuzeigen. `TEXT`

Wir empfehlen die Verwendung von Approach 1, da Aurora PostgreSQL-Compatible direkt in die Erweiterung integriert ist. `aws_s3`

Dieses Muster verwendet das Beispiel des Ladens einer Flat-Datei, die eine E-Mail-Vorlage mit Multibyte-Zeichen und unterschiedlicher Formatierung enthält, in eine Amazon Aurora PostgreSQL-kompatible Datenbank.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS-Instance oder eine Aurora PostgreSQL-kompatible Instance
- Ein grundlegendes Verständnis von SQL und dem relationalen Datenbankmanagementsystem (RDBMS)
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket.
- Kenntnisse der Systemfunktionen in Oracle und PostgreSQL
- RPM-Paket HexDump -XXD-0.1.1 (in Amazon Linux 2 enthalten)

Einschränkungen

- Für den TEXT Datentyp beträgt die längste mögliche Zeichenfolge, die gespeichert werden kann, etwa 1 GB.

Versionen der Produkte

- Aurora unterstützt die in Amazon Aurora PostgreSQL-Updates aufgeführten PostgreSQL-Versionen.

Architektur

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatibel

Zielarchitektur

Ansatz 1 — Verwendung von aws_s3.table_import_from_s3

Von einem lokalen Server wird eine Datei, die eine E-Mail-Vorlage mit Multibyte-Zeichen und benutzerdefinierter Formatierung enthält, an Amazon S3 übertragen. Die durch dieses Muster bereitgestellte benutzerdefinierte Datenbankfunktion verwendet die `aws_s3.table_import_from_s3` Funktion mit`file_encoding`, um Dateien in die Datenbank zu laden und Abfrageergebnisse als TEXT Datentyp zurückzugeben.

1. Dateien werden in den Staging-S3-Bucket übertragen.
2. Dateien werden in die Amazon Aurora PostgreSQL-kompatible Datenbank hochgeladen.
3. Mit dem pgAdmin-Client `load_file_into_clob` wird die benutzerdefinierte Funktion in der Aurora-Datenbank bereitgestellt.
4. Die benutzerdefinierte Funktion wird intern `table_import_from_s3` mit file_encoding verwendet. Die Ausgabe der Funktion wird durch die Verwendung von `array_to_string` und `array_agg` als TEXT Ausgabe abgerufen.

Ansatz 2 — Hexadezimale Kodierung außerhalb der Datenbank und Dekodierung zur Anzeige von TEXT innerhalb der Datenbank

Eine Datei von einem lokalen Server oder einem lokalen Dateisystem wird in einen Hex-Dump konvertiert. Dann wird die Datei als Feld in PostgreSQL importiert. `TEXT`

1. Konvertieren Sie die Datei in der Befehlszeile mit der Option in einen Hex-Dump. `xxd -p`
2. Laden Sie die Hex-Dump-Dateien mithilfe der `\copy` Option in das Aurora PostgreSQL-kompatible Format hoch und dekodieren Sie dann die Hex-Dump-Dateien in Binärdateien.
3. Kodieren Sie die Binärdaten, die zurückgegeben werden sollen als. `TEXT`

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere Tools

- pgAdmin4 ist eine Open-Source-Verwaltungs- und Entwicklungsplattform für PostgreSQL. pgAdmin4 kann unter Linux, Unix, Mac OS und Windows zur Verwaltung von PostgreSQL verwendet werden.

Epen

Ansatz 1: Daten von Amazon S3 nach Aurora PostgreSQL-kompatibel importieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten einer EC2-Instance.	Anweisungen zum Starten einer Instance finden Sie unter Starten Sie Ihre Instance.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das PostgreSQL-Client-Tool pgAdmin.	Laden Sie pgAdmin herunter und installieren Sie es.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie.	Erstellen Sie eine AWS Identity and Access Management (IAM) -Richtlinie mit dem Namen `aurora-s3-access-pol`, die Zugriff auf den S3-Bucket gewährt, in dem die Dateien gespeichert werden. Verwenden Sie den folgenden Code und `<bucket-name>` ersetzen Sie ihn durch den Namen Ihres S3-Buckets. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:AbortMultipartUpload", "s3:DeleteObject", "s3:ListMultipartUploadParts", "s3:PutObject", "s3:ListBucket" ], "Resource": [`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"arn:aws:s3:::<bucket-name>/*",
	
	"arn:aws:s3:::<bucket-name>"
	]
	}
	]
	}</pre>	

Erstellen Sie eine IAM-Rolle für den Objektimport von Amazon S3 nach Aurora PostgreSQL-kompatibel.	Verwenden Sie den folgenden Code, um eine IAM-Rolle mit dem Namen der Vertrauen sbeziehung zu erstellen. `aurora-s3-import-role` [AssumeRole](#) `AssumeRole` ermöglich t Aurora, in Ihrem Namen auf andere AWS-Services zuzugreifen.
	
	<pre>{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow","Principal": {
	"Service": "rds.amazonaws.com"
	},"Action": "sts:AssumeRole"
	}
	]
	}</pre>
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die IAM-Rolle dem Cluster zu.	Um die IAM-Rolle dem Aurora PostgreSQL-kompatiblen Datenbank-Cluster zuzuordnen, führen Sie den folgenden AWS-CLI-Befehl aus. Ändern Sie `<Account-ID>` die ID des AWS-Kontos, das die Aurora PostgreSQL-kompatible Datenbank hostet. Dadurch kann die Aurora PostgreSQL-kompatible Datenbank auf den S3-Bucket zugreifen. `aws rds add-role-to-db-cluster --db-cluster-identifier aurora-postgres-cl --feature-name s3Import --role-arn arn:aws:iam::<Account-ID>:role/aurora-s3-import-role`	DBA
Laden Sie das Beispiel auf Amazon S3 hoch.	1. Kopieren Sie im Abschnitt Zusätzliche Informationen dieses Musters den E-Mail-Vorlagencode in eine Datei mit dem Namen `salary.event.notification.email.vm` . 2. Laden Sie die Datei in den S3-Bucket hoch.	DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die benutzerd efinierte Funktion bereit.	1. Kopieren Sie im Abschnitt Zusätzliche Informationen den Inhalt der `load_file _into_clob` SQL-Datei mit der benutzerdefinierten Funktion in eine temporäre Tabelle. 2. Melden Sie sich bei der Aurora PostgreSQL-kompatiblen Datenbank an und stellen Sie sie mithilfe des pgAdmin-Clients im Datenbankschema bereit.	Besitzer der App, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die benutzerd efinierte Funktion zum Importieren der Daten in die Datenbank aus.	Führen Sie den folgenden SQL-Befehl aus und ersetzen Sie die Elemente in spitzen Klammern durch die entsprech enden Werte.
	`select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	Ersetzen Sie die Elemente in spitzen Klammern durch die entsprechenden Werte, wie im folgenden Beispiel gezeigt, bevor Sie den Befehl ausführen.
	`Select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	Der Befehl lädt die Datei aus Amazon S3 und gibt die Ausgabe als zurück`TEXT`.
		Besitzer der App, DBA

Ansatz 2: Konvertieren Sie die Vorlagendatei in einen Hex-Dump in einem lokalen Linux-System

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konvertiert die Vorlagendatei in einen Hex-Dump.	Das Hexdump-Hilfsprogramm zeigt den Inhalt von Binärdateien in Hexadezimal, Dezimal, Oktal oder ASCII an. Der `hexdump` Befehl ist Teil des `util-linux` Pakets und in Linux-Distributionen vorinstalliert. Das Hexdump RPM-Paket ist ebenfalls Teil von Amazon Linux 2.
	
	Führen Sie den folgenden Shell-Befehl aus, um den Dateiinhalt in einen Hex-Dump zu konvertieren.
	
	`xxd -p </path/file.vm> | tr -d '\n' > </path/file.hex>`
	
	Ersetzen Sie den Pfad und die Datei durch die entsprechenden Werte, wie im folgenden Beispiel gezeigt.
	
	`xxd -p employee.salary.event.notification.email.vm | tr -d '\n' > employee.salary.event.notification.email.vm.hex`
		DBA

Laden Sie die Hexdump-Datei in das Datenbankschema.	Verwenden Sie die folgenden Befehle, um die Hexdump-D	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	atei in die Aurora PostgreSQ L-kompatible Datenbank zu laden.
	
	1. Melden Sie sich bei der Aurora PostgreSQL-Datenbank an und erstellen Sie eine neue Tabelle mit dem Namen. `email_tem plate_hex`
	
	`CREATE TABLE email_tem plate_hex(hex_data TEXT);`
	
	2. Laden Sie die Dateien mit dem folgenden Befehl aus dem lokalen Dateisystem in das DB-Schema.
	
	`\copy email_tem plate_hex FROM '/ path/file.hex';`
	
	Ersetzen Sie den Pfad durch den Speicherort in Ihrem lokalen Dateisystem.
	
	`\copy email_tem plate_hex FROM '/ tmp/employee.sal ary.event.notifica tion.email.vm.hex';`
	
	3. Erstellen Sie eine weitere Tabelle	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	namensemail_template_bytea .
	
	`CREATE TABLE email_template_bytea(hex_data bytea);`
	
	4. Fügen Sie die Daten von email_template_hex in einemail_template_bytea .
	
	`INSERT INTO email_template_bytea (hex_data)`
	
	`(SELECT decode(hex_data, 'hex') FROM email_template_hex limit 1);`
	
	5. Um Hex-Bytea-Code als TEXT Daten zurückzugeben, führen Sie den folgenden Befehl aus.
	
	`SELECT encode(hex_data::bytea, 'escape') FROM email_template_bytea;`	

Zugehörige Ressourcen

Referenzen

- Verwenden einer PostgreSQL-Datenbank als Ziel für den AWS Database Migration Service

- Playbook zur Migration von Oracle Database 19c zu Amazon Aurora mit PostgreSQL-Kompatibilität (12.4)
- IAM-Richtlinien erstellen
- Zuordnen einer IAM-Rolle zu einem Amazon Aurora MySQL-DB-Cluster
- pgAdmin

Tutorials

- Erste Schritte mit Amazon RDS
- Migrieren Sie von Oracle zu Amazon Aurora

Zusätzliche Informationen

benutzerdefinierte Funktion load_file_into_clob

```
CREATE OR REPLACE FUNCTION load_file_into_clob(
    s3_bucket_name text,
    s3_bucket_region text,
    file_name text,
    file_delimiter character DEFAULT '&'::bpchar,
    file_encoding text DEFAULT 'UTF8'::text)
    RETURNS text
    LANGUAGE 'plpgsql'
    COST 100
    VOLATILE PARALLEL UNSAFE
AS $BODY$
DECLARE
    blob_data BYTEA;
    clob_data TEXT;
    l_table_name CHARACTER VARYING(50) := 'file_upload_hex';
    l_column_name CHARACTER VARYING(50) := 'template';
    l_return_text TEXT;
    l_option_text CHARACTER VARYING(150);
    l_sql_stmt CHARACTER VARYING(500);

BEGIN

    EXECUTE format ('CREATE TEMPORARY TABLE %I (%I text, id_serial serial)',
 l_table_name, l_column_name);
```

```
    l_sql_stmt := 'select ''(format text, delimiter ''''' || file_delimiter || ''''',
 encoding ''''' || file_encoding ||  ''''')'' ';

    EXECUTE FORMAT(l_sql_stmt)
    INTO l_option_text;

    EXECUTE FORMAT('SELECT aws_s3.table_import_from_s3($1,$2,$6,
 aws_commons.create_s3_uri($3,$4,$5))')
    INTO l_return_text
    USING l_table_name, l_column_name, s3_bucket_name,
 file_name,s3_bucket_region,l_option_text;

    EXECUTE format('select array_to_string(array_agg(%I order by id_serial),E''\n'')
 from %I', l_column_name, l_table_name)
    INTO clob_data;

    drop table file_upload_hex;

    RETURN clob_data;
END;
$BODY$;
```

E-Mail-Vorlage

```
##############################################################################################
##
 ##
##    johndoe Template Type: email
 ##
##    File: johndoe.salary.event.notification.email.vm
 ##
##    Author: Aimée Étienne    Date 1/10/2021
      ##
##  Purpose: Email template used by EmplmanagerEJB to inform a johndoe they         ##
##        have been given access to a salary event
 ##
##    Template Attributes:
 ##
##        invitedUser - PersonDetails object for the invited user
  ##
##        salaryEvent - OfferDetails object for the event the user was given access
 ##
```

```
##        buyercollege - CompDetails object for the college owning the salary event
 ##
##        salaryCoordinator - PersonDetails of the salary coordinator for the event
 ##
##        idp - Identity Provider of the email recipient
 ##
##        httpWebRoot - HTTP address of the server
 ##
##
 ##
#################################################################################

$!invitedUser.firstname $!invitedUser.lastname,

Ce courriel confirme que vous avez ete invite par $!salaryCoordinator.firstname $!
salaryCoordinator.lastname de $buyercollege.collegeName a participer a l'evenement
 "$salaryEvent.offeringtitle" sur johndoeMaster Sourcing Intelligence.

Votre nom d'utilisateur est $!invitedUser.username

Veuillez suivre le lien ci-dessous pour acceder a l'evenement.

${httpWebRoot}/myDashboard.do?idp=$!{idp}

Si vous avez oublie votre mot de passe, utilisez le lien "Mot de passe oublie" situe
 sur l'ecran de connexion et entrez votre nom d'utilisateur ci-dessus.

Si vous avez des questions ou des preoccupations, nous vous invitons a
 communiquer avec le coordonnateur de l'evenement $!salaryCoordinator.firstname $!
salaryCoordinator.lastname au ${salaryCoordinator.workphone}.

*******

johndoeMaster Sourcing Intelligence est une plateforme de soumission en ligne pour les
 equipements, les materiaux et les services.

Si vous avez des difficultes ou des questions, envoyez un courriel a
 support@johndoeMaster.com pour obtenir de l'aide.
```

Migrieren von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL im SSL-Modus mithilfe von AWS DMS

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Amazon RDS für Oracle	Ziel: Amazon RDS PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle; Open-Source	Technologien: Migration; Sicherheit, Identität, Compliance; Datenbanken
AWS-Services: AWS DMS; Amazon RDS		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Datenbank-Instance von Amazon Relational Database Service (Amazon RDS) für Oracle zu einer Datenbank von Amazon RDS für PostgreSQL in der Amazon Web Services (AWS) Cloud. Um Verbindungen zwischen den Datenbanken zu verschlüsseln, verwendet das Muster die Zertifizierungsstelle (CA) und den SSL-Modus in Amazon RDS und AWS Database Migration Service (AWS DMS).

Das Muster beschreibt eine Online-Migrationsstrategie mit geringer oder keiner Ausfallzeit für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen. Aus Gründen der Datensicherheit verwendet das Muster SSL bei der Übertragung der Daten.

Dieses Muster verwendet AWS Schema Conversion Tool (AWS SCT), um das Datenbankschema von Amazon RDS für Oracle in ein Amazon RDS for PostgreSQL-Schema zu konvertieren. Dann verwendet das Muster AWS DMS, um Daten von der Datenbank von Amazon RDS für Oracle in die Datenbank von Amazon RDS für PostgreSQL zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Amazon-RDS-Datenbank-Zertifizierungsstelle (CA), die nur mit rds-ca-2019 konfiguriert ist (das Zertifikat rds-ca-2015 ist am 5. März 2020 abgelaufen)
- AWS SCT
- AWS DMS
- pgAdmin
- SQL-Tools (z. B. SQL Developer oder SQL*Plus)

Einschränkungen

- Datenbank von Amazon RDS für Oracle – Die Mindestanforderung gilt für die Oracle-Versionen 19c für die Enterprise- und Standard Two-Editionen.
- Datenbank von Amazon RDS für PostgreSQL – Die Mindestanforderung gilt für PostgreSQL Version 12 und höher (für Versionen 9.x und höher).

Produktversionen

- Amazon RDS for Oracle-Datenbankversion 12.1.0.2-Instance
- Datenbankversion 11.5 von Amazon RDS für PostgreSQL

Architektur

Quelltechnologie-Stack

- Eine Datenbank-Instance von Amazon RDS für Oracle mit Version 12.1.0.2.v18.

Zieltechnologie-Stack

- AWS DMS
- Eine Datenbank-Instance von Amazon RDS für PostgreSQL mit Version 11.5.

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für die Datenmigrationsarchitektur zwischen Oracle (Quelle)- und PostgreSQL (Ziel)-Datenbanken. Die Architektur umfasst Folgendes:

- Eine Virtual Private Cloud (VPC)

- Eine Availability Zone
- Ein privates Subnetz
- Eine Datenbank von Amazon RDS für Oracle
- Eine AWS DMS-Replikations-Instance
- Eine Datenbank von RDS für PostgreSQL

Um Verbindungen für Quell- und Zieldatenbanken zu verschlüsseln, müssen der CA- und SSL-Modus in Amazon RDS und AWS DMS aktiviert sein.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Andere -Services

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.

Polen

Konfigurieren der Instance von Amazon RDS für Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Oracle-Datenbank-Instance.	Melden Sie sich bei Ihrem AWS-Konto an, öffnen Sie die AWS-Managementkonsole und navigieren Sie zur Amazon RDS-Konsole. Wählen Sie in der Konsole Datenbank erstellen und dann Oracle aus.	Allgemeines AWS, DBA
Konfigurieren Sie Sicherheitsgruppen.	Konfigurieren Sie ein- und ausgehende Sicherheitsgruppen.	Allgemeines AWS
Erstellen Sie eine Optionsgruppe.	Erstellen Sie eine Optionsgruppe in derselben VPC und Sicherheitsgruppe wie die Datenbank von Amazon RDS für Oracle. Wählen Sie für Option SSL aus. Wählen Sie für Port 2484 (für SSL-Verbindungen) aus.	Allgemeines AWS
Konfigurieren Sie die Optionseinstellungen.	Verwenden Sie die folgenden Einstellungen: • `SQLNET.CIPHER_SUITE : SSL_RSA_WITH_AES_256_CBC_SHA` • `SQLNET.SSL_VERSION : 1.2 or 1.0`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die DB-Instance von RDS für Oracle.	Legen Sie das CA-Zertifikat auf rds-ca-2019 fest. Fügen Sie unter Optionsgruppe die zuvor erstellte Optionsgruppe an.	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass die DB-Instance von RDS für Oracle verfügbar ist.	Stellen Sie sicher, dass die Datenbank-Instance von Amazon RDS für Oracle betriebsbereit ist und dass auf das Datenbankschema zugegriffen werden kann.
	
	Um eine Verbindung mit der DB von RDS für Oracle herzustellen, verwenden Sie den `sqlplus` Befehl aus der Befehlszeile.
	
	`$ sqlplus orcl/**** @myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com:1521/ORCL`
	`SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 15 18:11:07 2019`
	`Copyright (c) 1982, 2016, Oracle. All rights reserved.`
	`Last Successful login time: Mon Dec 16 2019 23:17:31 +05:30`
	`Connected to:`
	`Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production`
	`With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQL>`	
Erstellen Sie Objekte und Daten in der Datenbank von RDS für Oracle.	Erstellen Sie Objekte und fügen Sie Daten in das Schema ein.	DBA

Konfigurieren der Amazon RDS for PostgreSQL-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datenbank von RDS für PostgreSQL.	Wählen Sie auf der Seite Datenbank erstellen der Amazon-RDS-Konsole PostgreSQL aus, um eine Datenbank-Instance von Amazon RDS für PostgreSQL zu erstellen.	DBA, Allgemeines AWS
Konfigurieren Sie Sicherhei tsgruppen.	Konfigurieren Sie ein- und ausgehende Sicherhei tsgruppen.	Allgemeines AWS
Erstellen Sie eine Parameter gruppe.	Wenn Sie PostgreSQL Version 11.x verwenden, erstellen Sie eine Parameter gruppe, um SSL-Parameter festzulegen. In PostgreSQL Version 12 ist die SSL-Param etergruppe standardmäßig aktiviert.	Allgemeines AWS
Bearbeiten Sie Parameter.	Ändern Sie den `rds.force_ssl` Parameter in `1` (ein).	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardmäßig ist der `ssl` Parameter 1 (ein). Wenn Sie den `rds.force_ssl` Parameter auf setzen1, erzwingen Sie, dass alle Verbindungen nur über den SSL-Modus verbunden werden.	
Ändern Sie die DB-Instance von RDS für PostgreSQL.	Legen Sie das CA-Zertif ikat auf rds-ca-2019 fest. Fügen Sie je nach PostgreSQ L-Version die Standardp arametergruppe oder die zuvor erstellte Parameter gruppe an.	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass die DB-Instance von RDS für PostgreSQL verfügbar ist.	Stellen Sie sicher, dass die Datenbank von Amazon RDS für PostgreSQL betriebsbereit ist.
	
	Der `psql` Befehl stellt eine SSL-Verbindung her, bei der über die Befehlszeile `sslmode` festgelegt ist.
	
	Eine Option besteht darin, `sslmode=1` in der Parametergruppe festzulegen und eine `psql` Verbindung zu verwenden, ohne den `sslmode` Parameter in den Befehl aufzunehmen.
	
	Die folgende Ausgabe zeigt, dass die SSL-Verbindung hergestellt wurde.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Type "help" for help.`
	`pgdb=>`
	
	Eine zweite Option besteht darin, `sslmode=1` in der Parametergruppe festzulegen und den `sslmode` Parameter in den `psql` Befehl aufzunehmen.
	
	Die folgende Ausgabe zeigt, dass die SSL-Verbindung hergestellt wurde.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser sslmode=require"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
	`pgdb=>`	

Konfigurieren und Ausführen von AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SCT.	Installieren Sie die neueste Version der AWS SCT-Anwendung.	Allgemeines AWS
Konfigurieren Sie AWS SCT mit JDBC-Treibern.	Laden Sie die Java Database Connectivity (JDBC)-Treiber für Oracle (ojdbc8.jar) und PostgreSQL (postgresql-42.2.5.jar) herunter. Um die Treiber in AWS SCT zu konfigurieren, wählen Sie Einstellungen , Globale Einstellungen , Treiber .	Allgemeines AWS
Erstellen Sie das AWS SCT-Projekt.	Erstellen Sie das AWS SCT-Projekt und den Bericht mit Oracle als Quell-DB-Engine und Amazon RDS for PostgreSQL als Ziel-DB-Engine: 1. Testen Sie Verbindungen zur Oracle-Quelldatenbank und zielen Sie auf die Datenbank von Amazon RDS für PostgreSQL ab, indem Sie Verbindungsdetails angeben. Für die Oracle-Quelldatenbank sind die folgenden Berechtigungen oder	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Berechtigungen erforderl ich: • `CONNECT` • `SELECT_CATALOG_ROL E` • `SELECT ANY DICTIONARY` • `SELECT on SYS.USER$ TO <sct_user>` Weitere Informationen finden Sie unter Verwenden von Oracle Database als Quelle für AWS SCT . Sowohl Quell- als auch Zielverbindungen müssen erfolgreich sein, bevor AWS SCT den Migrationsbericht starten kann. 2. Geben Sie nach dem Bericht das Schema ein, das konvertiert werden soll, und wählen Sie Fertigste llen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbank objekte.	1. Wählen Sie Schema laden aus. AWS SCT zeigt die Quell- und die konvertierten Zielobjekte an, einschlie ßlich Objekte, die Fehler aufweisen. Aktualisieren Sie alle falschen Objekte in der Zieldatenbank. 2. Überprüfen Sie die Fehler und löschen Sie sie mithilfe manueller Eingriffe. 3. Nachdem alle Fehler gelöscht wurden, wählen Sie Schema erneut laden aus. 4. Wählen Sie Auf Datenbank anwenden aus. 5. Stellen Sie eine Verbindun g mit pgAdmin oder einem beliebigen Tool her, das eine PostgreSQL-DB-Verb indung unterstützt, und überprüfen Sie das Schema und die Objekte.	DBA, Allgemeines AWS

Konfigurieren und Ausführen von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikati ons-Instance.	1. Melden Sie sich bei Ihrem Konto an, öffnen Sie die	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS-Managementkonsole und navigieren Sie zur AWS DMS-Konsole. 2. Erstellen Sie eine Replikations-Instance mit gültigen Einstellungen für die VPC, die Sicherheitsgruppe, die Availability Zone und zusätzliche Verbindungsattribute.	
Importieren Sie das Zertifikat.	1. Laden Sie das Zertifikat rds-ca-2019-root.pem herunter. 2. Importieren Sie das Zertifikat auf der Seite Zertifikate als `rds-ca-2019-root` .	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Quellendpunkt.	1. Erstellen Sie einen Quellendpunkt für Amazon RDS für Oracle, indem Sie RDS-DB-Instance auswählen und dann die von Ihnen erstellte DB-Instance von RDS für Oracle auswählen. Die Details zur Endpunktkonfiguration werden automatisch ausgefüllt. 2. Wählen Sie Zugriffsinformationen manuell bereitstellen aus. Stellen Sie für Port sicher, dass Sie 2484 eingeben. 3. Wählen Sie unter Secure Socket Layer (SSL)-Modus die Option verify-ca, und dann das CA-Zertifikat aus, das Sie zuvor erstellt haben. 4. Fügen Sie unter Endpunkteinstellungen das zusätzliche Verbindungsattribut hinzu, `NumberDataTypeScale=-2` um den `NUMBER` Datentyp ohne Größe zu unterstützen. Weitere Informationen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für AWS Database Migration Service.	
Erstellen Sie den Zielendpunkt.	1. Erstellen Sie einen Zielendpunkt für Amazon RDS for PostgreSQL, indem Sie RDS-DB-Instance auswählen und dann Ihre RDS-for-PostgreSQL-DB-Instance auswählen. Die Details zur Endpunktkonfiguration werden automatisch ausgefüllt. 2. Wählen Sie Zugriffsinformationen manuell bereitstellen aus. Stellen Sie für Port sicher, dass Sie 2484 eingeben. Weitere Informationen finden Sie unter Verwenden einer PostgreSQL-Datenbank als Ziel für AWS Database Migration Service.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Endpunkte.	1. Testen Sie die Quell- und Zielendpunkte, um sicherzustellen, dass beide erfolgreich und verfügbar sind. 2. Wenn ein Test fehlschlägt, stellen Sie sicher, dass die Regeln für eingehenden Datenverkehr der Sicherheitsgruppe gültig sind.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Migration saufgaben.	Gehen Sie wie folgt vor, um eine Migrationsaufgabe für Volllast und Change Data Capture (CDC) oder für die Datenvalidierung zu erstellen: 1. Um eine Datenbank migrationsaufgabe zu erstellen, wählen Sie die Replikations-Instance, den Quelldatenbankendp unkt und den Zieldaten bankendpunkt aus. Geben Sie den Migrationstyp wie folgt an: • Migrieren vorhanden er Daten (vollständiges Laden) • Replizieren Sie nur Datenänderungen (CDC) • Migrieren vorhandener Daten und Replizieren laufender Änderungen (Volllast und CDC) 2. Unter Tabellenzuordnungen können Sie Auswahlregeln und Transformationsregeln im GUI- oder JSON-Format konfigurieren: • Wählen Sie unter Auswahlregeln das Schema aus, geben Sie den Tabellenn amen ein und wählen	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Aktion (Include oder Exclude) aus, die konfiguriert werden soll, z. B. Schema ORCL, Tabellenname %, Action Include. • Führen Sie unter Transformationsregeln einen der folgenden Schritte aus: • Wählen Sie das Schema aus und wählen Sie die Aktion aus (Groß-/Kleinschreibung, Präfix, Suffix), z. B. Zielschema ORCL, Aktion Kleinbuchstaben erstellen. • Wählen Sie das Schema aus, geben Sie den Tabellennamen ein und wählen Sie die Aktion aus (Groß- und Kleinschreibung, Präfix, Suffix), z. B. Zielschema ORCL, Tabelle %, Aktion in Kleinbuchstaben. 3. Aktivieren Sie die Amazon-CloudWatch Logs-Überwachung. 4. Fügen Sie für die Zuordnungsregeln den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgenden JSON-Code hinzu. `{ "rules": [{ "rule-type": "transformation", "rule-id": "1", "rule-name": "1", "rule-target": "table", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "transformation", "rule-id": "2", "rule-name": "2", "rule-target": "schema",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"object-locator": {
	"schema-name": "ORCL",
	"table-name": "%"
	},
	"rule-action": "convert-lowercase",
	"value": null,
	"old-value": null
	},
	{
	"rule-type": "selection",
	"rule-id": "3",
	"rule-name": "3",
	"object-locator": {
	"schema-name": "ORCL",
	"table-name": "DEPT"
	},
	"rule-action": "include",
	"filters": []
	}
	]
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie den Produktionslauf.	Bestätigen Sie Ausfallzeiten mit Stakeholdern wie Anwendungsbesitzern, um AWS DMS in Produktionssystemen auszuführen.	Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die -Migratio nsaufgabe aus.	1. Starten Sie die AWS DMS-Aufgabe mit dem Status Bereit und überwachen Sie die Migrationsaufgaben protokolle in Amazon CloudWatch auf Fehler. Wenn Sie Vorhanden e Daten migrieren und laufende Änderungen als Migrationstyp replizieren ausgewählt haben und der Status Laufende Replikati on laden lautet, ist der vollständige Ladevorgang mit CDC-Datenmigration abgeschlossen und die Validierung läuft. 2. Nachdem Sie die Migration gestartet haben, erhalten Sie zusätzliche Informati onen zur SSL-Verbindung unter CloudWatch. Für Oracle CloudWatch zeigt die folgende Verbindun gszeichenfolge an. `2019-12-17T09:15:1 1 [SOURCE_U NLOAD ]I: Connectin g to Oracle: Beginning session (oracle_endpoint_c onn.c:834)`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die PostgreSQL-Verbindungszeichenfolge ähnelt dem folgenden Beispiel. `2019-12-17T09:15:11 [TARGET_LOAD ]I: Going to connect to ODBC connection string: PROTOCOL=7.4-0;DRIVER={PostgreSQL};SERVER=mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com;DATABASE=pgdb;PORT=5432;sslmode=require;UID=pguser; (odbc_endpoint_imp.c:2218)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten.	Überprüfen Sie die Ergebnisse und Daten der Migrationsaufgabe in den Oracle-Quell- und PostgreSQLZieldatenbanken: 1. Stellen Sie eine Verbindung zu pgAdmin her und überprüfen Sie die Daten in Ihrer PostgreSQL-Datenbank mit Schema `ORCL`. 2. Überprüfen Sie für CDC die laufenden Änderungen, indem Sie Daten in die Oracle-Quelldatenbank einfügen oder aktualisieren.	DBA
Beenden Sie die Migrationsaufgabe.	Nachdem Sie die Datenvalidierung erfolgreich abgeschlossen haben, beenden Sie die Migrationsaufgabe.	Allgemeines AWS

Bereinigen der Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die AWS DMS-Aufgaben.	1. Navigieren Sie in der AWS DMS-Konsole zu Datenbankmigrationsaufgaben und beenden Sie alle laufenden oder laufenden AWS DMS-Aufgaben.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie die Aufgabe oder Aufgaben, Aktionen und dann Löschen aus.	
Löschen Sie die AWS DMS-Endpunkte.	Wählen Sie die Quell- und Zielendpunkte aus, die Sie erstellt haben, wählen Sie Aktionen und dann Löschen aus.	Allgemeines AWS
Löschen Sie die AWS DMS-Replikations-Instance.	Wählen Sie die Replikations-Instance, dann Aktionen und dann Löschen aus.	Allgemeines AWS
Löschen Sie die PostgreSQL-Datenbank.	1. Wählen Sie in der Amazon-RDS-Konsole Datenbanken aus. 2. Wählen Sie die PostgreSQL-Datenbank-Instance aus, die Sie erstellt haben, wählen Sie Aktionen und dann Löschen aus.	Allgemeines AWS
Löschen Sie die Oracle-Datenbank.	Wählen Sie in der Amazon RDS-Konsole die Oracle-Datenbank-Instance aus, wählen Sie Aktionen und dann Löschen aus.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
AWS SCT-Quell- und Zieltestverbindungen schlagen fehl.	Konfigurieren Sie JDBC-Treiberversionen und Regeln für eingehenden Datenverkehr der

Problem	Lösung
	VPC-Sicherheitsgruppe, um den eingehenden Datenverkehr zu akzeptieren.
Der Testlauf des Oracle-Quellendpunkts schlägt fehl.	Überprüfen Sie die Endpunkteinstellungen und ob die Replikations-Instance verfügbar ist.
Die Ausführung des vollständigen Ladevorgangs der AWS DMS-Aufgabe schlägt fehl.	Überprüfen Sie, ob die Quell- und Zieldatenbank übereinstimmende Datentypen und -größen haben.
Die AWS DMS-Validierungsmigrationsaufgabe gibt Fehler zurück.	1. Überprüfen Sie, ob die Tabelle über einen Primärschlüssel verfügt. Tabellen ohne Primärschlüssel werden nicht validiert. 2. Wenn die Tabelle über einen Primärschlüssel verfügt, aber Fehler zurückgibt, überprüfen Sie das zusätzliche Verbindungsattribut im Quellendpunkt. Das zusätzliche Verbindungsattribut muss `numberDataTypeScale=-2` den `NUMBER` Datentyp ohne Größe dynamisch basierend auf den in der Tabelle verfügbaren Daten unterstützen.

Zugehörige Ressourcen

Datenbanken

- Amazon RDS für Oracle
- Amazon RDS für PostgreSQL

SSL-DB-Verbindung

- Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung mit einer DB-Instance
  - Verwenden von SSL mit einer DB-Instance von RDS für Oracle
  - Sichern von Verbindungen zu RDS für PostgreSQL mit SSL/TLS
  - CA-2019-Stammzertifikat herunterladen

- Arbeiten mit Optionsgruppen
  - Hinzufügen von Optionen zu Oracle DB-Instances
  - Oracle Secure Sockets Layer
- Arbeiten mit Parametergruppen
- PostgreSQL-Verbindungsparameter sslmode
- Verwenden von SSL aus JDBC

AWS SCT

- AWS Schema Conversion Tool
- AWS Schema Conversion Tool – Benutzerhandbuch
- Verwenden der AWS SCT-Benutzeroberfläche
- Verwenden von Oracle Database als Quelle für AWS SCT

AWS DMS

- AWS Database Migration Service
- AWS Database Migration Service-Benutzerhandbuch
  - Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
  - Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS
- Verwenden von SSL mit AWS Database Migration Service
- Migrieren von Anwendungen mit relationalen Datenbanken zu AWS

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und AWS DMS mithilfe von AWS CLI und AWS CloudFormation

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Amazon RDS für Oracle	Ziel: Amazon RDS für PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle; Open-Source	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; Amazon RDS; AWS SCT		

Übersicht

Dieses Muster zeigt, wie eine Amazon Relational Database Service (Amazon RDS) for Oracle-DB-Instance mithilfe der AWS Command Line Interface (AWS CLI) zu einer Amazon RDS for PostgreSQL-DB-Instance migriert wird. Der Ansatz bietet minimale Ausfallzeiten und erfordert keine Anmeldung bei der AWS-Managementkonsole.

Dieses Muster trägt dazu bei, manuelle Konfigurationen und einzelne Migrationen mithilfe der AWS Schema Conversion Tool (AWS SCT)- und AWS Database Migration Service (AWS DMS)-Konsolen zu vermeiden. Die Lösung richtet eine einmalige Konfiguration für mehrere Datenbanken ein und führt die Migrationen mithilfe von AWS SCT und AWS DMS in der AWS CLI durch.

Das Muster verwendet AWS SCT, um Datenbankschemaobjekte von Amazon RDS für Oracle in Amazon RDS für PostgreSQL zu konvertieren, und verwendet dann AWS DMS, um die Daten zu migrieren. Mit Python-Skripten in AWS CLI erstellen Sie AWS SCT-Objekte und AWS DMS-Aufgaben mit einer AWS- CloudFormation Vorlage.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine vorhandene DB-Instance von Amazon RDS für Oracle.

- Eine vorhandene DB-Instance von Amazon RDS für PostgreSQL.
- Eine Amazon EC2-Instance oder ein lokaler Computer mit Windows- oder Linux-Betriebssystem zum Ausführen von Skripts.
- Ein Verständnis der folgenden AWS DMS-Migrationsaufgabentypen: `full-load`, `cdc`, `full-load-and-cdc`. Weitere Informationen finden Sie unter Erstellen einer Aufgabe in der AWS DMS-Dokumentation.
- AWS SCT, installiert und konfiguriert mit Java Database Connectivity (JDBC)-Treibern für Oracle- und PostgreSQL-Datenbank-Engines. Weitere Informationen finden Sie unter Installieren von AWS SCT und Installieren der erforderlichen Datenbanktreiber in der AWS SCT-Dokumentation.
- Die `AWSSchemaConversionToolBatch.jar` Datei aus dem installierten AWS SCT-Ordner, die in Ihr Arbeitsverzeichnis kopiert wurde.

- Die `-cli-sct-dms-cft.zip`Datei (angefügt), heruntergeladen und in Ihrem Arbeitsverzeichnis extrahiert.

- Die neueste Version der AWS DMS-Replikations-Instance-Engine. Weitere Informationen finden Sie unter Wie erstelle ich eine AWS DMS-Replikations-Instance? in der AWS Support-Dokumentation und unter AWS DMS 3.4.4 Versionshinweise in der AWS DMS-Dokumentation.
- AWS CLI Version 2, installiert und konfiguriert mit Ihrer Zugriffsschlüssel-ID, dem geheimen Zugriffsschlüssel und dem Standard-AWS-Regionsnamen für die Amazon Elastic Compute Cloud (Amazon EC2)-Instance oder das Betriebssystem (OS), auf dem die Skripts ausgeführt werden. Weitere Informationen finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI Version 2 und Konfigurieren der AWS CLI in der AWS CLI-Dokumentation.
- Vertrautheit mit AWS- CloudFormation Vorlagen. Weitere Informationen finden Sie unter AWS-CloudFormation Konzepte in der AWS- CloudFormation Dokumentation.
- Python Version 3, installiert und konfiguriert auf der Amazon EC2-Instance oder dem Betriebssystem, auf der/dem die Skripts ausgeführt werden. Weitere Informationen finden Sie in der Python-Dokumentation.

Einschränkungen

- Die Mindestanforderungen für Ihre Quell-DB-Instance von Amazon RDS für Oracle sind:
  - Oracle-Versionen 12c (v12.1.0.2, v12.2.0.1), 18c (v18.0.0.0) und 19c (v19.0.0.0) für die Editionen Enterprise, Standard, Standard One und Standard Two.

  - Obwohl Amazon RDS Oracle 18c (v18.0.0.0) unterstützt, befindet sich diese Version auf einem Veraltungspfad, da Oracle nach dem end-of-support Datum keine Patches mehr für 18c bereitstellt. Weitere Informationen finden Sie unter Oracle in Amazon RDS in der Amazon-RDS-Dokumentation.
  - Amazon RDS für Oracle 11g wird nicht mehr unterstützt.
- Die Mindestanforderungen für Ihre Ziel-DB-Instance von Amazon RDS für PostgreSQL sind:
  - PostgreSQL-Versionen 9 (Versionen 9.5 und 9.6), 10.x, 11.x, 12.x und 13.x

Produktversionen

- Amazon RDS für Oracle DB-Instance Version 12.1.0.2 und höher
- DB-Instance von Amazon RDS für PostgreSQL Version 11.5 und höher
- AWS CLI Version 2
- Die neueste Version von AWS SCT
- Die neueste Version von Python 3

Architektur

Quelltechnologie-Stack

- Amazon RDS für Oracle

Zieltechnologie-Stack

- Amazon RDS für PostgreSQL

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Migration einer DB-Instance von Amazon RDS für Oracle zu einer DB-Instance von Amazon RDS für PostgreSQL mithilfe von AWS DMS- und Python-Skripten.

Das Diagramm zeigt den folgenden Migrationsworkflow:

1. Das Python-Skript verwendet AWS SCT, um eine Verbindung zu den Quell- und Ziel-DB-Instances herzustellen.

2. Der Benutzer startet AWS SCT mit dem Python-Skript, konvertiert den Oracle-Code in PostgreSQL-Code und führt ihn auf der Ziel-DB-Instance aus.
3. Das Python-Skript erstellt AWS DMS-Replikationsaufgaben für die Quell- und Ziel-DB-Instances.
4. Der Benutzer stellt Python-Skripte bereit, um die AWS DMS-Aufgaben zu starten, und stoppt dann die Aufgaben, nachdem die Datenmigration abgeschlossen ist.

Automatisierung und Skalierung

Sie können diese Migration automatisieren, indem Sie Ihrem Python-Skript zusätzliche Parameter und sicherheitsbezogene Änderungen für mehrere Funktionen in einem einzigen Programm hinzufügen.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten. Dieses Muster konvertiert die CSV-Eingabedatei mithilfe eines Python-Skripts in eine JSON-Eingabedatei. Die .json-Datei wird in AWS CLI-Befehlen verwendet, um einen AWS-CloudFormation Stack zu erstellen, der mehrere AWS DMS-Replikationsaufgaben mit Amazon-Ressourcennamen (ARNs), Migrationstypen, Aufgabeneinstellungen und Tabellenzuordnungen erstellt.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen. Dieses Muster verwendet AWS DMS zum Erstellen, Starten und Stoppen von Aufgaben mit einem Python-Skript, das über die Befehlszeile ausgeführt wird, und zum Erstellen der AWS- CloudFormation Vorlage.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Für dieses Muster ist die `-AWSSchemaConversionToolBatch.jar`Datei aus dem installierten AWS SCT-Verzeichnis erforderlich.

Code

Die `cli-sct-dms-cft.zip` Datei (angefügt) enthält den vollständigen Quellcode für dieses Muster.

Polen

Konfigurieren von AWS SCT und Erstellen von Datenbankobjekten in AWS CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie AWS SCT für die Ausführung über die AWS CLI.	1. Konfigurieren Sie die Konfigurationsdetails der Quell- und Zielumgebung in der `database_migration.txt` Datei im folgenden Format:
	`#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432`
	2. Ändern Sie die AWS SCT-Konfigurationsparameter entsprechend Ihren Anforderungen in den folgenden
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dateien: `project_settings.xml` `Oracle_PG_Test_Batch.xml` , und `ORACLE-orcl-to-POSTGRESQL.xml` .	
Führen Sie das Python-Skript run_aws_sct.py aus.	Führen Sie das `run_aws_sct.py` Python-Skript mit dem folgenden Befehl aus: `$ python run_aws_sct.py database_migration.txt` Das Python-Skript konvertiert die Datenbankobjekte von Oracle in PostgreSQL und erstellt SQL-Dateien im PostgreSQL-Format. Das `Database migration assessment report` Skript erstellt auch die PDF-Datei, die Ihnen detaillierte Empfehlungen und Konvertierungsstatistiken für Datenbankobjekte bereitstellt.	DBA
Erstellen Sie Objekte in Amazon RDS for PostgreSQL .	1. Ändern Sie bei Bedarf die von AWS SCT generierten SQL-Dateien manuell. 2. Führen Sie die SQL-Dateien aus und erstellen Sie Objekte in Ihrer DB-Instance von Amazon RDS für PostgreSQL.	DBA

Konfigurieren und Erstellen von AWS DMS-Aufgaben mithilfe der AWS CLI und AWS CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS DMS-Konsole und erstellen Sie eine Replikations-Instance, die Ihren Anforderungen entsprich t. Weitere Informationen finden Sie unter Erstellen einer Replikations-Instance in der AWS DMS-Dokumentation und Wie erstelle ich eine AWS DMS-Replikations-Instance in der AWS Support-Dokumentat ion.	DBA
Erstellen Sie den Quellendp unkt.	Wählen Sie in der AWS DMS-Konsole Endpunkte aus und erstellen Sie dann einen Quellendpunkt für die Oracle-Datenbank entsprechend Ihren Anforderungen. Hinweis: Das zusätzliche Verbindungsattribut muss `numberDataTypeScale` mit einem `-2` Wert sein. Weitere Informationen finden Sie unter Erstellen von Quell- und Zielendpunkten in der AWS DMS-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Zielendpunkt.	Wählen Sie in der AWS DMS-Konsole Endpunkte aus und erstellen Sie dann einen Zielendpunkt für die PostgreSQL-Datenbank entsprechend Ihren Anforderungen. Weitere Informationen finden Sie unter Erstellen von Quell- und Zielendpunkten in der AWS DMS-Dokumentation.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die AWS DMS-Replikationsdetails für die Ausführung über die AWS CLI.	Konfigurieren Sie die AWS DMS-Quell- und Zielendpunkte und Replikationsdetails in der `dms-arn-list.txt` Datei mit dem Quellendpunkt-ARN, dem Zielendpunkt-ARN und dem Replikations-Instance-ARN im folgenden Format:
	`#sourceARN,targetARN,repARN`
	`arn:aws:dms:us-east-1:123456789012:endpoint:EH7AINRUDZ5GOYIY6HVMXECMCQ`
	`arn:aws:dms:us-east-1:123456789012:endpoint:HHJVUV57N7O3CQF4PJZKGIOYY5`
	`arn:aws:dms:us-east-1:123456789012:rep:LL57N77AQQAHHJF4PJFHNEDZ5G`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Python-Skript dms-create-task.py aus, um die AWS DMS-Aufgaben zu erstellen.	1. Führen Sie das `dms-create-task.py` Python-Skript mit dem folgenden Befehl aus: `$ python dms-create-task.py database_migration.txt dms-arn-list.txt <cft-stack-name> <migration-type>` • `database_migration.txt` ist die Textdatei für die Datenbankmigration • `dms-arn-list.txt` ist die ARN-Liste für AWS DMS • `<cft-stack-name>` ist der benutzerdefinierte AWS-CloudFormation Stack-Name • `<migration-type>` ist der Migrationstyp (Volllast, CDC oder full-load-and-cdc) 2. Je nach Migrationstyp können Sie die folgenden Befehle verwenden, um drei Arten von AWS DMS-Aufgaben zu erstellen: • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cli-cft-stack full-load` • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack cdc` • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack full-load-and-cdc` 3. Der AWS- CloudFormation Stack und die AWS DMS-Aufgaben werden erstellt	
Überprüfen Sie, ob AWS DMS-Aufgaben bereit sind.	Überprüfen Sie in der AWS-Konsole, ob sich Ihre AWS DMS-Aufgaben im `Ready` Statusbereich befinden.	DBA

Starten und Stoppen der AWS DMS-Aufgaben mithilfe der AWS CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die AWS DMS-Aufgaben.	Führen Sie das `dms-start-task.py` Python-Skript mit dem folgenden Befehl aus:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ python dms-start-task.py start '<cdc-start-datetime>'` Hinweis: Das Startdatum und die Startzeit müssen im Datentypformat `'DD-MON-YYYY'` oder `'YYYY-MM-DDTHH:MI:SS'` angegeben werden (z. B. `'01-Dec-2019'` oder `'2018-03-08T12:12:12'`) Sie können den AWS DMS-Aufgabenstatus auf der Registerkarte Tabellenstatistiken Ihrer Migrationsaufgaben auf der Seite Aufgaben der AWS DMS-Konsole überprüfen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten.	1. Nachdem die Volllastmigration abgeschlossen ist, wird die Aufgabe kontinuierlich für kontinuierliche Datenänderungen (CDC) ausgeführt. 2. Wenn CDC abgeschlossen ist oder keine Änderungen mehr migriert werden müssen, überprüfen und validieren Sie die Ergebnisse und Daten der Migrationsaufgabe in Ihren Oracle- und PostgreSQL-Datenbanken. 3. Sie können Ihre Daten validieren, indem Sie die Status- und Zählspalten (`Validation state`, `Validation pending`, `Validation failed` `Validation suspended` , und `Validation details`) auf der Registerkarte Tabellenstatistiken Ihrer Datenbankmigrationsaufgabe auf der Seite Aufgaben der AWS DMS-Konsole überprüfen. Weitere Informationen finden Sie unter AWS DMS-Daten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	validierung in der AWS DMS-Dokumentation.	
Halten Sie die AWS DMS-Aufgaben an.	Führen Sie das Python-Skript mit dem folgenden Befehl aus: `$ python dms-start-task.py stop` Hinweis: AWS DMS-Aufgaben werden je nach Validierungsstatus möglicherweise mit dem `failed`Status beendet. Weitere Informationen finden Sie in der Tabelle zur Fehlerbehebung im Abschnitt Zusätzliche Informationen.	DBA

Fehlerbehebung

Problem	Lösung
AWS SCT-Quell- und Zieltestverbindungen schlagen fehl	Konfigurieren Sie die JDBC-Treiberversionen und Regeln für eingehenden Datenverkehr der VPC-Sicherheitsgruppe, um den eingehenden Datenverkehr zu akzeptieren.
Quell- oder Zielendpunkt-Testlauf schlägt fehl	Überprüfen Sie, ob sich die Endpunkte instellungen und die Replikations-Instance im `Available` Status befinden. Überprüfen Sie, ob der Verbindungsstatus des Endpunkts lautet`Successful` . Weitere Informationen finden Sie unter Wie kann ich Fehler bei der AWS DMS-Endpu

Problem	Lösung
	nktkonnektivität beheben? in der AWS Support-Dokumentation.
Volllastausführung schlägt fehl	Überprüfen Sie, ob die Quell- und Zieldaten bank übereinstimmende Datentypen und -größen haben. Weitere Informationen finden Sie unter Fehlerbehebung bei Migrationsaufgaben in AWS DMS in der AWS DMS-Dokumentation.
Fehler bei Validierungsausführungen	Überprüfen Sie, ob die Tabelle über einen Primärschlüssel verfügt, da nicht-primäre Schlüsseltabellen nicht validiert werden. Wenn die Tabelle einen Primärschlüssel und Fehler enthält, überprüfen Sie, ob das zusätzlic he Verbindungsattribut im Quellendpunkt hatnumberDataTypeScale=-2 . Weitere Informationen finden Sie unter Zusätzliche Verbindungsattribute bei Verwendung von Oracle als Quelle für AWS DMS , OracleSettingsund Fehlerbehebung in der AWS DMS-Dokumentation.

Zugehörige Ressourcen

- Installieren von AWS SCT
- Einführung in AWS DMS (Video)
- Verwenden der AWS CLI in AWS CloudFormation
- Verwenden der AWS SCT-Benutzeroberfläche
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden von Oracle als Quelle für AWS SCT
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS

- Quellen für die Datenmigration in AWS DMS
- Ziele für die Datenmigration in AWS DMS
- cloudformation (AWS-CLI-Dokumentation)
- cloudformation create-stack (AWS-CLI-Dokumentation)
- dms (AWS-CLI-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren von Oracle SERIALLY_REUSABLE-Pragma-Paketen zu PostgreSQL

Erstellt von Vinaydi (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle; Open-Source	Technologien: Migration; Datenbanken
AWS-Services: AWS SCT; Amazon Aurora		

Übersicht

Dieses Muster bietet einen step-by-step Ansatz für die Migration von Oracle-Paketen, die als SERIALLY_REUSABLE pragma definiert sind, zu PostgreSQL in Amazon Web Services (AWS). Dieser Ansatz behält die Funktionalität des Pragma SERIALLY_REUSABLE bei.

PostgreSQL unterstützt das Paketkonzept und das SERIALLY_REUSABLE-Pragma nicht. Um ähnliche Funktionen in PostgreSQL zu erhalten, können Sie Schemata für Pakete erstellen und alle zugehörigen Objekte (wie Funktionen, Prozeduren und Typen) innerhalb der Schemata bereitstellen. Um die Funktionalität des SERIALLY_REUSABLE-Pragma zu erreichen, verwendet das in diesem Muster bereitgestellte Beispiel-Wrapper-Funktionsskript ein AWS Schema Conversion Tool (AWS SCT)-Erweiterungspaket .

Weitere Informationen finden Sie unter SERIALLY_REUSABLE Pragma in der Oracle-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die neueste Version von AWS SCT und die erforderlichen Treiber

- Eine Datenbank von Amazon Aurora PostgreSQL -kompatible Edition oder eine Datenbank von Amazon Relational Database Service (Amazon RDS) für PostgreSQL

Produktversionen

- Oracle Database Version 10g und höher

Architektur

Quelltechnologie-Stack

- Oracle Database On-Premises

Zieltechnologie-Stack

- Aurora PostgreSQL – kompatibel oder Amazon RDS für PostgreSQL
- AWS SCT

Migrationsarchitektur

Tools

AWS-Services

- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.

Andere Tools

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.

Polen

Migrieren des Oracle-Pakets mithilfe von AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Konfigurieren Sie die AWS SCT-Konnektivität zur Quelldatenbank. Weitere Informationen finden Sie unter Verwenden von Oracle Database als Quelle für AWS SCT .	DBA, Entwickler
Konvertieren Sie das Skript.	Verwenden Sie AWS SCT, um das Oracle-Paket zu konvertieren, indem Sie die Zieldatenbank als Aurora PostgreSQL-kompatibel auswählen.	DBA, Entwickler
Speichern Sie die .sql-Dateien.	Bevor Sie die .sql-Datei speichern, ändern Sie die Option Projekteinstellungen in AWS SCT in Einzelne Datei pro Stufe . AWS SCT trennt die .sql-Datei je nach Objekttyp in mehrere .sql-Dateien.	DBA, Entwickler
Ändern Sie den Code.	Öffnen Sie die von AWS SCT generierte `init` Funktion und ändern Sie sie wie im Beispiel im Abschnitt Zusätzliche Informationen gezeigt. Es wird eine Variable hinzugefü	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gt, um die Funktionalität zu erreichen`pg_serialize = 0`.	
Testen Sie die Konvertierung.	Stellen Sie die `init` Funktion in der Aurora-PostgreSQL-kompatiblen Datenbank bereit und testen Sie die Ergebnisse.	DBA, Entwickler

Zugehörige Ressourcen

- AWS Schema Conversion Tool
- Amazon RDS
- Amazon-Aurora-Funktionen
- SERIAL_REUSABLE Pragma

Zusätzliche Informationen

```
Source Oracle Code:

CREATE OR REPLACE PACKAGE test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
PROCEDURE function_1
 (test_id number);
PROCEDURE function_2
 (test_id number
 );
END;

CREATE OR REPLACE PACKAGE BODY test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
v_char VARCHAR2(20) := 'shared.airline';
v_num number := 123;

PROCEDURE function_1(test_id number)
```

```
IS
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
v_char:='test1';
function_2(0);
END;

PROCEDURE function_2(test_id number)
is
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
END;
END test_pkg_var;

Calling the above functions

set serveroutput on


EXEC test_pkg_var.function_1(1);


EXEC test_pkg_var.function_2(1);


Target Postgresql Code:


CREATE SCHEMA test_pkg_var;

CREATE OR REPLACE FUNCTION test_pkg_var.init(pg_serialize IN INTEGER DEFAULT 0)

RETURNS void
AS
$BODY$

DECLARE

BEGIN

if aws_oracle_ext.is_package_initialized( 'test_pkg_var' ) AND pg_serialize = 0
```

```
then

return;

end if;

PERFORM aws_oracle_ext.set_package_initialized( 'test_pkg_var' );

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'shared.airline.basecurrency'::CHARACTER

VARYING(100));

PERFORM aws_oracle_ext.set_package_variable('test_pkg_var', 'v_num', 123::integer);

END;

$BODY$

LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_1(pg_serialize int default 1)

RETURNS void
AS

$BODY$
DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'test1'::varchar);

PERFORM test_pkg_var.function_2(0);
END;
```

```
$BODY$
LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_2(IN pg_serialize integer default 1)

RETURNS void

AS

$BODY$

DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

END;
$BODY$
LANGUAGE plpgsql;


Calling the above functions

select test_pkg_var.function_1()

 select test_pkg_var.function_2()
```

Migrieren externer Oracle-Tabellen zu Amazon Aurora PostgreSQL – kompatibel

Erstellt von anuradha chintha (AWS) und Rakesh Raghav (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: Aurora PostgreSQL
R-Typ: Neuarchitektur	Workload: Open-Source	Technologien: Migration; Datenbanken; Modernisierung
AWS-Services: AWS Identity and Access Managemen t ;AWS Lambda ;Amazon S3; Amazon SNS; Amazon Aurora		

Übersicht

Externe Tabellen bieten Oracle die Möglichkeit, Daten abzufragen, die außerhalb der Datenbank in flachen Dateien gespeichert sind. Sie können den ORACLE_LOADER-Treiber verwenden, um auf alle Daten zuzugreifen, die in einem beliebigen Format gespeichert sind und vom SQL*Loader-Dienstprogramm geladen werden können. Sie können Data Manipulation Language (DML) nicht für externe Tabellen verwenden, aber Sie können externe Tabellen für Abfrage-, Join- und Sortiervorgänge verwenden.

Amazon Aurora PostgreSQL -Compatible Edition bietet keine Funktionen, die externen Tabellen in Oracle ähneln. Stattdessen müssen Sie die Modernisierung verwenden, um eine skalierbare Lösung zu entwickeln, die funktionale Anforderungen erfüllt und fehlerhaft ist.

Dieses Muster enthält Schritte zur Migration verschiedener Arten externer Oracle-Tabellen zu Aurora PostgreSQL – kompatible Edition in der Amazon Web Services (AWS) Cloud mithilfe der `-aws_s3`Erweiterung.

Wir empfehlen, diese Lösung gründlich zu testen, bevor Sie sie in einer Produktionsumgebung implementieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- Eine verfügbare mit Aurora PostgreSQL kompatible Datenbank-Instance.
- Eine lokale Oracle-Datenbank mit einer externen Tabelle
- pg.Client-API
- Datendateien

Einschränkungen

- Dieses Muster bietet nicht die Funktionalität, als Ersatz für externe Oracle-Tabellen zu fungieren. Die Schritte und der Beispielcode können jedoch weiter verbessert werden, um Ihre Ziele für die Datenbank-Modernisierung zu erreichen.
- Dateien sollten nicht das Zeichen enthalten, das als Trennzeichen in `aws_s3` Export- und Importfunktionen übergeben wird.

Produktversionen

- Um aus Amazon S3 in RDS für PostgreSQL zu importieren, muss die Datenbank PostgreSQL Version 10.7 oder höher ausführen.

Architektur

Quelltechnologie-Stack

- Oracle

Quellarchitektur

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL – kompatibel

- Amazon CloudWatch
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Darstellung der Lösung.

1. Dateien werden in den S3-Bucket hochgeladen.
2. Die Lambda-Funktion wird initiiert.
3. Die Lambda-Funktion initiiert den DB-Funktionsaufruf.
4. Secrets Manager stellt die Anmeldeinformationen für den Datenbankzugriff bereit.
5. Abhängig von der DB-Funktion wird ein SNS-Alarm erstellt.

Automatisierung und Skalierung

Alle Ergänzungen oder Änderungen an den externen Tabellen können mit Metadatenwartung behandelt werden.

Tools

- Amazon Aurora PostgreSQL – kompatibel – Amazon Aurora PostgreSQL – Kompatible Edition ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-kompatible relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Kosteneffizienz von Open-Source-Datenbanken kombiniert.
- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services. Mit nur einem Tool zum Herunterladen und Konfigurieren können Sie mehrere AWS-Services über die Befehlszeile steuern und über Skripts automatisieren.
- Amazon CloudWatch – Amazon CloudWatch überwacht Amazon S3-Ressourcen und -Auslastung.
- AWS Lambda – AWS Lambda ist ein Serverless-Compute-Service, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern, die Erstellung einer Workload-fähigen Cluster-Skalierungslogik, die Aufrechterhaltung von Ereignisintegrationen oder die Verwaltung von

Laufzeiten unterstützt. In diesem Muster führt Lambda die Datenbankfunktion immer dann aus, wenn eine Datei in Amazon S3 hochgeladen wird.

- AWS Secrets Manager – AWS Secrets Manager ist ein Service zum Speichern und Abrufen von Anmeldeinformationen. Mit Secrets Manager können Sie fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager ersetzen, um das Secret programmgesteuert abzurufen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) bietet eine Speicherebene zum Empfangen und Speichern von Dateien für die Verwendung und Übertragung zum und vom Aurora PostgreSQL -kompatiblen Cluster.
- aws_s3 – Die `aws_s3` Erweiterung integriert Amazon S3 und Aurora PostgreSQL – kompatibel.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients. In diesem Muster wird Amazon SNS verwendet, um Benachrichtigungen zu senden.

Code

Jedes Mal, wenn eine Datei im S3-Bucket abgelegt wird, muss eine DB-Funktion von der Verarbeitungsanwendung oder der Lambda-Funktion erstellt und aufgerufen werden. Weitere Informationen finden Sie im Code (angefügt).

Polen

Erstellen einer externen Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Quelldatenbank eine externe Datei hinzu.	Erstellen Sie eine externe Datei und verschieben Sie sie in das `oracle` Verzeichnis .	DBA

Konfigurieren des Ziels (Aurora PostgreSQL – kompatibel)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora-PostgreSQL-Datenbank.	Erstellen Sie eine DB-Instance in Ihrem mit Amazon Aurora	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PostgreSQL kompatiblen Cluster.	
Erstellen Sie ein Schema, eine aws_s3-Erweiterung und Tabellen.	Verwenden Sie den Code unter `ext_tbl_scripts` im Abschnitt Zusätzliche Informationen. Die Tabellen enthalten tatsächliche Tabellen, Staging-Tabellen, Fehler- und Protokolltabellen sowie eine Metatabelle.	DBA, Entwickler
Erstellen Sie die DB-Funktion.	Um die DB-Funktion zu erstellen, verwenden Sie den Code unter `load_external_table_latest` Funktion im Abschnitt Zusätzliche Informationen.	DBA, Entwickler

Erstellen und Konfigurieren der Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle.	Erstellen Sie eine Rolle mit Berechtigungen für den Zugriff auf Amazon S3 und Amazon Relational Database Service (Amazon RDS). Diese Rolle wird Lambda zum Ausführen des Musters zugewiesen.	DBA
So erstellen Sie die Lambda-Funktion:	Erstellen Sie eine Lambda-Funktion, die den Dateinamen aus Amazon S3 liest (z. B. `file_key = info.get(`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`'object', {}).get('key') )` und die DB-Funktion aufruft (z. B. `curs.callproc("load_external_tables", [file_key]) )` mit dem Dateinamen als Eingabeparameter. Abhängig vom Ergebnis des Funktionsaufrufs wird eine SNS-Benachrichtigung initiiert (z. B. `client.publish(TopicArn='arn:',Message='fileloadsuccess',Subject='fileloadsuccess') )`. Je nach Ihren Geschäftsanforderungen können Sie bei Bedarf eine Lambda-Funktion mit zusätzlichem Code erstellen. Weitere Informationen finden Sie in der Lambda-Dokumentation.	
Konfigurieren Sie einen S3-Bucket-Ereignisauslöser.	Konfigurieren Sie einen Mechanismus zum Aufrufen der Lambda-Funktion für alle Ereignisse zur Objektverstellung im S3-Bucket.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Secret.	Erstellen Sie mithilfe von Secrets Manager einen geheimen Namen für die Datenbankanmeldeinformationen. Übergeben Sie das Secret in der Lambda-Funktion.	DBA
Laden Sie die Lambda-Unterstützungsdateien hoch.	Laden Sie eine ZIP-Datei hoch, die die Lambda-Unterstützungspakete und das angehängte Python-Skript für die Verbindung mit Aurora PostgreSQL – kompatibel enthält. Der Python-Code ruft die Funktion auf, die Sie in der Datenbank erstellt haben.	DBA
Erstellen Sie ein SNS-Thema.	Erstellen Sie ein SNS-Thema, um E-Mails für den Erfolg oder Misserfolg des Datenladevorgangs zu senden.	DBA

Integration mit Amazon S3 hinzufügen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie in der Amazon S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	allen AWS-Konten gemeinsam genutzt.	
Erstellen Sie IAM-Richtlinien.	Um die AWS Identity and Access Management (IAM)-Richtlinien zu erstellen , verwenden Sie den Code unter `s3bucketpolicy_for_import` im Abschnitt Zusätzliche Informationen.	DBA
Erstellen Sie Rollen.	Erstellen Sie zwei Rollen für Aurora PostgreSQL – kompatibel, eine Rolle für Import und eine Rolle für Export. Weisen Sie den Rollen die entsprechenden Richtlinien zu.	DBA
Fügen Sie die Rollen an den Aurora PostgreSQL -kompatiblen Cluster an.	Fügen Sie unter Rollen verwalten die Rollen Importieren und Exportieren an den Aurora-PostgreSQL-Cluster an.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie unterstützende Objekte für Aurora PostgreSQL – kompatibel.	Verwenden Sie für die Tabellenskripte den Code unter `ext_tbl_scripts` im Abschnitt Zusätzliche Informationen. Verwenden Sie für die benutzerdefinierte Funktion den Code unter `load_external_Table_latest` im Abschnitt Zusätzliche Informationen.	DBA

Verarbeiten einer Testdatei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie eine Datei in den S3-Bucket hoch.	Um eine Testdatei in den S3-Bucket hochzuladen, verwenden Sie die -Konsole oder den folgenden Befehl in AWS CLI. `aws s3 cp /Users/Desktop/ukpost/exttbl/"testing files"/aps s3://s3importtest/inputext/aps` Sobald die Datei hochgeladen ist, initiiert ein Bucket-Ereignis die Lambda-Funktion, die die Aurora-PostgreSQL-kompatible Funktion ausführt.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Daten sowie die Protokoll- und Fehlerdateien.	Die Aurora-PostgreSQL-kompatible Funktion lädt die Dateien in die Haupttabelle und erstellt - `.log` und -`.bad`Dateien im S3-Bucket.	DBA
Überwachen Sie die Lösung.	Überwachen Sie in der Amazon- CloudWatch Konsole die Lambda-Funktion.	DBA

Zugehörige Ressourcen

- Amazon S3-Integration
- Amazon S3
- Arbeiten mit Amazon Aurora PostgreSQL – Kompatible Edition
- AWS Lambda
- Amazon CloudWatch
- AWS Secrets Manager
- Einrichten von Amazon SNS-Benachrichtigungen

Zusätzliche Informationen

ext_table_scripts

```
CREATE EXTENSION aws_s3 CASCADE;
CREATE TABLE IF NOT EXISTS meta_EXTERNAL_TABLE
(
    table_name_stg character varying(100) ,
    table_name character varying(100)  ,
    col_list character varying(1000)  ,
    data_type character varying(100)  ,
    col_order numeric,
    start_pos numeric,
    end_pos numeric,
    no_position character varying(100)  ,
```

```
    date_mask character varying(100)  ,
    delimeter character(1)  ,
    directory character varying(100)  ,
    file_name character varying(100)  ,
    header_exist character varying(5)
);
CREATE TABLE IF NOT EXISTS ext_tbl_stg
(
    col1 text
);
CREATE TABLE IF NOT EXISTS error_table
(
    error_details text,
    file_name character varying(100),
    processed_time timestamp without time zone
);
CREATE TABLE IF NOT EXISTS log_table
(
    file_name character varying(50) COLLATE pg_catalog."default",
    processed_date timestamp without time zone,
    tot_rec_count numeric,
    proc_rec_count numeric,
    error_rec_count numeric
);
sample insert scripts of meta data:
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'source_filename', 'character varying', 2, 8, 27, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'record_type_identifier', 'character varying', 3, 28, 30, NULL, NULL, NULL,
 'databasedev', 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'fad_code', 'numeric', 4, 31, 36, NULL, NULL, NULL, 'databasedev', 'externalinterface/
loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
```

```
 'session_sequence_number', 'numeric', 5, 37, 42, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'transaction_sequence_number', 'numeric', 6, 43, 48, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
```

s3bucketpolicy_für den Import

```
---Import role policy
--Create an IAM policy to allow, Get,  and list actions on S3 bucket
 {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest",
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
--Export Role policy
--Create an IAM policy to allow, put,  and list actions on S3 bucket
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3export",
            "Action": [
                "S3:PutObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest/*"
```

```
            ]
        }
    ]
}
```

Beispiel-DB-Funktion load_external_tables_latest

```
CREATE OR REPLACE FUNCTION public.load_external_tables(pi_filename text)
 RETURNS character varying
 LANGUAGE plpgsql
AS $function$
/* Loading data from S3 bucket into a APG table */
DECLARE
 v_final_sql TEXT;
 pi_ext_table TEXT;
 r refCURSOR;
 v_sqlerrm text;
 v_chunk numeric;
 i integer;
 v_col_list TEXT;
 v_postion_list CHARACTER VARYING(1000);
 v_len  integer;
 v_delim varchar;
 v_file_name CHARACTER VARYING(1000);
 v_directory CHARACTER VARYING(1000);
 v_table_name_stg CHARACTER VARYING(1000);
 v_sql_col TEXT;
 v_sql TEXT;
 v_sql1 TEXT;
 v_sql2 TEXT;
 v_sql3 TEXT;
 v_cnt integer;
 v_sql_dynamic TEXT;
 v_sql_ins TEXT;
 proc_rec_COUNT integer;
 error_rec_COUNT integer;
 tot_rec_COUNT integer;
 v_rec_val integer;
 rec record;
 v_col_cnt integer;
 kv record;
 v_val text;
 v_header text;
```

```
 j integer;
 ERCODE VARCHAR(5);
 v_region text;
 cr CURSOR FOR
 SELECT distinct DELIMETER,
   FILE_NAME,
   DIRECTORY
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
   AND DELIMETER IS NOT NULL;


 cr1 CURSOR FOR
   SELECT   col_list,
   data_type,
   start_pos,
   END_pos,
   concat_ws('',' ',TABLE_NAME_STG) as TABLE_NAME_STG,
   no_position,date_mask
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
 order by col_order asc;
cr2 cursor FOR
SELECT  distinct table_name,table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);


BEGIN
 -- PERFORM utl_file_utility.init();
   v_region := 'us-east-1';
   /* find tab details from file name */


   --DELETE FROM  ERROR_TABLE WHERE file_name= pi_filename;
  -- DELETE FROM  log_table WHERE file_name= pi_filename;


 BEGIN


   SELECT distinct table_name,table_name_stg INTO strict pi_ext_table,v_table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);
```

```
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
    raise notice 'error 1,%',sqlerrm;
    pi_ext_table := null;
    v_table_name_stg := null;
      RAISE USING errcode = 'NTFIP' ;
    when others then
        raise notice 'error others,%',sqlerrm;
 END;
 j :=1 ;

for rec in  cr2
 LOOP




  pi_ext_table     := rec.table_name;
  v_table_name_stg := rec.table_name_stg;
  v_col_list := null;


 IF pi_ext_table IS NOT NULL
  THEN
    --EXECUTE concat_ws('','truncate table  ' ,pi_ext_table) ;
   EXECUTE concat_ws('','truncate table  ' ,v_table_name_stg) ;




       SELECT distinct DELIMETER INTO STRICT v_delim
       FROM  meta_EXTERNAL_TABLE
       WHERE table_name = pi_ext_table;


       IF v_delim IS NOT NULL THEN
     SELECT distinct DELIMETER,
       FILE_NAME,
       DIRECTORY ,
       concat_ws('',' ',table_name_stg),
       case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
     INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
     FROM  meta_EXTERNAL_TABLE
     WHERE table_name = pi_ext_table
```

```
       AND DELIMETER IS NOT NULL;


    IF    upper(v_delim) = 'CSV'
    THEN
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3 ( ''',
      v_table_name_stg,''','''',
      ''DELIMITER '''','''' CSV HEADER QUOTE '''''''''', aws_commons.create_s3_uri
( ''',
      v_directory,''','''',v_file_name,''', ''',v_region,'''))');
      ELSE
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
          v_table_name_stg, ''','''', ''DELIMITER AS ''''^''''',''',','
         aws_commons.create_s3_uri
          ( ''',v_directory, ''','''',
          v_file_name, ''',',
           '''',v_region,''')
         )');
         raise notice 'v_sql , %',v_sql;
      begin
       EXECUTE  v_sql;
      EXCEPTION
        WHEN OTHERS THEN
          raise notice 'error 1';
        RAISE USING errcode = 'S3IMP' ;
      END;


      select count(col_list) INTO v_col_cnt
      from  meta_EXTERNAL_TABLE where table_name = pi_ext_table;







       -- raise notice 'v_sql 2, %',concat_ws('','update ',v_table_name_stg, ' set
col1 = col1||''',v_delim,''''');


      execute concat_ws('','update ',v_table_name_stg, ' set col1 =
col1||''',v_delim,''''');
```

```
      i :=1;
      FOR rec in cr1
      loop
      v_sql1 := concat_ws('',v_sql1,'split_part(col1,''',v_delim,''',', i,')',' as
',rec.col_list,',');
      v_sql2 := concat_ws('',v_sql2,rec.col_list,',');
  --    v_sql3 := concat_ws('',v_sql3,'rec.',rec.col_list,'::',rec.data_type,',');


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                coalesce((trim(split_part(col1,''',v_delim,''',',
i,')))::NUMERIC,0)::',rec.data_type,' END as ',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''99990101''),''YYYYMMDD'')::',rec.data_type,' END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
 'MM/DD/YYYY hh24:mi:ss'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''01/01/9999 0024:00:00''),''MM/DD/YYYY hh24:mi:ss'')::',rec.data_type,' END as
',rec.col_list,',');
         ELSE
       v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                 coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''''):',rec.data_type,' END as ',rec.col_list,',') ;
      END case;
```

```
       i :=i+1;
       end loop;


         -- raise notice 'v_sql 3, %',v_sql3;


       SELECT trim(trailing ' ' FROM v_sql1) INTO v_sql1;
       SELECT trim(trailing ',' FROM v_sql1) INTO v_sql1;


       SELECT trim(trailing ' ' FROM v_sql2) INTO v_sql2;
       SELECT trim(trailing ',' FROM v_sql2) INTO v_sql2;


       SELECT trim(trailing ' ' FROM v_sql3) INTO v_sql3;
       SELECT trim(trailing ',' FROM v_sql3) INTO v_sql3;


       END IF;
      raise notice 'v_delim , %',v_delim;


     EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)  INTO v_cnt;


    raise notice 'stg cnt , %',v_cnt;


    /* if upper(v_delim) = 'CSV' then
       v_sql_ins := concat_ws('', ' SELECT * from ' ,v_table_name_stg );
     else
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       END IF;*/


v_chunk := v_cnt/100;
```

```
for i in 1..101
loop
     BEGIN
    -- raise notice 'v_sql , %',v_sql;
       -- raise notice 'Chunk number , %',i;
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ' offset ',v_chunk*(i-1), ' limit ',v_chunk,') sub ');


     v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
     -- raise notice 'select statement , %',v_sql_ins;
          -- v_sql := null;
     -- EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins, 'offset
 ',v_chunk*(i-1), ' limit ',v_chunk );
     --v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins );


     -- raise notice 'insert statement , %',v_sql;


    raise NOTICE 'CHUNK START %',v_chunk*(i-1);
   raise NOTICE 'CHUNK END %',v_chunk;


     EXECUTE v_sql;


  EXCEPTION
       WHEN OTHERS THEN
       -- v_sql_ins := concat_ws('',' SELECT ',v_sql1, '  from (select col1 from
 ' ,v_table_name_stg , ' )sub ');
         -- raise notice 'Chunk number for cursor , %',i;


    raise NOTICE 'Cursor - CHUNK START %',v_chunk*(i-1);
   raise NOTICE 'Cursor -  CHUNK END %',v_chunk;
         v_sql_ins := concat_ws('',' SELECT ',v_sql3, '  from (select col1 from
 ' ,v_table_name_stg , ' )sub ');


         v_final_sql := REPLACE (v_sql_ins, ''''::text, ''''''::text);
        -- raise notice 'v_final_sql %',v_final_sql;
```

```
        v_sql :=concat_ws('','do $a$ declare  r refcursor;v_sql text; i
 numeric;v_conname text;  v_typ  ',pi_ext_table,'[]; v_rec  ','record',';
          begin









          open r for execute ''select col1 from ',v_table_name_stg ,'  offset
 ',v_chunk*(i-1), ' limit ',v_chunk,''';
          loop
          begin
          fetch r into v_rec;
          EXIT WHEN NOT FOUND;




          v_sql := concat_ws('''',''insert into  ',pi_ext_table,' SELECT ',REPLACE
 (v_sql3, ''''::text, ''''''::text) , '  from ( select ''''''',v_rec.col1,''''''' as
 col1) v'');
           execute v_sql;


          exception
           when others then
         v_sql := ''INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''''''','''''Error
 Name: ''''',$$''||SQLERRM||''$$,'''''Error State: ''''',''''''||
SQLSTATE||'''''',''''record : ''''',$$''||v_rec.col1||''$$),'''''||
pi_filename||'''''',now())'';


             execute v_sql;
            continue;
          end ;
          end loop;
          close r;
          exception
          when others then
        raise;
          end ; $a$');
     -- raise notice ' inside excp v_sql %',v_sql;
         execute v_sql;
```

```
     --  raise notice 'v_sql %',v_sql;
      END;
 END LOOP;
    ELSE


    SELECT distinct DELIMETER,FILE_NAME,DIRECTORY ,concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
      INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table                  ;
    v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
      v_table_name_stg, ''','''', ''DELIMITER AS ''''#'''' ',v_header,' '','','
     aws_commons.create_s3_uri
      ( ''',v_directory, ''','''',
      v_file_name, ''',',
       '''',v_region,''')
     )');
        EXECUTE  v_sql;


    FOR rec in cr1
    LOOP


     IF rec.start_pos IS NULL AND rec.END_pos IS NULL AND rec.no_position = 'recnum'
     THEN
       v_rec_val := 1;
     ELSE


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
              THEN null
               ELSE
               coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1)))::NUMERIC,0)::',rec.data_type,' END as
',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
```

```
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''99990101''),''YYYYMMDD''):::',rec.data_type,'
END as ',rec.col_list,',');
       WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDDHH24MISS'
       THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''9999010100240000''),''YYYYMMDDHH24MISS''):::',rec.data_
END as ',rec.col_list,',');
        ELSE
      v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                 coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),'''')::',rec.data_type,' END as
',rec.col_list,',') ;
     END case;


    END IF;
    v_col_list := concat_ws('',v_col_list ,v_sql1);
   END LOOP;




         SELECT trim(trailing ' ' FROM v_col_list) INTO v_col_list;
         SELECT trim(trailing ',' FROM v_col_list) INTO v_col_list;


         v_sql_col   :=  concat_ws('',trim(trailing ',' FROM v_col_list) , ' FROM
 ',v_table_name_stg,' WHERE col1 IS NOT NULL AND length(col1)>0 ');




         v_sql_dynamic := v_sql_col;
```

```
          EXECUTE  concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg) INTO v_cnt;




        IF v_rec_val = 1 THEN
            v_sql_ins := concat_ws('',' select row_number() over(order by ctid) as
line_number ,' ,v_sql_dynamic) ;


        ELSE
              v_sql_ins := concat_ws('',' SELECT' ,v_sql_dynamic) ;
          END IF;


    BEGIN
      EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
          EXCEPTION
             WHEN OTHERS THEN
         IF v_rec_val = 1 THEN
                v_final_sql := ' select row_number() over(order by ctid) as
line_number ,col1 from ';
              ELSE
               v_final_sql := ' SELECT col1 from';
             END IF;
      v_sql :=concat_ws('','do $a$ declare  r refcursor;v_rec_val numeric :=
',coalesce(v_rec_val,0),';line_number numeric; col1 text; v_typ  ',pi_ext_table,'[];
v_rec  ',pi_ext_table,';
            begin
            open r for execute ''',v_final_sql, ' ',v_table_name_stg,' WHERE col1 IS
NOT NULL AND length(col1)>0 '' ;
            loop
            begin
            if   v_rec_val = 1 then
            fetch r into line_number,col1;
            else
            fetch r into col1;
            end if;


            EXIT WHEN NOT FOUND;
             if v_rec_val = 1 then
             select line_number,',trim(trailing ',' FROM v_col_list) ,' into v_rec;
```

```
             else
               select ',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             end if;


            insert into  ',pi_ext_table,' select v_rec.*;
             exception
             when others then
              INSERT INTO  ERROR_TABLE VALUES (concat_ws('''','Error Name:
'',SQLERRM,''Error State: '',SQLSTATE,''record : '',v_rec),''',pi_filename,''',now());
             continue;
             end ;
              end loop;
            close r;
             exception
             when others then
             raise;
             end ; $a$');
        execute v_sql;


    END;


        END IF;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  ' ,pi_ext_table)   INTO proc_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  error_table WHERE file_name
='''',pi_filename,''' and processed_time::date = clock_timestamp()::date')  INTO
error_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)   INTO tot_rec_COUNT;


  INSERT INTO  log_table values(pi_filename,now(),tot_rec_COUNT,proc_rec_COUNT,
error_rec_COUNT);


  raise notice 'v_directory, %',v_directory;
```

```
   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT
 replace(trim(substring(error_details,position(''('' in
 error_details)+1),'')''),'','','';''),file_name,processed_time FROM  error_table WHERE
 file_name = '''||pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );


raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  log_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.log', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );




   END IF;
 j := j+1;
 END LOOP;


       RETURN 'OK';
EXCEPTION
    WHEN  OTHERS THEN
  raise notice 'error %',sqlerrm;
   ERCODE=SQLSTATE;
```

```
   IF ERCODE = 'NTFIP' THEN
     v_sqlerrm := concat_Ws('',sqlerrm,'No data for the filename');
   ELSIF ERCODE = 'S3IMP' THEN
    v_sqlerrm := concat_Ws('',sqlerrm,'Error While exporting the file from S3');
   ELSE
      v_sqlerrm := sqlerrm;
   END IF;


 select distinct directory into v_directory from  meta_EXTERNAL_TABLE;




 raise notice 'exc v_directory, %',v_directory;


   raise notice 'exc pi_filename, %',pi_filename;


   raise notice 'exc v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  error_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );
    RETURN null;
END;
$function$
```

Migrieren von funktionsbasierten Indizes von Oracle zu PostgreSQL

Erstellt von Veeranjaney Bol Grandhi (AWS) und Navah Boluri (AWS)

Umgebung: Produktion	Quelle: Oracle	Ziel: PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken

Übersicht

Indizes sind eine gängige Methode zur Verbesserung der Datenbankleistung. Ein Index ermöglicht es dem Datenbankserver, bestimmte Zeilen viel schneller zu finden und abzurufen als ohne Index. Indizes erhöhen jedoch auch den Overhead für das Datenbanksystem als Ganzes, daher sollten sie sinnvoll verwendet werden. Funktionsbasierte Indizes, die auf einer Funktion oder einem Ausdruck basieren, können mehrere Spalten und mathematische Ausdrücke umfassen. Ein funktionsbasierter Index verbessert die Leistung von Abfragen, die den Indexausdruck verwenden.

PostgreSQL unterstützt nicht die Erstellung von funktionsbasierten Indizes mit Funktionen, deren Volatilität als stabil definiert ist. Sie können jedoch ähnliche Funktionen mit Volatilität wie erstellen `IMMUTABLE`und sie bei der Indexerstellung verwenden.

Eine -`IMMUTABLE`Funktion kann die Datenbank nicht ändern, und es wird garantiert, dass sie bei gleichen Argumenten dauerhaft dieselben Ergebnisse zurückgibt. Diese Kategorie ermöglicht es dem Optimierer, die Funktion vorab zu bewerten, wenn eine Abfrage sie mit konstanten Argumenten aufruft.

Dieses Muster hilft bei der Migration der funktionsbasierten Indizes von Oracle`to_date`, wenn es mit Funktionen wie `to_char`, und `to_number` zum PostgreSQL-Äquivalent verwendet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto
- Eine Oracle-Quelldatenbank-Instance mit eingerichtetem und ausgeführtem Listener-Service
- Vertrautheit mit PostgreSQL-Datenbanken

Einschränkungen

- Die maximale Datenbankgröße beträgt 64 TB.
- Funktionen, die bei der Indexerstellung verwendet werden, müssen IMMUTABLE sein.

Produktversionen

- Alle Oracle-Datenbank-Editionen für die Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c
- PostgreSQL-Versionen 9.6 und höher

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank On-Premises oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance oder einer Amazon RDS for Oracle-DB-Instance

Zieltechnologie-Stack

- Jede PostgreSQL-Engine

Tools

- pgAdmin 4 ist ein Open-Source-Verwaltungstool für Postgres. Das Tool pgAdmin 4 bietet eine grafische Oberfläche zum Erstellen, Verwalten und Verwenden von Datenbankobjekten.
- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung (IDE) für die Entwicklung und Verwaltung von Oracle Database in herkömmlichen und Cloud-Bereitstellungen.

Polen

Erstellen eines funktionsbasierten Index mit einer Standardfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen funktions basierten Index für eine Spalte mithilfe der Funktion to_char.	Verwenden Sie den folgenden Code, um den funktions basierten Index zu erstellen.
	
	`postgres=# create table funcindex( col1 timestamp without time zone);`
	`CREATE TABLE`
	`postgres=# insert into funcindex values (now());`
	`INSERT 0 1`
	`postgres=# select * from funcindex;`
	`col1`
	`----------`
	`2022-08-09 16:00:57.77414`
	`(1 rows)`
	
	`postgres=# create index funcindex_idx on funcindex(to_char(col1,'DD-MM-YYYY HH24:MI:SS'));`
	`ERROR: functions in index expression must be marked IMMUTABLE`
	
	Hinweis: PostgreSQL erlaubt das Erstellen eines funktions
		DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	basierten Index ohne die `-IMMUTABLE` Klausel nicht.	
Überprüfen Sie die Volatilität der Funktion.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um die Volatilität der Funktion zu überprüfen.	DBA

Erstellen von funktionsbasierten Indizes mithilfe einer Wrapper-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Wrapper-Funktion.	Um eine Wrapper-Funktion zu erstellen, verwenden Sie den Code im Abschnitt Zusätzliche Informationen.	PostgreSQL-Entwickler
Erstellen Sie einen Index mithilfe der Wrapper-Funktion.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um eine benutzerdefinierte Funktion mit dem Schlüsselwort `IMMUTABLE` im selben Schema wie die Anwendung zu erstellen, und verweisen Sie im Indexerstellungsskript darauf. Wenn eine benutzerdefinierte Funktion in einem gemeinsamen Schema (aus dem vorherigen Beispiel) erstellt wird, aktualisieren Sie wie `search_path` gezeigt.	DBA, PostgreSQL-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ALTER ROLE <ROLENAME> set search_path=$user, COMMON;`	

Validieren der Indexerstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Indexerstellung.	Überprüfen Sie, ob der Index basierend auf Abfragezugriffsmustern erstellt werden muss.	DBA
Überprüfen Sie, ob der Index verwendet werden kann.	Um zu überprüfen, ob der funktionsbasierte Index vom PostgreSQL Optimizer übernommen wird, führen Sie eine SQL-Anweisung mit explain oder explain analyze aus. Verwenden Sie den Code im Abschnitt Zusätzliche Informationen. Sammeln Sie nach Möglichkeit auch die Tabellenstatistiken. Hinweis: Wenn Sie den Erläuterungsplan feststellen, hat der PostgreSQL-Optimierer aufgrund der Prädikatbedingung einen funktionsbasierten Index ausgewählt.	DBA

Zugehörige Ressourcen

- Funktionsbasierte Indizes (Oracle-Dokumentation)
- Indizes für Ausdrücke (PostgreSQL-Dokumentation)
- PostgreSQL-Volatilität (PostgreSQL-Dokumentation)
- PostgreSQL search_path (PostgreSQL-Dokumentation)
- Oracle Database 19c zu Amazon Aurora PostgreSQL Migration Playbook

Zusätzliche Informationen

Erstellen einer Wrapper-Funktion

```
CREATE OR REPLACE FUNCTION myschema.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
```

Erstellen eines Index mithilfe der Wrapper-Funktion

```
postgres=# create function common.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
CREATE FUNCTION
postgres=# create index funcindex_idx on funcindex(common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS'));
CREATE INDEX
```

Überprüfen Sie die Volatilität der Funktion

```
SELECT DISTINCT p.proname as "Name",p.provolatile as "volatility" FROM
 pg_catalog.pg_proc p
 LEFT JOIN pg_catalog.pg_namespace n ON n.oid = p.pronamespace
 LEFT JOIN pg_catalog.pg_language l ON l.oid = p.prolang
 WHERE n.nspname OPERATOR(pg_catalog.~) '^(pg_catalog)$' COLLATE pg_catalog.default AND
 p.proname='to_char'GROUP BY p.proname,p.provolatile
ORDER BY 1;
```

Überprüfen, ob der Index verwendet werden kann

```
explain analyze <SQL>
```

```
postgres=# explain select col1 from funcindex where common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS') = '09-08-2022 16:00:57';
                                                    QUERY PLAN
-------------------------------------------------------------------------------------------------------
 Index Scan using funcindex_idx on funcindex  (cost=0.42..8.44 rows=1 width=8)
   Index Cond: ((common.to_char(col1, 'DD-MM-YYYY HH24:MI:SS'::character
 varying))::text = '09-08-2022 16:00:57'::text)
(2 rows)
```

Migrieren von nativen Oracle-Funktionen zu PostgreSQL mithilfe von Erweiterungen

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle; Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon EC2; Amazon RDS		

Übersicht

Dieses Migrationsmuster bietet step-by-step Anleitungen für die Migration einer Datenbank-Instance von Amazon Relational Database Service (Amazon RDS) für Oracle zu einer Datenbank von Amazon RDS für PostgreSQL oder Amazon Aurora PostgreSQL -kompatible Edition, indem die `orafce` Erweiterungen `aws_oracle_ext` und in den nativen integrierten Code von PostgreSQL (`psql`) geändert werden. Dies spart Verarbeitungszeit.

Das Muster beschreibt eine manuelle Offline-Migrationsstrategie ohne Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen.

Der Migrationsprozess verwendet AWS Schema Conversion Tool (AWS SCT) mit den `orafce` Erweiterungen `aws_oracle_ext` und , um ein Datenbankschema von Amazon RDS für Oracle in ein mit Amazon RDS für PostgreSQL oder Aurora PostgreSQL kompatibles Datenbankschema zu konvertieren. Anschließend wird der Code manuell in von PostgreSQL unterstützten `psql` nativen integrierten Code geändert. Dies liegt daran, dass sich die Erweiterungsaufrufe auf die Codeverarbeitung auf dem PostgreSQL-Datenbankserver auswirken und nicht der gesamte Erweiterungscode vollständig beschwert oder mit dem PostgreSQL-Code kompatibel ist.

Dieses Muster konzentriert sich hauptsächlich auf die manuelle Migration von SQL-Codes mit AWS SCT und den Erweiterungen `aws_oracle_ext` und `orafce`. Sie konvertieren die bereits verwendeten Erweiterungen in native `psql`integrierte PostgreSQL (). Anschließend entfernen Sie alle Verweise auf die Erweiterungen und konvertieren die Codes entsprechend.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Betriebssystem (Windows oder Mac) oder Amazon EC2-Instance (in Betrieb)
- Orafce

Einschränkungen

Nicht alle Oracle-Funktionen, die - `aws_oracle_ext` oder -`orafce`Erweiterungen verwenden, können in native PostgreSQL-Funktionen konvertiert werden. Möglicherweise sind manuelle Überarbeitungen erforderlich, um sie mit PostgreSQL-Bibliotheken zu kompilieren.

Ein Nachteil der Verwendung von AWS SCT-Erweiterungen ist die langsame Leistung beim Ausführen und Abrufen der Ergebnisse. Die Kosten sind aus dem einfachen PostgreSQL EXPLAIN-Plan (Ausführungsplan einer -Anweisung) für die Oracle-`SYSDATE`Funktionsmigration zur PostgreSQL-`NOW()`Funktion zwischen allen drei Codes (`aws_oracle_ext`, und `psql` Standard) zu verstehen`orafce`, wie im Abschnitt Leistungsvergleichsprüfung im angehängten Dokument erläutert.

Produktversionen

- Quelle:Amazon RDS for Oracle Database 10.2 und höher (für 10.x), 11g (11.2.0.3.v1 und höher) und bis zu 12.2, 18c und 19c (und höher) für Enterprise Edition, Standard Edition, Standard Edition 1 und Standard Edition 2
- Ziel : Amazon RDS for PostgreSQL oder Aurora PostgreSQL – Kompatible Datenbank 9.4 und höher (für 9.x), 10.x, 11.x, 12.x, 13.x und 14.x (und höher)
- AWS SCT: Neueste Version (dieses Muster wurde mit 1.0.632 getestet)
- Orafce : Neueste Version (dieses Muster wurde mit 3.9.0 getestet)

Architektur

Quelltechnologie-Stack

- Eine Datenbank-Instance von Amazon RDS für Oracle mit Version 12.1.0.2.v18

Zieltechnologie-Stack

- Eine mit Amazon RDS for PostgreSQL oder Aurora PostgreSQL kompatible Datenbank-Instance mit Version 11.5

Datenbankmigrationsarchitektur

Das folgende Diagramm stellt die Datenbankmigrationsarchitektur zwischen den Oracle-Quell- und PostgreSQLZieldatenbanken dar. Die Architektur umfasst AWS Cloud, eine Virtual Private Cloud (VPC), Availability Zones, ein privates Subnetz, eine Datenbank von Amazon RDS für Oracle, AWS SCT, eine mit Amazon RDS für PostgreSQL oder Aurora PostgreSQL kompatible Datenbank, Erweiterungen für Oracle (`aws_oracle_ext` und `orafce`) und SQL-Dateien (Struktured Query Language).

1. Starten Sie die DB-Instance von Amazon RDS für Oracle (Quell-DB).
2. Verwenden Sie AWS SCT mit den `orafce` Erweiterungspaketen `aws_oracle_ext` und , um den Quellcode von Oracle in PostreSQL zu konvertieren.
3. Die Konvertierung erzeugt von PostgreSQL unterstützte migrierte .sql-Dateien.
4. Konvertieren Sie die nicht konvertierten Oracle-Erweiterungscodes manuell in PostgreSQL-`psql`Codes ().
5. Die manuelle Konvertierung erzeugt von PostgreSQL unterstützte konvertierte .sql-Dateien.
6. Führen Sie diese SQL-Dateien auf Ihrer Amazon RDS for PostgreSQL-DB-Instance (Ziel-DB) aus.

Tools

Tools

AWS-Services

- AWS SCT – AWS Schema Conversion Tool (AWS SCT) konvertiert Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere. Sie können das relationale Online Transactional Processing (OLTP)-Schema oder das Data-Warehouse-Schema konvertieren. Ihr konvertiertes Schema eignet sich für eine DB-Instance von Amazon RDS für MySQL, einen DB-Cluster von Amazon Aurora, eine DB-Instance von Amazon RDS für PostgreSQL oder einen Amazon-Redshift-Cluster. Das konvertierte Schema kann auch mit einer Datenbank auf einer Amazon EC2-Instance verwendet oder als Daten in einem Amazon S3-Bucket gespeichert werden.

AWS SCT bietet eine projektbasierte Benutzeroberfläche, mit der Sie das Datenbankschema Ihrer Quelldatenbank automatisch in ein mit Ihrer Amazon RDS-Ziel-Instance kompatibles Format konvertieren können.

Sie können AWS SCT verwenden, um eine Migration von einer Oracle-Quelldatenbank zu einem der oben aufgeführten Ziele durchzuführen. Mit AWS SCT können Sie die Quelldatenbankobjektdefinitionen wie Schema, Ansichten, gespeicherte Prozeduren und Funktionen exportieren.

Sie können AWS SCT verwenden, um Daten von Oracle in Amazon RDS for PostgreSQL oder Amazon Aurora PostgreSQL -kompatible Edition zu konvertieren.

In diesem Muster verwenden Sie AWS SCT, um Oracle-Code mithilfe der Erweiterungen und in PostgreSQL zu konvertieren `aws_oracle_ext` und zu migrieren `orafce`und die Erweiterungscodes manuell in `psql` Standard- oder nativen integrierten Code zu migrieren.

- Das AWS SCT-Erweiterungspaket ist ein Add-on-Modul, das Funktionen in der Quelldatenbank emuliert, die beim Konvertieren von Objekten in die Zieldatenbank erforderlich sind. Bevor Sie das AWS SCT-Erweiterungspaket installieren können, müssen Sie Ihr Datenbankschema konvertieren.

  Wenn Sie Ihre Datenbank oder Ihr Data Warehouse-Schema konvertieren, fügt AWS SCT Ihrer Zieldatenbank ein zusätzliches Schema hinzu. Über dieses Schema werden SQL-Systemfunktionen der Quelldatenbank implementiert, die zum Schreiben des konvertierten Schemas in die Zieldatenbank benötigt werden. Dieses Zusätzliche Schema wird als Erweiterungspaketschema bezeichnet.

  Das Erweiterungspaketschema für OLTP-Datenbanken wird entsprechend der Quelldatenbank benannt. Für Oracle-Datenbanken lautet das Erweiterungspaketschema `AWS_ORACLE_EXT`.

Andere Tools

- Orafce – Orafce ist ein Modul, das Oracle-kompatible Funktionen, Datentypen und Pakete implementiert. Es handelt sich um ein Open-Source-Tool mit einer Berkeley Source Distribution (BSD)-Lizenz, sodass jeder es verwenden kann. Das `orafce` Modul ist nützlich für die Migration von Oracle zu PostgreSQL, da viele Oracle-Funktionen in PostgreSQL implementiert sind.

Code

Eine Liste aller häufig verwendeten und migrierten Codes von Oracle zu PostgreSQL, um die Verwendung von AWS SCT-Erweiterungscodes zu vermeiden, finden Sie im angehängten Dokument.

Polen

Konfigurieren der Quelldatenbank von Amazon RDS für Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Oracle-Datenbank-Instance.	Erstellen Sie eine mit Amazon RDS für Oracle oder Aurora PostgreSQL kompatible Datenbank-Instance über die Amazon-RDS-Konsole.	Allgemeines AWS, DBA
Konfigurieren Sie die Sicherheitsgruppen.	Konfigurieren Sie ein- und ausgehende Sicherheitsgruppen.	Allgemeines AWS
Erstellen Sie die Datenbank.	Erstellen Sie die Oracle-Datenbank mit den erforderlichen Benutzern und Schemata.	Allgemeines AWS, DBA
Erstellen Sie die Objekte.	Erstellen Sie Objekte und fügen Sie Daten in das Schema ein.	DBA

Konfigurieren der Zieldatenbank von Amazon RDS für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die PostgreSQL-Datenbank-Instance.	Erstellen Sie eine Datenbank-Instance von Amazon RDS für PostgreSQL oder Amazon Aurora PostgreSQL über die Amazon RDS-Konsole.	Allgemeines AWS, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Sicherheitsgruppen.	Konfigurieren Sie ein- und ausgehende Sicherheitsgruppen.	Allgemeines AWS
Erstellen Sie die Datenbank.	Erstellen Sie die PostgreSQL-Datenbank mit den erforderlichen Benutzern und Schemata.	Allgemeines AWS, DBA
Validieren Sie die Erweiterungen.	Stellen Sie sicher, dass `aws_oracle_ext` und in der PostgreSQL-Datenbank installiert und korrekt konfiguriert `orafce` sind.	DBA
Stellen Sie sicher, dass die PostgreSQL-Datenbank verfügbar ist.	Stellen Sie sicher, dass die PostgreSQL-Datenbank betriebsbereit ist.	DBA

Migrieren des Oracle-Schemas zu PostgreSQL mithilfe von AWS SCT und den Erweiterungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SCT.	Installieren Sie die neueste Version von AWS SCT.	DBA
Konfigurieren Sie AWS SCT.	Konfigurieren Sie AWS SCT mit Java Database Connectivity (JDBC)-Treibern für Oracle (`ojdbc8.jar`) und PostgreSQL (`postgresql-42.2.5.jar`).	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie das AWS SCT-Erweiterungspaket oder die Vorlage.	Aktivieren Sie unter AWS SCT-Projekteinstellungen die integrierte Funktionsimplementierung mit den `orafce` Erweiterungen `aws_oracle_ext` und für das Oracle-Datenbankschema.	DBA
Konvertieren Sie das Schema.	Wählen Sie in AWS SCT Schema konvertieren aus, um das Schema von Oracle in PostgreSQL zu konvertieren und die .sql-Dateien zu generieren.	DBA

Konvertieren des AWS SCT-Erweiterungscodes in psql-Code

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie den Code manuell.	Konvertieren Sie jede Zeile des von der Erweiterung unterstützten Codes manuell in integrierten `psql` Standardcode, wie im angehängten Dokument beschrieben. Ändern Sie beispielsweise `AWS_ORACLE_EXT.SYSDATE()` oder `ORACLE.SYSDATE()` in `NOW()`.	DBA
Validieren des Codes	(Optional) Validieren Sie jede Codezeile, indem Sie sie vorübergehend in der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PostgreSQL-Datenbank ausführen.	
Erstellen Sie Objekte in der PostgreSQL-Datenbank.	Um Objekte in der PostgreSQL-Datenbank zu erstellen, führen Sie die .sql-Dateien aus, die von AWS SCT generiert und in den beiden vorherigen Schritten geändert wurden.	DBA

Zugehörige Ressourcen

- Datenbank
  - Oracle auf Amazon RDS
  - PostgreSQL auf Amazon RDS
  - Arbeiten mit Amazon Aurora PostgreSQL
  - PostgreSQL EXPLAIN-Plan
- AWS SCT
  - Übersicht über das AWS Schema Conversion Tool
  - AWS SCT-Benutzerhandbuch
  - Verwenden der AWS SCT-Benutzeroberfläche
  - Verwenden von Oracle Database als Quelle für AWS SCT
- Erweiterungen für AWS SCT
  - Verwenden des AWS SCT-Erweiterungspakets
  - Oracle-Funktionalität (en)
  - PN-Orafce
  - GitHub orafce

Zusätzliche Informationen

Weitere Informationen finden Sie in den detaillierten Befehlen mit Syntax und Beispielen für die manuelle Konvertierung von Code im angehängten Dokument.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren einer Db2-Datenbank von Amazon EC2 zu Aurora MySQL – kompatibel mithilfe von AWS DMS

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: IBM Db2 auf Amazon EC2	Ziel: Amazon Aurora MySQL – Kompatible Edition
R-Typ: Neuarchitektur	Workload: IBM	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; Amazon EC2; AWS SCT; Amazon Aurora		

Übersicht

Nachdem Sie Ihre Datenbank von IBM Db2 für LUW zu Amazon Elastic Compute Cloud (Amazon EC2) migriert haben, sollten Sie erwägen, die Datenbank neu zu strukturieren, indem Sie zu einer cloudnativen Datenbank von Amazon Web Services (AWS) wechseln. Dieses Muster umfasst die Migration einer Datenbank von IBM Db2 für LUW, die auf einer Amazon EC2-Instance ausgeführt wird, zu einer Datenbank der Amazon Aurora MySQL-kompatiblen Edition in AWS.

Das Muster beschreibt eine Online-Migrationsstrategie mit minimalen Ausfallzeiten für eine Multi-Terabyte-Db2-Quelldatenbank mit einer hohen Anzahl von Transaktionen.

Dieses Muster verwendet AWS Schema Conversion Tool (AWS SCT), um das Db2-Datenbankschema in ein Aurora MySQL-kompatibles Schema zu konvertieren. Dann verwendet das Muster AWS Database Migration Service (AWS DMS), um Daten von der Db2-Datenbank zur Aurora MySQL-kompatiblen Datenbank zu migrieren. Für den Code, der nicht von AWS SCT konvertiert wird, sind manuelle Konvertierungen erforderlich.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einer Virtual Private Cloud (VPC)

- AWS SCT
- AWS DMS

Produktversionen

- AWS SCT neueste Version
- Db2 für Linux Version 11.1.4.4 und höher

Architektur

Quelltechnologie-Stack

- DB2/Linux x86-64-Bit auf einer EC2-Instance gemountet

Zieltechnologie-Stack

- Eine Datenbank-Instance von Amazon Aurora MySQL -Compatible Edition

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Datenmigrationsarchitektur zwischen der Quelldatenbank Db2 und den Aurora MySQL-kompatiblen Zieldatenbanken. Die Architektur in der AWS Cloud umfasst eine Virtual Private Cloud (VPC) (Virtual Private Cloud), eine Availability Zone, ein öffentliches Subnetz für die Db2-Instance und die AWS DMS-Replikations-Instance sowie ein privates Subnetz für die Aurora MySQL-kompatible Datenbank.

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. AWS SCT unterstützt als Quelle IBM Db2 für LUW-Versionen 9.1, 9.5, 9.7, 10.1, 10.5, 11.1 und 11.5.

Bewährte Methoden

Bewährte Methoden finden Sie unter Bewährte Methoden für AWS Database Migration Service.

Polen

Konfigurieren der IBM Db2-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IBM-Db2-Datenbank auf Amazon EC2.	Sie können eine IBM Db2-Datenbank auf einer EC2-Instance erstellen, indem Sie ein Amazon Machine Image (AMI) aus AWS Marketplace verwenden oder Db2-Software auf einer EC2-Instance installieren. Starten Sie eine EC2-Instance, indem Sie ein AMI für IBM Db2 auswählen (z. B. IBM Db2 v11.5.7 RHEL 7.9), das einer On-Premises-Datenbank ähnelt.	DBA, Allgemeines AWS
Konfigurieren Sie Sicherheitsgruppen.	Konfigurieren Sie die Regeln für eingehenden Datenverkehr der VPC-Sicherheitsgruppe für	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SSH (Secure Shell) bzw. TCP mit Port 22 bzw. 50 000.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datenbank-Instance.	Erstellen Sie eine neue Instance (Benutzer) und Datenbank (Schema) oder verwenden Sie die Standard`db2inst1`-Instance und die Beispieldatenbank. 1. Stellen Sie über das Terminal eine Verbindung mit der EC2-Instance her, um eine Verbindung zur Db2-Datenbank herzustellen. Alternativ können Sie jede DB-Client-Software installieren, die eine Verbindung zur Db2-Datenbank herstellt. 2. Um das Passwort des db2inst1-Benutzers festzulegen, führen Sie den Befehl aus`sudo passwd db2inst1`. 3. Um eine Verbindung mit der db2inst1-Instance herzustellen, führen Sie den Befehl aus`sudo su - db2inst1`. 4. Um eine Verbindung mit der Db2-Datenbank herzustellen, führen Sie den Befehl ausdb2. 5. Verwenden Sie den Befehl , um eine Verbindung mit der Beispieldatenbank	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	herzustellen`connect to sample`. Stellen Sie alternativ eine Verbindung zu der Datenbank her, die Sie erstellt haben. 6. Nachdem Sie eine Verbindung mit der Datenbank-Instance hergestellt haben, erstellen Sie Objekte und fügen Sie Daten mithilfe von Db2-SQL-Anweisungen in diese Objekte ein.	
Vergewissern Sie sich, dass die Db2-DB-Instance verfügbar ist.	Verwenden Sie den `Db2pd -` Befehl , um zu bestätigen, dass die Db2-Datenbank-Instance betriebsbereit ist.	DBA

Konfigurieren der Aurora MySQL-kompatiblen Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die mit Aurora MySQL kompatible Datenbank .	Erstellen einer Amazon Aurora mit MySQL-Kompatibilität sdatenbank aus dem AWS RDS-Service • Erstellen Sie eine Datenbank auf Amazon Aurora mit MySQL-Kompatibilität und Version Ihrer Wahl, z. B. Aurora (MySQL)–5.6.10a	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Installieren Sie die MySQL-Workbench-Anwendung oder Ihre bevorzugte DB-Client-Software, mit der Sie eine Verbindung mit der MySQL-Datenbank herstellen können	
Konfigurieren Sie Sicherheitsgruppen.	Konfigurieren Sie die Regeln für eingehenden Datenverkehr der VPC-Sicherheitsgruppe für SSH- und TCP-Verbindungen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die Aurora-Datenbank verfügbar ist.	Gehen Sie wie folgt vor, um sicherzustellen, dass die mit Aurora MySQL kompatible Datenbank betriebsbereit ist: 1. Stellen Sie über SSH eine Verbindung mit der EC2-Instance her. 2. Konfigurieren Sie die mit Aurora MySQL kompatibl e Instance von MySQL Workbench aus und stellen Sie eine Verbindung mit ihr her. Verwenden Sie den Endpunkt als Hostnamen, wie im folgenden Beispiel gezeigt. `mysql-cluster-inst ance-1.cokmvis0v46 q.us-east-1.rds.am azonaws.com` 3. Erstellen Sie das neue Schema und stellen Sie eine Verbindung mit ihm her (z. B. `mysql-sample-db2`). 4. Führen Sie die MySQL-Anweisungen aus, um die Schemata und Objekte in der Datenbank zu überprüfe n.	DBA

Konfigurieren und Ausführen von AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SCT.	Laden Sie die neueste Version von AWS SCT (die aktuelle neueste Version 1.0.628) herunter und installieren Sie sie.	Allgemeines AWS
Konfigurieren Sie AWS SCT.	1. Laden Sie die Java Database Connectivity (JDBC)-Treiber für IBM Db2 (4.22.X-Version) und MySQL (8.x) herunter. 2. Um die Treiber in AWS SCT zu konfigurieren, wählen Sie Einstellungen , Globale Einstellungen , Treiber .	Allgemeines AWS
Erstellen Sie ein AWS SCT-Projekt.	Erstellen Sie ein AWS SCT-Projekt und einen Bericht, der Db2 für LUW als Quell-DB-Engine und Aurora MySQL – kompatibel für die Ziel-DB-E ngine verwendet. Informationen zu den Berechtigungen, die für die Verbindung mit einer Db2-für-LUW-Datenbank erforderl ich sind, finden Sie unter Verwenden von Db2 LUW als Quelle für AWS SCT .	Allgemeines AWS
Validieren Sie die Objekte.	Wählen Sie Schema laden und validieren Sie die Objekte.	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aktualisieren Sie alle falschen Objekte in der Zieldatenbank: 1. Stellen Sie eine Verbindung mit dem Amazon Aurora MySQL-kompatiblen Server her, indem Sie die Verbindungsdetails angeben, und wählen Sie Verbindung testen aus. Sowohl Quell- als auch Zielverbindungen müssen erfolgreich sein, bevor AWS SCT den Migrationsbericht starten kann. 2. Nachdem der Bericht abgeschlossen ist, geben Sie das Schema ein, das konvertiert werden soll, und wählen Sie Fertigstellen aus. AWS SCT listet alle Quell- und Zielobjekte auf, die konvertiert werden und Fehler aufweisen. 3. Überprüfen Sie die Fehler und löschen Sie sie manuell. 4. Nachdem alle Fehler gelöscht wurden, öffnen Sie das Kontextmenü (rechte Maustaste) für das Schema	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und wählen Sie Schema laden aus. 5. Wählen Sie Auf Datenbank anwenden aus. 6. Stellen Sie in MySQL Workbench eine Verbindung mit der Aurora MySQL-kompatiblen Datenbank her und überprüfen Sie das Schema und die Objekte.	

Konfigurieren und Ausführen von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikations-Instance.	Melden Sie sich bei der AWS-Managementkonsole an, navigieren Sie zum AWS DMS-Service und erstellen Sie eine Replikations-Instance mit gültigen Einstellungen für die VPC-Sicherheitsgruppe, die Sie für die Quell- und Zieldatenbanken konfiguriert haben.	Allgemeines AWS
Erstellen Sie Endpunkte.	Erstellen Sie den Quellendpunkt für die Db2-Datenbank und den Zielendpunkt für die Aurora MySQL-kompatible Datenbank: 1. Erstellen Sie einen Endpunkt für IBM Db2 als	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quelle, indem Sie RDS-DB-Instance auswählen und dann die von Ihnen erstellte Db2-Instance auswählen. Die Details zur Endpunktkonfiguration werden automatisch ausgefüllt. 2. Fügen Sie in den endpunktspezifischen Einstellungen die folgenden zusätzlichen Verbindungsattribute hinzu. `CurrentLSN=<scan>; MaxKBytesPerRead=64; SetDataCaptureChanges=true` Wenn Sie diese Attribute nicht angeben, ist die Testverbindung des Quellendpunkts nicht erfolgreich. Weitere Informationen finden Sie unter Verwenden von IBM Db2 LUW als Quelle für AWS DMS. 3. Erstellen Sie einen Endpunkt für Aurora MySQL -kompatibel als Ziel, indem Sie RDS-DB-Instance auswählen und dann die von Ihnen erstellte Aurora MySQL -kompatible Instance	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auswählen. Die Details zur Endpunktkonfigurat ion werden automatisch ausgefüllt. Weitere Informati onen finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS Database Migration Service. 4. Testen Sie die Quell- und Zielendpunkte. Bestätigen Sie, dass beide erfolgreich und verfügbar sind 5. Wenn der Test fehlschlä gt, stellen Sie sicher, dass die Regeln für eingehenden Datenverkehr der Sicherhei tsgruppe gültig sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Migration saufgaben.	Erstellen Sie eine einzelne Migrationsaufgabe oder mehrere Migrationsaufgaben für Volllast und CDC- oder Datenvalidierung: 1. Um eine Datenbank migrationsaufgabe zu erstellen, wählen Sie die Replikations-Instance, den Quelldatenbankendp unkt und den Zieldaten bankendpunkt aus. Geben Sie den Migrationstyp als Vorhandene Daten migrieren (Volllast), Nur Datenänderungen replizier en (CDC) oder Vorhanden e Daten migrieren und laufende Änderungen replizieren (Volllast und CDC) an. 2. Unter Tabellenzuordnungen können Sie Auswahlregeln und Transformationsregeln im GUI- oder JSON-Format konfigurieren. 3. Wählen Sie unter Auswahlregeln das Schema aus, geben Sie den Tabellennamen ein und wählen Sie Aktion (Einschli eßen/Ausschließen), die konfiguriert werden soll	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(z. B. Schema: SAMPLE; Tabellenname: %, Aktion: Einschließen). 4. Wählen Sie unter Transformationsregeln das Ziel aus (Schema, Tabelle oder Spalte). Wählen Sie den Schemanamen aus und wählen Sie die Aktion aus (Groß-/Kleinschreibung, Präfix, Suffix), z. B. Ziel: Schema; `mysql-sample-db` ; Aktion: Kleinbuchstaben erstellen. 5. Aktivieren Sie die Amazon-CloudWatch Logs-Überwachung.	
Planen Sie den Produktionslauf.	Bestätigen Sie Ausfallzeiten mit Stakeholdern wie Anwendungsbesitzern, um AWS DMS in Produktionssystemen auszuführen.	Migrationsleiter
Führen Sie die Migrationsaufgaben aus.	1. Starten Sie die AWS DMS-Aufgabe mit dem Status Bereit. 2. Überwachen Sie die Protokolle der Migrationsaufgaben in Amazon CloudWatch Logs auf Fehler.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten.	Überprüfen Sie die Ergebnisse und Daten der Migrationsaufgabe in den Quell-Db2- und Ziel-MySQL-Datenbanken: 1. Wenn der Status Laufende Replikation laden lautet, wird der vollständige Ladevorgang mit CDC-Datenmigration abgeschlossen und die Validierung wird fortgesetzt. 2. Stellen Sie eine Verbindung mit der Aurora MySQL-kompatiblen Datenbank her und überprüfen Sie die Daten. 3. Überprüfen Sie die laufenden Änderungen, indem Sie Daten in die Db2-Datenbank einfügen oder aktualisieren.	DBA
Beenden Sie Migrationsaufgaben.	Nachdem die Datenvalidierung erfolgreich abgeschlossen wurde, beenden Sie die Validierungsmigrationsaufgaben.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
AWS SCT-Quell- und Zieltestverbindungen schlagen fehl.	Konfigurieren Sie JDBC-Treiberversionen und Regeln für eingehenden Datenverkehr der VPC-Sicherheitsgruppe, um den eingehenden Datenverkehr zu akzeptieren.
Der Testlauf des Db2-Quellendpunkts schlägt fehl.	Konfigurieren Sie die zusätzliche Verbindungseinstellung `CurrentLSN=<scan>;` .

Die AWSDMS Aufgabe kann keine Verbindung zur Db2-Quelle herstellen und der folgende Fehler wird zurückgegeben.
`database is recoverable if either or both of the database configuration parameters LOGARCHMETH1 and LOGARCHMETH2 are set to ON`
	Führen Sie die folgenden Befehle aus, um den Fehler zu vermeiden:
	1. `$ db2 update db cfg for sample using LOGARCHMETH1 DISK:/home/db2inst1/logs`
	2. `$ db2stop`
	3. `$ db2start`
	4. `$ db2 connect to sample`
	`SQL1116N A connection to or activation of database "SAMPLE" cannot be made because of BACKUP PENDING. SQLSTATE=57019`
	5. `$ db2 backup database sample to ../logs`
	`SQL2036N The path for the file or device "../logs" is not valid`
	6. `$ cd`
	7. `$ pwd`
	`/home/db2inst1`
	8. `$ mkdir /tmp/backup`

Problem	Lösung

	9. `$ db2 backup database sample to /tmp/backup`
	`Backup successful. The timestamp for this backup image is : 20190530084921`
	10. `$ db2 connect to sample`
	`Database Connection Information`
	`Database server = DB2/LINUX 9.7.1`
	`SQL authorization ID = DB2INST1`
	`Local database alias = SAMPLE`

Zugehörige Ressourcen

Amazon EC2

- Amazon EC2
- Amazon EC2-Benutzerhandbuchs

Datenbanken

- IBM-Db2-Datenbank
- Amazon Aurora
- Arbeiten mit Amazon Aurora MySQL

AWS SCT

- AWS DMS Schemakonvertierung
- AWS Schema Conversion Tool – Benutzerhandbuch
- Verwenden der AWS SCT-Benutzeroberfläche
- Verwenden von IBM Db2 LUW als Quelle für AWS SCT

AWS DMS

- AWS Database Migration Service
- AWS Database Migration Service-Benutzerhandbuch
- Quellen für die Datenmigration
- Ziele für die Datenmigration
- AWS Database Migration Service und AWS Schema Conversion Tool unterstützen jetzt IBM Db2 LUW als Quelle (Blogbeitrag)
- Migrieren von Anwendungen mit relationalen Datenbanken zu AWS

Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS von Amazon EC2 zu Amazon DocumentDB

Quelle: Microsoft SQL Server auf Amazon EC2	Ziel: Amazon DocumentDB	R-Typ: Re-Architect
Umgebung: PoC oder Pilotprojekt	Technologien: Cloud-nativ; Datenbanken; Migration	Arbeitslast: Microsoft
AWS-Dienste: Amazon EC2; Amazon DocumentDB		

Übersicht

Dieses Muster beschreibt, wie AWS Database Migration Service (AWS DMS) verwendet wird, um eine Microsoft SQL Server-Datenbank, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance gehostet wird, zu einer Amazon DocumentDB DocumentDB-Datenbank (mit MongoDB-Kompatibilität) zu migrieren.

Die AWS DMS-Replikationsaufgabe liest die Tabellenstruktur der SQL Server-Datenbank, erstellt die entsprechende Sammlung in Amazon DocumentDB und führt eine Volllastmigration durch.

Sie können dieses Muster auch verwenden, um eine lokale SQL Server- oder Amazon Relational Database Service (Amazon RDS) für SQL Server-DB-Instance zu Amazon DocumentDB zu migrieren. Weitere Informationen finden Sie im Leitfaden Migration von Microsoft SQL Server-Datenbanken zur AWS-Cloud auf der AWS Prescriptive Guidance-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine bestehende SQL Server-Datenbank auf einer EC2-Instance.
- Feste Datenbankrolle (db_owner), die AWS DMS in der SQL Server-Datenbank zugewiesen wurde. Weitere Informationen finden Sie unter Rollen auf Datenbankebene in der SQL Server-Dokumentation.

- Vertrautheit mit der Verwendung der `mongoimport` Dienstprogramme `mongodump` `mongorestoremongoexport`,, und zum Verschieben von Daten in und aus einem Amazon DocumentDB-Cluster.
- Microsoft SQL Server Management Studio, installiert und konfiguriert.

Einschränkungen

- Die Clustergrößenbeschränkung in Amazon DocumentDB beträgt 64 TB. Weitere Informationen finden Sie unter Cluster-Grenzwerte in der Amazon DocumentDB DocumentDB-Dokumentation.
- AWS DMS unterstützt nicht die Zusammenführung mehrerer Quelltabellen zu einer einzigen Amazon DocumentDB-Sammlung.
- Wenn AWS DMS Änderungen aus einer Quelltabelle ohne Primärschlüssel verarbeitet, ignoriert es große Objektspalten (LOB) in der Quelltabelle.

Architektur

Quelltechnologie-Stack

- Amazon EC2

Zielarchitektur

Zieltechnologie-Stack

- Amazon DocumentDB

Tools

- AWS DMS — Mit dem AWS Database Migration Service (AWS DMS) können Sie Datenbanken einfach und sicher migrieren.
- Amazon DocumentDB — Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein schneller, zuverlässiger und vollständig verwalteter Datenbankservice.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud.

- Microsoft SQL Server — SQL Server ist ein relationales Datenbankverwaltungssystem.
- SQL Server Management Studio (SSMS) — SSMS ist ein Tool zur Verwaltung von SQL Server, einschließlich des Zugriffs auf, der Konfiguration und Verwaltung von SQL Server-Komponenten.

Epen

Eine VPC erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. Erstellen Sie eine virtuelle private Cloud (VPC) mit einem IPv4-CIDR-Blockber eich.	Systemadministrator
Erstellen Sie Sicherhei tsgruppen und Netzwerk-ACLs.	Erstellen Sie auf der Amazon VPC-Konsole gemäß Ihren Anforderungen Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten (Netzwerk -ACLs) für Ihre VPC. Sie können auch die Standarde instellungen für diese Konfigurationen verwenden . Weitere Informationen zu dieser und anderen Geschicht en finden Sie im Abschnitt „Verwandte Ressourcen“.	Systemadministrator

Erstellen und konfigurieren Sie den Amazon DocumentDB-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon DocumentDB-Cluster.	Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole und wählen Sie „Clusters“. Wählen Sie „Erstellen“ und erstellen Sie einen Amazon DocumentDB-Cluster mit einer Instance. Wichtig: Stellen Sie sicher, dass Sie diesen Cluster mit den Sicherheitsgruppen Ihrer VPC konfigurieren.	Systemadministrator
Installieren Sie die Mongo-Shell.	Die Mongo-Shell ist ein Befehlszeilenprogramm, mit dem Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen und ihn abfragen können. Um es zu installieren, führen Sie den Befehl „/etc/yum.repos.d/mongodb-org-3.6.repo“ aus, um die Repository-Datei zu erstellen. Führen Sie den Befehl „ mongodb-org-shellsudo yum install -y“ aus, um die Mongo-Shell zu installieren. Um Daten während der Übertragung zu verschlüsseln, laden Sie den öffentlichen Schlüssel für Amazon DocumentDB herunter und stellen Sie dann eine Verbindung zu	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihrer Amazon DocumentDB DocumentDB-Instance her. Weitere Informationen zu diesen Schritten finden Sie im Abschnitt „Verwandte Ressourcen“.	
Erstellen Sie eine Datenbank im Amazon DocumentDB-Cluster.	Führen Sie den Befehl „use“ mit dem Namen Ihrer Datenbank aus, um eine Datenbank in Ihrem Amazon DocumentDB-Cluster zu erstellen.	Systemadministrator

Erstellen und konfigurieren Sie die AWS DMS-Replikationsinstanz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Replikationsinstanz.	Öffnen Sie die AWS DMS-Konsole und wählen Sie „Replikationsinstanz erstellen “. Geben Sie einen Namen und eine Beschreibung für Ihre Replikationsaufgabe ein. Wählen Sie die Instanzklasse, die Engine-Version, den Speicher, die VPC und die Multi-AZ aus und machen Sie sie öffentlich zugänglich. Wählen Sie den Tab „Erweitert“, um die Netzwerk- und Verschlüsselungseinstellungen festzulegen. Geben Sie die Wartungseinstellungen an	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und wählen Sie dann „Replikat ionsinstanz erstellen“.	
Konfigurieren Sie die SQL Server-Datenbank.	Melden Sie sich bei Microsoft SQL Server an und fügen Sie eine eingehende Regel für die Kommunikation zwischen dem Quellendpunkt und der AWS DMS-Replikationsin stanz hinzu. Verwenden Sie die private IP-Adresse der Replikationsinstanz als Quelle. Wichtig: Die Replikati onsinstanz und der Zielendpu nkt sollten sich auf derselben VPC befinden. Verwenden Sie eine alternative Quelle in der Sicherheitsgruppe, wenn die VPCs für die Quell- und Replikationsinstanzen unterschiedlich sind.	Systemadministrator

Quell- und Zielendpunkte in AWS DMS erstellen und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quell- und Zieldatenbank-Endpunkte.	Öffnen Sie die AWS DMS-Konsole und wählen Sie „Quell- und Zieldatenbank-Endpunkte Connect“. Geben Sie die Verbindungsinforma tionen für die Quell- und Zieldatenbanken an. Wählen Sie bei Bedarf die Registerk arte „Erweitert“, um Werte	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für „Zusätzliche Verbindungsattribute“ festzulegen. Laden Sie das Zertifikatspaket herunter und verwenden Sie es in Ihrer Endpunktkonfiguration.	
Testen Sie die Endpunktverbindung.	Wählen Sie „Test ausführen“, um die Verbindung zu testen. Beheben Sie alle Fehlermeldungen, indem Sie die Sicherheitsgruppeneinstellungen und die Verbindungen zur AWS DMS-Replikationsinstanz sowohl von der Quell- als auch von der Zieldatenbank-Instance aus überprüfen.	Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Migrationsaufgabe.	Wählen Sie in der AWS DMS-Konsole „Aufgaben“, „Aufgabe erstellen“. Geben Sie die Aufgabenoptionen an, einschließlich der Namen der Quell- und Zielendpunkte sowie der Namen der Replikationsinstanzen. Wählen Sie unter „Migrationstyp“ die Optionen „Bestehende Daten migrieren“ und „Nur Datenänderungen replizier	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en“ aus. Wählen Sie „Aufgabe starten“.	
Führen Sie die AWS DMS-Migrationsaufgabe aus.	Geben Sie unter „Aufgaben einstellungen“ die Einstellungen für den Tabellenvorbereitungsmodus an, z. B. „Nichts tun“, „Tabellen auf Ziel löschen“, „Kürzen“ und „LOB-Spalten in die Replikation einbeziehen“. Legen Sie eine maximale LOB-Größe fest, die AWS DMS akzeptiert, und wählen Sie „Protokollierung aktivieren“. Behalten Sie für die „Erweiterten Einstellungen“ die Standardwerte bei und wählen Sie „Aufgabe erstellen“.	Systemadministrator
Überwachen Sie die Migration.	Wählen Sie in der AWS DMS-Konsole „Aufgaben“ und wählen Sie Ihre Migrationsaufgabe aus. Wählen Sie „Aufgabenüberwachung“, um Ihre Aufgabe zu überwachen. Die Aufgabe wird beendet, wenn die Volllastmigration abgeschlossen ist und die zwischengespeicherten Änderungen übernommen wurden.	Systemadministrator

Testen und verifizieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe der Mongo-Shell eine Connect zum Amazon DocumentDB-Cluster her.	Öffnen Sie die Amazon DocumentDB DocumentD B-Konsole und wählen Sie Ihren Cluster unter „Clusters “ aus. Wählen Sie auf der Registerkarte „Konnektivität und Sicherheit“ die Option „Mit der Mongo-Shell mit diesem Cluster Connect“.	Systemadministrator
Überprüfen Sie die Ergebnisse Ihrer Migration.	Führen Sie den Befehl „use“ mit dem Namen Ihrer Datenbank und anschließend den Befehl „show collectio ns“ aus. Führen Sie den Befehl „db. .count ();“ mit dem Namen Ihrer Datenbank aus. Wenn die Ergebnisse mit Ihrer Quelldatenbank übereinst immen, war Ihre Migration erfolgreich.	Systemadministrator

Zugehörige Ressourcen

Eine VPC erstellen und konfigurieren

- Erstellen Sie eine Sicherheitsgruppe für Ihre VPC
- Erstellen Sie eine Netzwerk-ACL

Erstellen und konfigurieren Sie den Amazon DocumentDB-Cluster

- Erstellen Sie einen Amazon DocumentDB-Cluster
- Installieren Sie die Mongo-Shell für Amazon DocumentDB
- Connect zu Ihrem Amazon DocumentDB-Cluster her

Erstellen und konfigurieren Sie die AWS DMS-Replikationsinstanz

- Verwenden Sie öffentliche und private Replikationsinstanzen

Quell- und Zielendpunkte in AWS DMS erstellen und testen

- Verwenden Sie Amazon DocumentDB als Ziel für AWS DMS
- Verwenden Sie eine SQL Server-Datenbank als Quelle für AWS DMS
- Verwenden Sie AWS DMS-Endpunkte

Daten migrieren

- Zu Amazon DocumentDB migrieren

Sonstige Ressourcen

- Einschränkungen bei der Verwendung von SQL Server als Quelle für AWS DMS
- So verwenden Sie Amazon DocumentDB, um skalierbare Anwendungen zu erstellen und zu verwalten

Migrieren einer lokalen ThoughtSpot Falcon-Datenbank zu Amazon Redshift

Erstellt von Battulga Bolvragchaa (AWS) und Antony Prasad Thevaraj (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises ThoughtSpot -Falcon-Datenbank	Ziel: Amazon Redshift
R-Typ: Neuarchitektur	Workload: Alle anderen Workloads	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; Amazon Redshift		

Übersicht

On-Premises-Data-Warehouses erfordern erhebliche Verwaltungszeit und Ressourcen, insbesondere für große Datensätze. Die finanziellen Kosten für den Aufbau, die Wartung und den Aufbau dieser Lager sind ebenfalls sehr hoch. Um die Kosten zu verwalten, die Komplexität von Extract, Transform, Load (ETL) gering zu halten und Leistung zu liefern, wenn Ihre Daten zunehmen, müssen Sie ständig auswählen, welche Daten geladen und welche Daten archiviert werden sollen.

Durch die Migration Ihrer On-Premises-ThoughtSpot Falcon-Datenbanken in die Amazon Web Services (AWS) Cloud können Sie auf cloudbasierte Data Lakes und Data Warehouses zugreifen, die Ihre geschäftliche Agilität, Sicherheit und Anwendungszuverlässigkeit erhöhen und gleichzeitig Ihre gesamten Infrastrukturkosten senken. Amazon Redshift trägt dazu bei, den Kosten- und Betriebsaufwand eines Data Warehouse erheblich zu senken. Sie können Amazon Redshift Spectrum auch verwenden, um große Datenmengen im nativen Format ohne Datenladevorgang zu analysieren.

Dieses Muster beschreibt die Schritte und den Prozess für die Migration einer ThoughtSpot Falcon-Datenbank von einem On-Premises-Rechenzentrum zu einer Amazon Redshift-Datenbank in der AWS Cloud.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine ThoughtSpot Falcon-Datenbank, die in einem On-Premises-Rechenzentrum gehostet wird

Produktversionen

- ThoughtSpot Version 7.0.1

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Die Daten werden in einer On-Premises-Relational-Datenbank gehostet.
2. AWS Schema Conversion Tool (AWS SCT) konvertiert die Data Definition Language (DDL), die mit Amazon Redshift kompatibel ist.
3. Nachdem die Tabellen erstellt wurden, können Sie die Daten mithilfe von AWS Database Migration Service (AWS DMS) migrieren.
4. Die Daten werden in Amazon Redshift geladen.
5. Die Daten werden in Amazon Simple Storage Service (Amazon S3) gespeichert, wenn Sie Redshift Spectrum verwenden oder die Daten bereits in Amazon S3 hosten.

Tools

- AWS DMS – AWS Data Migration Service (AWS DMS) unterstützt Sie bei der schnellen und sicheren Migration von Datenbanken zu AWS.
- Amazon Redshift – Amazon Redshift ist ein schneller, vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich, mit dem Sie alle Ihre Daten mithilfe Ihrer vorhandenen Business-Intelligence-Tools einfach und kostengünstig analysieren können.
- AWS SCT – AWS Schema Conversion Tool (AWS SCT) konvertiert Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere.

Polen

Vorbereiten der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die entsprechende Amazon-Redshift-Konfiguration.	Identifizieren Sie die entsprechende Amazon-Redshift-Clusterkonfiguration basierend auf Ihren Anforderungen und Ihrem Datenvolumen. Weitere Informationen finden Sie unter Amazon-Redshift-Cluster in der Amazon-Redshift-Dokumentation.	DBA
Untersuchen Sie Amazon Redshift, um zu prüfen, ob es Ihren Anforderungen entspricht.	Verwenden Sie die häufig FAQs zu Amazon Redshift, um zu verstehen und zu bewerten, ob Amazon Redshift Ihre Anforderungen erfüllt.	DBA

Den Amazon-Redshift-Zielcluster vorbereiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-Redshift-Cluster.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Redshift-Konsole und erstellen Sie dann einen Amazon Redshift-Cluster in einer Virtual Private Cloud (VPC). Weitere Informationen finden Sie unter Erstellen eines	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Clusters in einer VPC in der Amazon-Redshift-Dokumentation.	
Führen Sie ein PoC für Ihr Amazon-Redshift-Datenbankdesign durch.	Befolgen Sie die bewährten Methoden von Amazon Redshift, indem Sie einen Machbarkeitsnachweis (PoC) für Ihr Datenbankdesign durchführen. Weitere Informationen finden Sie unter Durchführen eines Machbarkeitsnachweises für Amazon Redshift in der Amazon-Redshift-Dokumentation.	DBA
Erstellen Sie Datenbankbenutzer.	Erstellen Sie die Benutzer in Ihrer Amazon-Redshift-Datenbank und gewähren Sie die entsprechenden Rollen für den Zugriff auf das Schema und die Tabellen. Weitere Informationen finden Sie unter Gewähren von Zugriffsberechtigungen für einen Benutzer oder eine Benutzergruppe in der Amazon-Redshift-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie Konfigura tionseinstellungen auf die Zieldatenbank an.	Wenden Sie die Konfigura tionseinstellungen entsprech end Ihren Anforderungen auf die Amazon-Redshift-Da tenbank an. Weitere Informationen zum Aktivieren von Parametern auf Datenbank-, Sitzungs- und Serverebene finden Sie in der Konfigurationsreferenz in der Amazon-Redshift-Dokumentati on.	DBA

Erstellen von Objekten im Amazon-Redshift-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Manuelles Erstellen von Tabellen mit DDL in Amazon Redshift.	(Optional) Wenn Sie AWS SCT verwenden, werden die Tabellen automatisch erstellt. Wenn beim Replizieren von DDLs jedoch Fehler auftreten , müssen Sie die Tabellen manuell erstellen.	DBA
Erstellen Sie externe Tabellen für Redshift Spectrum.	Erstellen Sie eine externe Tabelle mit einem externen Schema für Amazon Redshift Spectrum. Um externe Tabellen zu erstellen, müssen Sie der Besitzer des externen Schemas oder ein Datenbank-Superuser sein.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Erstellen externer Tabellen für Amazon Redshift Spectrum in der Amazon-Redshift-Dokumentation.	

Migrieren von Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS DMS, um die Daten zu migrieren.	Nachdem Sie die DDL der Tabellen in der Amazon-Redshift-Datenbank erstellt haben, migrieren Sie Ihre Daten mithilfe von AWS DMS zu Amazon Redshift. Ausführliche Schritte und Anweisungen finden Sie unter Verwenden einer Amazon-Redshift-Datenbank als Ziel für AWS DMS in der AWS-DMS-Dokumentation.	DBA
Verwenden Sie den COPY-Befehl, um die Daten zu laden.	Verwenden Sie den Amazon-Redshift-`COPY`Befehl, um die Daten aus Amazon S3 in Amazon Redshift zu laden. Weitere Informationen finden Sie unter Verwenden des Befehls COPY zum Laden aus Amazon S3 in der Amazon-Redshift-Dokumentation.	DBA

Validieren des Amazon-Redshift-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatensätze.	Validieren Sie die Tabellenanzahl für die Quell- und Zieldatensätze, die aus Ihrem Quellsystem geladen wurden.	DBA
Implementieren Sie bewährte Methoden für Amazon Redshift zur Leistungsoptimierung.	Implementieren Sie bewährte Methoden für Amazon Redshift für das Tabellen- und Datenbankdesign. Weitere Informationen finden Sie im Blogbeitrag Top 10 Performance Tuning techniques for Amazon Redshift .	DBA
Optimieren Sie die Abfrageleistung.	Amazon Redshift verwendet SQL-basierte Abfragen, um mit Daten und Objekten im System zu interagieren. Data Manipulation Language (DML) ist die Teilmenge von SQL, mit der Sie Daten anzeigen, hinzufügen, ändern und löschen können. DDL ist die Teilmenge von SQL, mit der Sie Datenbankobjekte wie Tabellen und Ansichten hinzufügen, ändern und löschen. Weitere Informationen finden Sie unter Optimieren der Abfrageleistung in der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-Redshift-Dokumentation.	
Implementieren Sie WLM.	Sie können Workload Management (WLM) verwenden, um mehrere Abfragewarteschlangen zu definieren und Abfragen zur Laufzeit an geeignete Warteschlangen weiterzuleiten. Weitere Informationen finden Sie unter Implementieren des Workload-Managements in der Amazon-Redshift-Dokumentation.	DBA
Arbeiten Sie mit Nebenläufigkeitsskalierung.	Durch die Verwendung der Gleichzeitigkeitsskalierungsfunktion können Sie praktisch unbegrenzt gleichzeitige Benutzer und gleichzeitige Abfragen mit konstant schneller Abfrageleistung unterstützen. Weitere Informationen finden Sie unter Arbeiten mit Nebenläufigkeitsskalierung in der Amazon-Redshift-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die bewährten Methoden von Amazon Redshift für das Tabellend esign.	Wenn Sie Ihre Datenbank planen, können bestimmte wichtige Tabellenentwurfsen tscheidungen die allgemeine Abfrageleistung stark beeinflus sen. Weitere Informationen zur Auswahl der am besten geeigneten Tabellendesignopti on finden Sie unter Bewährte Methoden für das Design von Tabellen in Amazon Redshift in der Amazon-Redshift-Do kumentation.	DBA
Erstellen Sie materialisierte Ansichten in Amazon Redshift.	Eine materialisierte Ansicht enthält einen vorberech neten Ergebnissatz, der auf einer SQL-Abfrage über eine oder mehrere Basistabellen basiert. Sie können `SELECT` Anweisungen ausgeben, um eine materialisierte Ansicht auf die gleiche Weise abzufragen, wie Sie andere Tabellen oder Ansichten in der Datenbank abfragen. Weitere Informationen finden Sie unter Erstellen materiali sierter Ansichten in Amazon Redshift in der Amazon-Re dshift-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie Verknüpfungen zwischen den Tabellen.	Um mehr als eine Tabelle gleichzeitig in zu durchsuch en ThoughtSpot, müssen Sie Verknüpfungen zwischen den Tabellen definieren, indem Sie Spalten angeben, die übereinstimmende Daten für zwei Tabellen enthalten. Diese Spalten stellen die `primary key` und `foreign key` der Verknüpfung dar. Sie können sie mithilfe des `ALTER TABLE` Befehls in Amazon Redshift oder definieren ThoughtSpot. Weitere Informationen finden Sie unter ALTER TABLE in der Amazon-Redshift-Do kumentation.	DBA

Einrichten einer ThoughtSpot Verbindung zu Amazon Redshift

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Amazon-Re dshift-Verbindung hinzu.	Fügen Sie Ihrer lokalen ThoughtSpot Falcon-Da tenbank eine Amazon-Re dshift-Verbindung hinzu. Weitere Informationen finden Sie unter Hinzufüge n einer Amazon-Redshift-Ve	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rbindung in der - ThoughtSpot Dokumentation.	
Bearbeiten Sie die Amazon-Redshift-Verbindung.	Sie können die Amazon-Redshift-Verbindung bearbeiten, um Tabellen und Spalten hinzuzufügen. Weitere Informationen finden Sie unter Bearbeiten einer Amazon-Redshift-Verbindung in der - ThoughtSpot Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie die Amazon-Redshift-Verbindung neu zu.	Ändern Sie die Verbindungsparameter, indem Sie die .yaml-Quellzuordnungsdatei bearbeiten, die beim Hinzufügen der Amazon-Redshift-Verbindung erstellt wurde. Sie können beispielsweise die vorhandene Tabelle oder Spalte einer anderen Tabelle oder Spalte in einer vorhandenen Datenbankverbindung zuordnen. ThoughtSpot empfiehlt, die Abhängigkeiten vor und nach der Neuzuweisung einer Tabelle oder Spalte in einer Verbindung zu überprüfen, um sicherzustellen, dass sie wie erforderlich angezeigt werden. Weitere Informationen finden Sie unter Neuzuordnung einer Amazon-Redshift-Verbindung in der - ThoughtSpot Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie eine Tabelle aus der Amazon-Redshift-Verbindung.	(Optional) Wenn Sie versuchen, eine Tabelle in einer Amazon-Redshift-Verbindung zu entfernen, ThoughtSpot prüft auf Abhängigkeiten und zeigt eine Liste der abhängigen Objekte an. Sie können die aufgelisteten Objekte auswählen, um sie zu löschen oder die Abhängigkeit zu entfernen. Anschließend können Sie die Tabelle entfernen. Weitere Informationen finden Sie unter Löschen einer Tabelle aus einer Amazon-Redshift-Verbindung in der -ThoughtSpot Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie eine Tabelle mit abhängigen Objekten aus einer Amazon-Redshift-Verbindung.	(Optional) Wenn Sie versuchen, eine Tabelle mit abhängigen Objekten zu löschen, wird der Vorgang blockiert. Es wird ein `Cannot delete` Fenster mit einer Liste von Links zu abhängigen Objekten angezeigt. Wenn alle Abhängigkeiten entfernt werden, können Sie die Tabelle löschen Weitere Informationen finden Sie unter Löschen einer Tabelle mit abhängigen Objekten aus einer Amazon-Redshift-Verbindung in der - ThoughtSpot Dokumentation.	DBA
Löschen Sie eine Amazon-Redshift-Verbindung.	(Optional) Da eine Verbindung in mehreren Datenquellen oder Visualisierungen verwendet werden kann, müssen Sie alle Quellen und Aufgaben löschen, die diese Verbindung verwenden, bevor Sie die Amazon-Redshift-Verbindung löschen können. Weitere Informationen finden Sie unter Löschen einer Amazon-Redshift-Verbindung in der - ThoughtSpot Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Verbindungsreferenz für Amazon Redshift.	Stellen Sie sicher, dass Sie die erforderlichen Informationen für Ihre Amazon-Redshift-Verbindung angeben, indem Sie die Verbindungsreferenz in der - ThoughtSpot Dokumentation verwenden.	DBA

Zusätzliche Informationen

- KI-gestützte Analysen in jeder Größenordnung mit ThoughtSpot und Amazon Redshift
- Amazon-Redshift-Preise
- Erste Schritte mit AWS SCT
- Erste Schritte mit Amazon Redshift
- Verwenden von Datenextraktionsagenten
- Chick--A verbessert die Erkenntnisgeschwindigkeit mit ThoughtSpot und AWS

Migrieren einer Oracle-Datenbank zu Amazon DynamoDB mit AWS DMS

Erstellt von Rambabu Karnena (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon DynamoDB
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon DynamoDB		

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer Oracle-Datenbank zu Amazon DynamoDB mithilfe von AWS Database Migration Service (AWS DMS). Es deckt drei Arten von Quelldatenbanken ab:

- On-Premises-Oracle-Datenbanken
- Oracle-Datenbanken in Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instances

In diesem Machbarkeitsnachweis konzentriert sich dieses Muster auf die Migration von einer DB-Instance von Amazon RDS für Oracle.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Anwendung, die eine Verbindung zu einer Datenbank von Amazon RDS für Oracle herstellt
- Eine Tabelle, die in der Quelldatenbank von Amazon RDS für Oracle mit einem Primärschlüssel und Beispieldaten erstellt wurde

Einschränkungen

- Oracle-Datenbankobjekte wie Prozeduren, Funktionen, Pakete und Auslöser werden für die Migration nicht berücksichtigt, da Amazon DynamoDB diese Datenbankobjekte nicht unterstützt.

Produktversionen

- Dieses Muster gilt für alle Editionen und Versionen von Oracle-Datenbanken, die von AWS DMS unterstützt werden. Weitere Informationen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer Amazon DynamoDB-Datenbank als Ziel für AWS DMS. Wir empfehlen Ihnen, die neuesten Versionen von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden.

Architektur

Quelltechnologie-Stack

- DB-Instances von Amazon RDS für Oracle, Oracle auf Amazon EC2 oder On-Premises-Oracle-Datenbanken

Zieltechnologie-Stack

- Amazon DynamoDB

AWS-Datenmigrationsarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud. Dieses Muster verwendet Amazon RDS für Oracle.

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie in Ihrem AWS-Konto eine Virtual Private Cloud (VPC) und ein privates Subnetz.	Systemadministrator
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten.	Weitere Informationen finden Sie in der AWS-Dokum entation.	Systemadministrator
Konfigurieren und starten Sie die DB-Instance von Amazon RDS für Oracle.	Weitere Informationen finden Sie in der AWS-Dokum entation.	DBA, Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den Zugriff auf DynamoDB .	Erstellen Sie in der AWS Identity and Access Management (IAM)-Kon sole die Rolle, fügen Sie die Richtlinie an `AmazonDyn amoDBFullAccess to it`und wählen Sie AWS DMS als Service aus.	Systemadministrator
Erstellen Sie eine AWS DMS-Replikations-Instance für die Migration.	Die Replikations-Instance sollte sich in derselben Availability Zone und VPC wie die Quelldatenbank befinden.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Quell- und Zielendpunkte in AWS DMS.	Um den Endpunkt der Quelldatenbank zu erstellen, haben Sie zwei Möglichkeiten: • Wählen Sie in der Amazon-RDS-Konsole Datenbanken, DB-ID, Konnektivität und Sicherheit und wählen Sie den Endpunkt aus. • Wählen Sie in der AWS DMS-Konsole RDS-DB-Instance auswählen aus. Um den Zieldatenbankendpunkt zu erstellen, wählen Sie den Amazon-Ressourcennamen (ARN) der Rolle aus der vorherigen Aufgabe aus, um auf DynamoDB zuzugreifen.	Systemadministrator
Erstellen Sie eine AWS DMS-Aufgabe, um die Oracle-Quelldatenbanktabellen in DynamoDB zu laden.	Wählen Sie die Quell- und Zielendpunktnamen und die Replikations-Instance aus den vorherigen Schritten aus. Der Typ kann Volllast sein. Wählen Sie das Oracle-Schema aus und geben Sie % an, um alle Tabellen auszuwählen.	Systemadministrator
Validieren Sie die Tabellen in DynamoDB .	Um die Migrationsergebnisse anzuzeigen, wählen Sie im linken Navigationsbereich der DynamoDB-Konsole Tabellen aus.	DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie den Anwendung scode.	Um eine Verbindung zu DynamoDB herzustellen und Daten von DynamoDB abzurufen, aktualisieren Sie den Anwendungscode.	App-Besitzer, DBA, Systemadministrator

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie die Anwendung sclients zur Verwendung von DynamoDB .		DBA, App-Besitzer, Systemadministrator

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die AWS-Resso urcen herunter.	Beispielsweise fährt die Amazon RDS for Oracle-In stance, DynamoDB und die AWS DMS-Replikations-I nstance herunter.	DBA, Systemadministrator
Erfassen Sie Metriken.	Zu den Metriken gehören die Zeit für die Migration, der Prozentsatz der manuellen Arbeit und der vom Tool ausgeführten Arbeit sowie Kosteneinsparungen.	DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

- AWS Database Migration Service und Amazon DynamoDB: Was Sie wissen müssen (Blogbeitrag)
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer Amazon DynamoDB-Datenbank als Ziel für AWS Database Migration Service
- Bewährte Methoden für die Migration von RDBMS zu Amazon DynamoDB (Whitepaper)

Migrieren einer partitionierten Oracle-Tabelle zu PostgreSQL mithilfe von AWS DMS

Erstellt vonrav Mishra (AWS) und Eduardoentim (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: PostgreSQL 9.0
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken; Speicher und Backup
AWS-Services: AWS DMS		

Übersicht

Dieses Muster beschreibt, wie Sie das Laden einer partitionierten Tabelle von Oracle nach PostgreSQL beschleunigen können, indem Sie AWS Database Migration Service (AWS DMS) verwenden, der keine native Partitionierung unterstützt. Die PostgreSQL-Zieldatenbank kann auf Amazon Elastic Compute Cloud (Amazon EC2) installiert werden oder es kann sich um eine Amazon Relational Database Service (Amazon RDS) for PostgreSQL- oder Amazon Aurora PostgreSQL -kompatible Edition-DB-Instance handeln.

Das Hochladen einer partitionierten Tabelle umfasst die folgenden Schritte:

1. Erstellen Sie eine übergeordnete Tabelle ähnlich der Oracle-Partitionstabelle, enthalten Sie jedoch keine Partition.
2. Erstellen Sie untergeordnete Tabellen, die von der übergeordneten Tabelle erben, die Sie in Schritt 1 erstellt haben.
3. Erstellen Sie eine Prozedurfunktion und einen Auslöser, um die Einfügungen in der übergeordneten Tabelle zu verarbeiten.

Da der Auslöser jedoch für jede Einfügung ausgelöst wird, kann das anfängliche Laden mit AWS DMS sehr langsam sein.

Um das anfängliche Laden von Oracle zu PostgreSQL 9.0 zu beschleunigen, erstellt dieses Muster eine separate AWS DMS-Aufgabe für jede Partition und lädt die entsprechenden untergeordneten Tabellen. Anschließend erstellen Sie während des Cutovers einen Auslöser.

PostgreSQL Version 10 unterstützt native Partitionierung. In einigen Fällen können Sie jedoch die geerbte Partitionierung verwenden. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank mit einer partitionierten Tabelle
- Eine PostgreSQL-Datenbank in AWS

Produktversionen

- PostgreSQL 9.0

Architektur

Quelltechnologie-Stack

- Eine partitionierte Tabelle in Oracle

Zieltechnologie-Stack

- Eine partitionierte Tabelle in PostgreSQL (auf Amazon EC2, Amazon RDS für PostgreSQL oder Aurora PostgreSQL)

Zielarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.

Polen

Einrichten von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Tabellen in PostgreSQL .	Erstellen Sie die übergeord neten und die entsprechenden untergeordneten Tabellen in PostgreSQL mit den erforderl ichen Prüfungsbedingungen für Partitionen.	DBA
Erstellen Sie die AWS DMS-Aufgabe für jede Partition.	Fügen Sie die Filterbedingung der Partition in die AWS DMS-Aufgabe ein. Ordnen Sie die Partitionen den entsprech enden untergeordneten PostgreSQL-Tabellen zu.	DBA
Führen Sie die AWS DMS-Aufgaben mit Volllast und Change Data Capture (CDC) aus.	Stellen Sie sicher, dass der `StopTaskCachedChan gesApplied` Parameter auf `true` und der `StopTaskC achedChangesNotApp lied` Parameter auf gesetzt ist`false`.	DBA

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die Replikati onsaufgaben an.	Bevor Sie die Aufgaben beenden, stellen Sie sicher, dass Quelle und Ziel synchron sind.	DBA
Erstellen Sie einen Auslöser für die übergeordnete Tabelle.	Da die übergeordnete Tabelle alle Einfüge- und Aktualisi erungsbefehle empfängt, erstellen Sie einen Auslöser, der diese Befehle basierend auf der Partitionierungsbe dingung an die jeweiligen untergeordneten Tabellen weiterleitet.	DBA

Zugehörige Ressourcen

- AWS DMS
- Tabellenpartitionierung (PostgreSQL-Dokumentation)

Zusätzliche Informationen

Obwohl PostgreSQL Version 10 die native Partitionierung unterstützt, können Sie sich für die folgenden Anwendungsfälle für die Verwendung der geerbten Partitionierung entscheiden:

- Partitionierung erzwingt eine Regel, dass alle Partitionen denselben Spaltensatz wie das übergeordnete haben müssen, aber die Tabellenvererbung unterstützt untergeordnete Elemente mit zusätzlichen Spalten.
- Die Tabellenvererbung unterstützt mehrere Vererbungen.
- Die deklarative Partitionierung unterstützt nur die Listen- und Bereichspartitionierung. Mit der Tabellenvererbung können Sie die Daten nach Ihren Wünschen teilen. Wenn der

Einschränkungsausschluss Partitionen jedoch nicht effektiv bereinigen kann, wird die Abfrageleistung beeinträchtigt.

- Einige Operationen benötigen eine stärkere Sperre, wenn deklarative Partitionierung verwendet wird als bei der Verwendung der Tabellenvererbung. Zum Beispiel erfordert das Hinzufügen oder Entfernen einer Partition zu oder aus einer partitionierten Tabelle eine `ACCESS EXCLUSIVE` Sperre für die übergeordnete Tabelle, wohingegen eine `SHARE UPDATE EXCLUSIVE` Sperre für die reguläre Vererbung ausreicht.

Wenn Sie separate Auftragspartitionen verwenden, können Sie Partitionen auch neu laden, wenn AWS DMS-Validierungsprobleme auftreten. Um die Leistung und Replikationssteuerung zu verbessern, führen Sie Aufgaben auf separaten Replikations-Instances aus.

Migrieren von Amazon RDS für Oracle zu Amazon RDS für MySQL

Erstellt von Jitender Kumar (AWS), Neha Sharma (AWS) und Srini Ramaswamy (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Amazon RDS für Oracle	Ziel: Amazon RDS für MySQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) for Oracle-DB-Instance zu einer Amazon RDS for MySQL-DB-Instance in Amazon Web Services (AWS). Das Muster verwendet AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT).

Das Muster bietet bewährte Methoden für die Migration von gespeicherten Prozeduren. Außerdem werden - und -Codeänderungen zur Unterstützung der Anwendungsebene behandelt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Quelldatenbank von Amazon RDS für Oracle.
- Eine Zieldatenbank von Amazon RDS für MySQL. Quell- und Zieldatenbanken sollten sich in derselben Virtual Private Cloud (VPC) befinden. Wenn Sie mehrere VPCs verwenden oder über die erforderlichen Zugriffsberechtigungen verfügen.
- Sicherheitsgruppen, die Konnektivität zwischen der Quell- und der Zieldatenbank, AWS SCT, dem Anwendungsserver und AWS DMS ermöglichen.
- Ein Benutzerkonto mit der erforderlichen Berechtigung zum Ausführen von AWS SCT in der Quelldatenbank.
- Zusätzliche Protokollierung für die Ausführung von AWS DMS in der Quelldatenbank aktiviert.

Einschränkungen

- Die Größenbeschränkung für die Quell- und Zieldatenbank von Amazon RDS beträgt 64 TB. Informationen zur Amazon RDS-Größe finden Sie in der AWS-Dokumentation.
- Bei Oracle wird bei Datenbankobjekten die Groß- und Kleinschreibung nicht beachtet, bei MySQL hingegen nicht. AWS SCT kann dieses Problem beim Erstellen eines Objekts beheben. Allerdings sind einige manuelle Arbeiten erforderlich, um die vollständige Nichtbeachtung der Groß- und Kleinschreibung zu unterstützen.
- Bei dieser Migration werden keine MySQL-Erweiterungen verwendet, um Oracle-native Funktionen zu aktivieren. AWS SCT übernimmt den größten Teil der Konvertierung, aber einige Arbeit ist erforderlich, um Code manuell zu ändern.
- Java Database Connectivity (JDBC)-Treiberänderungen sind in der Anwendung erforderlich.

Produktversionen

- Amazon RDS für Oracle 12.2.0.1 und höher. Derzeit unterstützte Versionen von RDS für Oracle finden Sie in der AWS-Dokumentation.
- Amazon RDS für MySQL 8.0.15 und höher. Informationen zu derzeit unterstützten Versionen von RDS für MySQL finden Sie in der AWS-Dokumentation.
- AWS DMS Version 3.3.0 und höher. Weitere Informationen zu von AWS DMS unterstützten Quellendpunkten und Zielendpunkten finden Sie in der AWS-Dokumentation.
- AWS SCT Version 1.0.628 und höher. Weitere Informationen finden Sie in der Support-Matrix für AWS-SCT-Quellen- und -Zielendpunkte in der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Amazon RDS für Oracle. Weitere Informationen finden Sie unterVerwenden einer Oracle-Datenbank als Quelle für AWS DMS.

Zieltechnologie-Stack

- Amazon RDS für MySQL . Weitere Informationen finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS.

Migrationsarchitektur

Im folgenden Diagramm kopiert und konvertiert AWS SCT Schemaobjekte aus der Quelldatenbank von Amazon RDS für Oracle und sendet die Objekte an die Zieldatenbank von Amazon RDS für MySQL. AWS DMS repliziert Daten aus der Quelldatenbank und sendet sie an die Amazon RDS for MySQL-Instance.

Tools

- AWS Data Migration Service unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud. Dieses Muster verwendet Amazon RDS für Oracle und Amazon RDS für MySQL .
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Polen

Vorbereitung auf die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen und Engines.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserver-Instance.		DBA, SysAdmin
Identifizieren Sie Speichera nforderungen (Speichertyp und Kapazität).		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instance-Typ (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Wählen Sie eine Strategie für die Anwendungsmigration aus.	Überlegen Sie, ob Sie vollständige oder teilweise Ausfallzeiten für Cutover-Aktivitäten wünschen.	DBA, SysAdmin, App-Besitzer

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC und Subnetze.		SysAdmin
Erstellen Sie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs).		SysAdmin
Konfigurieren und starten Sie die Instance von Amazon RDS für Oracle.		DBA, SysAdmin
Konfigurieren und starten Sie die Amazon RDS for MySQL-Instance.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie einen Testfall für die Validierung der Codekonvertierung vor.	Dies hilft bei der Komponentenprüfung für den konvertierten Code.	DBA, Entwickler
Konfigurieren Sie die AWS DMS-Instance.		
Konfigurieren Sie Quell- und Zielendpunkte in AWS DMS.		

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie das Zieldatenbankskript mit AWS SCT.	Überprüfen Sie die Genauigkeit des Codes, der von AWS SCT konvertiert wurde. Einige manuelle Arbeiten sind erforderlich.	DBA, Entwickler
Wählen Sie in AWS SCT die Einstellung „Fallunsensibel“ aus.	Wählen Sie in AWS SCT Projekteinstellungen, Ziel-Case-Senitivität, Groß- und Kleinschreibung wird nicht beachtet.	DBA, Entwickler
Wählen Sie in AWS SCT aus, dass die native Oracle-Funktion nicht verwendet werden soll.	Überprüfen Sie in Projekteinstellungen die Funktionen TO_CHAR/TO_NUMBER/TO_DATE.	DBA, Entwickler
Nehmen Sie Änderungen für den Code „sql%not Found“ vor.	Möglicherweise müssen Sie den Code manuell konvertieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fragen Sie Tabellen und Objekte in gespeicherten Prozeduren ab (verwende n Sie Abfragen in Kleinbuch staben).		DBA, Entwickler
Erstellen Sie das primäre Skript, nachdem alle Änderungen vorgenomm en wurden, und stellen Sie dann das primäre Skript in der Zieldatenbank bereit.		DBA, Entwickler
Gespeicherte Prozeduren und Anwendungsaufrufe mit Einheitentest anhand von Beispieldaten.		
Bereinigen Sie Daten, die während des Komponent entests erstellt wurden.		DBA, Entwickler
Entfernen Sie Fremdschl üsseleinschränkungen in der Zieldatenbank.	Dieser Schritt ist erforderl ich, um anfängliche Daten zu laden. Wenn Sie die Fremdschlüsseleinschränkung en nicht löschen möchten, müssen Sie eine Migration saufgabe für Daten erstellen , die für die primäre und sekundäre Tabelle spezifisch sind.	DBA, Entwickler
Löschen Sie Primärschlüssel und eindeutige Schlüssel in der Zieldatenbank.	Dieser Schritt führt zu einer besseren Leistung beim ersten Laden.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die zusätzlic he Protokollierung in der Quelldatenbank.		DBA
Erstellen Sie eine Migration saufgabe für den ersten Ladevorgang in AWS DMS und führen Sie sie dann aus.	Wählen Sie die Option zum Migrieren vorhandener Daten aus.	DBA
Fügen Sie die Primärsch lüssel und Fremdschlüssel zur Zieldatenbank hinzu.	Einschränkungen müssen nach dem ersten Laden hinzugefügt werden.	DBA, Entwickler
Erstellen Sie eine Migration saufgabe für die laufende Replikation.	Durch die fortlaufende Replikation wird die Zieldaten bank mit der Quelldatenbank synchronisiert.	DBA

Migrieren von Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ersetzen Sie native Oracle-Fu nktionen durch native MySQL-Funktionen.		App-Besitzer
Stellen Sie sicher, dass nur Kleinbuchstabennamen für Datenbankobjekte in SQL-Abfragen verwendet werden.		DBA, SysAdmin, App-Besitzer

Umstellung auf die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie den Anwendungsserver herunter.		App-Besitzer
Überprüfen Sie, ob die Quell- und Zieldatenbanken synchron sind.		DBA, App-Besitzer
Halten Sie die DB-Instance von Amazon RDS für Oracle an.		DBA
Beenden Sie die Migrationsaufgabe.	Dies wird automatisch beendet, nachdem Sie den vorherigen Schritt abgeschlossen haben.	DBA
Ändern Sie die JDBC-Verbindung von Oracle zu MySQL .		App-Eigentümer, DBA
Starten Sie die Anwendung.		DBA, SysAdmin, App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin
Erfassen Sie Metriken über die zu migrierende Zeit, den Prozentsatz manueller Aufgaben im Vergleich zu Tool-Aufgaben, Kostenein sparungen usw.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie AWS DMS-Instances an und löschen Sie sie.		DBA
Entfernen Sie die Quell- und Zielendpunkte.		DBA
Entfernen Sie Migration saufgaben.		DBA
Erstellen Sie einen Snapshot der DB-Instance von Amazon RDS für Oracle.		DBA
Löschen Sie die DB-Instance von Amazon RDS für Oracle.		DBA
Fahren Sie alle anderen von Ihnen verwendeten temporären AWS-Ressourcen herunter und löschen Sie sie.		DBA, SysAdmin
Schließen Sie das Projekt und geben Sie Feedback.		DBA

Zugehörige Ressourcen

- AWS DMS
- AWS SCT
- Amazon RDS – Preise
- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS

Migrieren von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL – kompatibel mit AWS DMS und AWS SCT

Erstellt vonsendu Halder (AWS) und Sachin Kotwal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: IBM Db2	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Neuarchitektur	Workload: IBM	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora; AWS DMS; AWS SCT		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer IBM-Db2-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance zu einer Amazon-Aurora-PostgreSQL-kompatible Edition-DB-Instance. Dieses Muster verwendet AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT) für die Datenmigration und Schemakonvertierung.

Das Muster zielt auf eine Online-Migrationsstrategie mit geringer oder keiner Ausfallzeit für eine IBM Db2-Datenbank mit mehreren Terabyte ab, die eine hohe Anzahl von Transaktionen aufweist. Wir empfehlen, die Spalten in Primärschlüsseln (PKs) und Fremdschlüsseln (FKs) mit dem Datentyp in `INT` oder `BIGINT` in PostgreSQL zu konvertieren`NUMERIC`, um eine bessere Leistung zu erzielen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine IBM Db2-Quelldatenbank auf einer EC2-Instance

Produktversionen

- DB2/LINUXX8664 Version 11.1.4.4 und höher

Architektur

Quelltechnologie-Stack

- Eine Db2-Datenbank auf einer EC2-Instance

Zieltechnologie-Stack

- Eine DB-Instance von Aurora PostgreSQL -kompatible Version 10.18 oder höher

Datenbankmigrationsarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenbanken in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen. Die Quelldatenbank bleibt während der Migration voll funktionsfähig und minimiert Ausfallzeiten für Anwendungen, die auf der Datenbank basieren. Sie können AWS DMS verwenden, um Ihre Daten zu und von den gängigsten kommerziellen und Open-Source-Datenbanken zu migrieren. AWS DMS unterstützt heterogene Migrationen zwischen verschiedenen Datenbankplattformen, z. B. IBM Db2 zu Aurora PostgreSQL – kompatible Version 10.18 oder höher. Weitere Informationen finden Sie unter Quellen für die Datenmigration und Ziele für die Datenmigration in der AWS DMS-Dokumentation.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und die meisten Datenbankcodeobjekte, einschließlich Ansichten, gespeicherter Prozeduren und Funktionen, automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Alle Objekte, die nicht automatisch konvertiert werden, sind klar markiert, sodass sie manuell konvertiert werden können, um die Migration abzuschließen. AWS SCT kann auch den Anwendungsquellcode nach eingebetteten SQL-Anweisungen scannen und konvertieren.

Polen

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine mit Aurora PostgreSQL kompatible DB-Instance.	Um die DB-Instance zu erstellen, folgen Sie den Anweisungen in der AWS-Dokumentation. Wählen Sie als Engine-Typ Amazon Aurora aus. Wählen Sie für Edition die Option Amazon Aurora PostgreSQL – Kompatible Edition aus. Die DB-Instance von Aurora PostgreSQL -kompatible Version 10.18 oder höher sollte sich in derselben Virtual Private Cloud (VPC) wie die IBM-Db2-Quelldatenbank befinden.	Amazon RDS

Konvertieren Ihres Datenbankschemas

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und überprüfen Sie AWS SCT.	1. Installieren Sie AWS SCT, indem Sie die Schritte in der AWS SCT-Dokumentation befolgen. 2. Überprüfen Sie die Installation, indem Sie die Verfahren in der AWS SCT-Dokumentation befolgen.	AWS-Administrator, DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie AWS SCT und erstellen Sie ein Projekt.	Um das AWS SCT-Tool zu starten und ein neues Projekt zur Ausführung eines Bewertungsberichts zur Datenbankmigration zu erstellen, folgen Sie den Anweisungen in der AWS SCT-Dokumentation.	Migrationsingenieur
Fügen Sie Datenbankserver hinzu und erstellen Sie eine Zuordnungsregel.	1. Fügen Sie Quell- und Zieldatenbankserver hinzu, indem Sie den Anweisungen in der AWS SCT-Dokumentation folgen. 2. Erstellen Sie eine Zuordnungsregel, um die Zieldatenbankplattform für Ihre Quelldatenbank zu definieren. Anweisungen finden Sie in der AWS SCT-Dokumentation.	Migrationsingenieur
Erstellen Sie einen Bewertungsbericht zur Datenbankmigration.	Erstellen Sie den Bewertungsbericht zur Datenbankmigration, indem Sie die Schritte in der AWS SCT-Dokumentation befolgen.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie den Bewertungsbericht an.	Verwenden Sie die Registerkarte Zusammenfassung des Bewertungsberichts zur Datenbankmigration, um den Bericht anzuzeigen und die Daten zu analysieren. Diese Analyse hilft Ihnen dabei, die Komplexität der Migration zu ermitteln. Weitere Informationen finden Sie in der AWS SCT-Dokumentation.	Migrationsingenieur
Konvertieren Sie das Schema.	So konvertieren Sie Ihre Quelldatenbankschemata: 1. Wählen Sie in der AWS SCT-Konsole Anzeigen und dann Hauptansicht aus. 2. Wählen Sie das Objekt oder den übergeordneten Knoten aus Ihrem Quellschema aus, öffnen Sie das Kontextmenü (rechte Maustaste) und wählen Sie dann Schema konvertieren aus. Weitere Informationen finden Sie in der AWS SCT-Dokumentation.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie das konvertierte Datenbankschema auf die Ziel-DB-Instance an.	1. Wählen Sie das Schema-Element im rechten Bereich Ihres Projekt aus, der das geplante Schema für Ihre Ziel-DB-Instance anzeigt. 2. Öffnen Sie das Kontextmenü (rechte Maustaste) für das Schema-Element und wählen Sie Apply to database aus. Weitere Informationen finden Sie in der AWS SCT-Dokumentation.	Migrationsingenieur

Migrieren Ihrer Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine VPC und DB-Parametergruppen ein.	Richten Sie eine VPC und DB-Parametergruppen ein und konfigurieren Sie die für die Migration erforderlichen Regeln und Parameter für eingehenden Datenverkehr. Anweisungen finden Sie in der AWS DMS-Dokumentation. Wählen Sie für die VPC-Sicherheitsgruppe sowohl die EC2-Instance für Db2 als auch die mit Aurora PostgreSQL kompatible DB-Instance aus. Diese Replikations-Instance	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	muss sich in derselben VPC wie die Quell- und Ziel-DB-I nstances befinden.	
Bereiten Sie Quell- und Ziel-DB-Instances vor.	Bereiten Sie die Quell- und Ziel-DB-Instances für die Migration vor. In einer Produktionsumgebung ist die Quelldatenbank bereits vorhanden. Für die Quelldatenbank muss der Servername das öffentlic he Domain Name System (DNS) der EC2-Instance sein, in der Db2 ausgeführ t wird. Für den Benutzern amen können Sie verwenden , `db2inst1` gefolgt vom Port, der 5000 für IBM Db2 sein wird.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon EC2-Client und Endpunkte.	1. Erstellen Sie einen Amazon EC2-Client. Sie verwenden diesen Client, um Ihre Quelldatenbank mit zu replizierenden Daten zu füllen. Sie verwenden diesen Client auch, um die Replikation zu überprüfen, indem Sie Abfragen in der Zieldatenbank ausführen. 2. Erstellen Sie Endpunkte für die Quelldatenbank und die Ziel-DB-Instance, die Sie für die nächsten Schritte verwenden möchten. Anweisungen finden Sie in der AWS DMS-Dokumentation. Sie müssen separate Endpunkte für die Quell- und Zieldatenbanken erstellen. Für Aurora PostgreSQL -kompatible Version 10.18 oder höher lautet der Port 5432, und Sie können den Servernamen vom Endpunkt der DB-Instance abrufen.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikati ons-Instance.	Erstellen Sie eine Replikati ons-Instance mithilfe der AWS DMS-Konsole und geben Sie die Quell- und Zielendpunkte an. Die Replikations-Insta nce führt die Datenmigration zwischen den Endpunkten durch. Weitere Informationen finden Sie in der AWS DMS-Dokumentation.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe, um die Daten zu migrieren.	Erstellen Sie eine Aufgabe, um die IBM Db2-Quelltabellen in die PostgreSQL-DB-Ziel-Instance zu laden, indem Sie die Schritte in der AWS DMS-Dokumentation befolgen. • Verwenden Sie für Quelle und Ziel die Namen des Quell- und Zielendpunkts. • Der Migrationstyp kann Volllast sein. • Für die Schemaregel können Sie das Schema aus der Db2`inst1`-Datenbank verwenden. • Geben Sie für den Tabellennamen an, `%` um alle Tabellen zu migrieren . Wenn der Ladevorga ng abgeschlossen ist, werden die Db2-Tabellen des `inst1` Schemas in der mit Aurora PostgreSQ L kompatiblen Datenbank angezeigt.	Migrationsingenieur

Zugehörige Ressourcen

Referenzen

- Amazon-Aurora-Dokumentation
- PostgreSQL-FDW-Dokumentation (Foreign Data Wrapper)
- PostgreSQL IMPORT FOREIGN SCHEMA-Dokumentation

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation

Tutorials und Videos

- Erste Schritte mit AWS DMS (Walkthrough)
- Einführung in Amazon EC2 – Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mit SharePlex und AWS DMS

Erstellt von Kumar Bolbu P G (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS für PostgreSQL/Amazon Aurora PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS; Amazon Aurora		

Übersicht

Dieses Muster beschreibt, wie Sie eine lokale Oracle 8i- oder 9i-Datenbank zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL migrieren. AWS Database Migration Service (AWS DMS) unterstützt Oracle 8i oder 9i nicht als Quelle. Daher SharePlex repliziert Quest Daten aus einer lokalen 8i- oder 9i-Datenbank in eine mit AWS DMS kompatible Oracle-Zwischendatenbank (Oracle 10g oder 11g).

Von der Oracle-Zwischen-Instance werden das Schema und die Daten mithilfe von AWS Schema Conversion Tool (AWS SCT) und AWS DMS in die PostgreSQL-Datenbank in AWS migriert. Diese Methode hilft dabei, ein kontinuierliches Streaming von Daten von der Oracle-Quelldatenbank zur PostgreSQL-DB-Ziel-Instance mit minimaler Replikationsverzögerung zu erreichen. In dieser Implementierung ist die Ausfallzeit auf die Zeit beschränkt, die benötigt wird, um alle Fremdschlüssel, Auslöser und Sequenzen in der PostgreSQL-Zieldatenbank zu erstellen oder zu validieren.

Bei der Migration wird eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance mit installiertem Oracle 10g oder 11g verwendet, um die Änderungen aus der Oracle-Quelldatenbank zu hosten. AWS DMS verwendet diese Oracle-Zwischen-Instance als Quelle, um die Daten an Amazon RDS for PostgreSQL oder Aurora PostgreSQL zu streamen. Die Datenreplikation kann angehalten und von der lokalen Oracle-Datenbank zur zwischengeschalteten Oracle-Instance fortgesetzt werden. Sie kann auch von der Oracle-Zwischen-Instance zur PostgreSQL-Zieldatenbank angehalten und

fortgesetzt werden, sodass Sie die Daten entweder mithilfe der AWS DMS-Datenvalidierung oder eines benutzerdefinierten Datenvalidierungstools validieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle 8i- oder 9i-Quelldatenbank in einem On-Premises-Rechenzentrum
- AWS Direct Connect zwischen dem On-Premises-Rechenzentrum und AWS konfiguriert
- Java Database Connectivity (JDBC)-Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder auf der EC2-Instance installiert sind, auf der AWS SCT installiert ist
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als AWS DMS-Quelle
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als AWS DMS-Ziel
- Vertrautheit mit der Bol- SharePlex Datenreplikation

Einschränkungen

- Die Datenbankgrößenbeschränkung beträgt 64 TB
- Die lokale Oracle-Datenbank muss Enterprise Edition sein.

Produktversionen

- Oracle 8i oder 9i für die Quelldatenbank
- Oracle 10g oder 11g für die Zwischendatenbank
- PostgreSQL 9.6 oder höher

Architektur

Quelltechnologie-Stack

- Oracle 8i- oder 9i-Datenbank
- Quest SharePlex

Zieltechnologie-Stack

- Amazon RDS für PostgreSQL oder Aurora PostgreSQL

Quell- und Zielarchitektur

Tools

- AWS DMS – AWS Database Migration Service (AWS DMS) unterstützt Sie bei der schnellen und sicheren Migration von Datenbanken. Die Quelldatenbank bleibt während der Migration voll funktionsfähig und minimiert Ausfallzeiten für Anwendungen, die auf der Datenbank basieren. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren.
- AWS SCT – AWS Schema Conversion Tool (AWS SCT) macht heterogene Datenbankmigrationen vorhersehbar, indem das Quelldatenbankschema und die meisten Datenbankcodeobjekte, einschließlich Ansichten, gespeicherter Prozeduren und Funktionen, automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden. Objekte, die nicht automatisch konvertiert werden können, sind deutlich markiert, sodass sie manuell konvertiert werden können, um die Migration abzuschließen. AWS SCT kann auch Ihren Anwendungsquellcode nach eingebetteten SQL-Anweisungen scannen und sie im Rahmen eines Datenbankschemakonvertierungsprojekts konvertieren. Während dieses Prozesses führt AWS SCT eine cloudnative Codeoptimierung durch, indem ältere Oracle- und SQL Server-Funktionen in ihre AWS-Entsprechungen konvertiert werden, um Sie bei der Modernisierung Ihrer Anwendungen bei der Migration Ihrer Datenbanken zu unterstützen. Wenn die Schemakonvertierung abgeschlossen ist, kann AWS SCT mithilfe von integrierten Datenmigrationsagenten bei der Migration von Daten aus einer Reihe von Data Warehouses zu Amazon Redshift helfen.
- Bol SharePlex – Bol SharePlex ist ein Oracle-zu-Oracle-Datenreplikationstool zum Verschieben von Daten mit minimalen Ausfallzeiten und ohne Datenverlust.

Polen

Erstellen der EC2-Instance und Installieren von Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Netzwerk für Amazon EC2 ein.	Erstellen Sie die Virtual Private Cloud (VPC), Subnetze, Internet-Gateway, Routing-Tabellen und Sicherheitsgruppen.	AWS SysAdmin
Erstellen Sie die neue EC2-Instance.	Wählen Sie das Amazon Machine Image (AMI) für die EC2-Instance aus. Wählen Sie die Instance-Größe aus und konfigurieren Sie die Instance-Details: die Anzahl der Instances (1), die VPC und das Subnetz aus dem vorherigen Schritt, weisen Sie die öffentliche IP automatis ch zu und andere Optionen. Fügen Sie Speicher hinzu, konfigurieren Sie Sicherhei tsgruppen und starten Sie die Instance. Wenn Sie dazu aufgefordert werden, erstellen und speichern Sie ein Schlüsselpaar für den nächsten Schritt.	AWS SysAdmin
Installieren Sie Oracle auf der EC2-Instance.	Erlangen Sie die Lizenzen und die erforderlichen Oracle-Bi närdateien und installieren Sie Oracle 10g oder 11g auf der EC2-Instance.	DBA

Einrichten von SharePlex auf einer EC2-Instance und Konfigurieren der Datenreplikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie ein SharePlex.	Erstellen Sie eine Amazon EC2-Instance und installieren Sie die SharePlex Binärdate ien, die mit Oracle 8i oder 9i kompatibel sind.	AWS SysAdmin, DBA
Konfigurieren Sie die Datenreplikation.	Befolgen Sie SharePlex bewährte Methoden, um die Datenreplikation von einer lokalen Oracle 8i/9i-Datenbank zu einer Oracle 10g/11g-I nstance zu konfigurieren.	DBA

Konvertieren des Oracle-Datenbankschemas in PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Erstellen Sie einen neuen Bericht und stellen Sie dann eine Verbindung zu Oracle als Quelle und PostgreSQ L als Ziel her. Öffnen Sie in den Projekteinstellungen die Registerkarte SQL Scripting und ändern Sie das Ziel-SQL-Skript in Mehrere Dateien.	DBA
Konvertieren Sie das Oracle-Datenbankschema.	Wählen Sie auf der Registerk arte Aktion die Option Bericht generieren, Schema konvertie ren und dann Als SQL speichern aus.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die von AWS SCT generierten SQL-Skripts.		DBA

Erstellen und Konfigurieren der Amazon RDS-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-DB-Instance.	Erstellen Sie in der Amazon-RDS-Konsole eine neue PostgreSQL-DB-Instance.	AWS SysAdmin, DBA
Konfigurieren Sie die DB-Instance.	Geben Sie die DB-Engine -Version, die DB-Instan ce-Klasse, die Multi-AZ-Bereitstellung, den Speichert yp und den zugewiesenen Speicher an. Geben Sie die DB-Instance-Kennung, einen Masterbenutzernamen und ein Masterpasswort ein.	AWS SysAdmin, DBA
Konfigurieren Sie Netzwerk und Sicherheit.	Geben Sie die VPC, die Subnetzgruppe, die öffentliche Zugänglichkeit, die Availabil ity Zone-Präferenz und die Sicherheitsgruppen an.	AWS SysAdmin, DBA
Konfigurieren Sie Datenbank optionen.	Geben Sie den Datenbank namen, den Port, die Parametergruppe, die Verschlüsselung und den Masterschlüssel an.	AWS SysAdmin, DBA
Konfigurieren Sie die Sicherungen.	Geben Sie den Aufbewahr ungszeitraum für Backups,	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Backup-Fenster, die Startzeit, die Dauer und die Frage an, ob Tags in Snapshots kopiert werden sollen.	
Konfigurieren Sie Überwachungsoptionen.	Aktivieren oder deaktivieren Sie erweiterte Überwachung und Leistungseinblicke.	AWS SysAdmin, DBA
Konfigurieren Sie die Wartungsoptionen.	Geben Sie das automatische Upgrade der Nebenversion, das Wartungsfenster sowie den Starttag, die Uhrzeit und die Dauer an.	AWS SysAdmin, DBA
Führen Sie die Vormigrationsskripts von AWS SCT aus.	Führen Sie auf der Amazon-RDS-Instance diese Skripte aus: create_database.sql, create_sequence.sql, create_table.sql, create_view.sql und create_function.sql.	AWS SysAdmin, DBA

Migrieren von Daten mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikations-Instance in AWS DMS.	Füllen Sie die Felder für den Namen, die Instance-Klasse, die VPC (wie bei der EC2-Instance), Multi-AZ und den öffentlichen Zugriff aus. Geben Sie im Abschnitt Erweiterte Konfiguration den zugewiesenen Speicher, die Subnetzgr	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	uppe, die Availability Zone, die VPC-Sicherheitsgruppen und den AWS Key Managemen t Service (AWS KMS)-Root-Schlüssel an.	
Erstellen Sie den Endpunkt der Quelldatenbank.	Geben Sie den Endpunktn amen, den Typ, die Quell-Eng ine (Oracle), den Servernam en (Amazon EC2-DNS-N amen), den Port, den SSL-Modus, den Benutzernamen, das Passwort, die SID, die VPC (geben Sie die VPC an, die über die Replikations-Instance verfügt) und die Replikations-Instance an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDat aTypeSkalieren.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Replikationsaufgabe.	Geben Sie den Aufgabennamen, die Replikations-Instance, die Quell- und Zielendpunkte sowie die Replikations-Instance an. Wählen Sie für den Migrationstyp die Option „Bestehende Daten migrieren und laufende Änderungen replizieren“. Deaktivieren Sie das Kontrollkästchen „Aufgabe beim Erstellen starten“.	AWS SysAdmin, DBA
Konfigurieren Sie die AWS DMS-Replikationsaufgabeneinstellungen.	Wählen Sie für den Vorbereitungsmodus der Zieltabelle die Option „Nichts tun“. Halten Sie die Aufgabe nach Abschluss des vollständigen Ladevorgangs an, um Primärschlüssel zu erstellen. Geben Sie den eingeschränkten oder vollständigen LOB-Modus an und aktivieren Sie die Steuertabellen. Optional können Sie die CommitRate erweiterte Einstellung konfigurieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Tabellenzuordnungen.	Erstellen Sie im Abschnitt Tabellenzuordnungen eine Einschließen-Regel für alle Tabellen in allen Schemata, die in der Migration enthalten sind, und erstellen Sie dann eine Ausschließen-Regel. Fügen Sie drei Transform ationsregeln hinzu, um Schema-, Tabellen- und Spaltennamen in Kleinbuch staben zu konvertieren, und fügen Sie alle anderen Regeln hinzu, die für diese spezifische Migration erforderlich sind.	DBA
Starten Sie die Aufgabe.	Starten Sie die Replikati onsaufgabe. Stellen Sie sicher, dass der vollständ ige Ladevorgang ausgeführ t wird. Führen Sie ALTER SYSTEM SWITCH LOGFILE in der primären Oracle-Da tenbank aus, um die Aufgabe zu starten.	DBA
Führen Sie die Skripts für die mittlere Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: create_index.sql und create_constraint.sql.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe neu, um die Erfassung von Datenänderungen (Change Data Capture, CDC) fortzusetzen.	Führen Sie in der DB-Instance von Amazon RDS für PostgreSQL VACUUM aus und starten Sie die AWS DMS-Aufgabe neu, um die zwischengespeicherten CDC-Änderungen anzuwenden.	DBA

Umstellung auf die PostgreSQL-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS DMS-Protokolle und Metadatentabellen.	Validieren Sie alle Fehler und beheben Sie sie bei Bedarf.	DBA
Halten Sie alle Oracle-Abhängigkeiten an.	Fahren Sie Listener in der Oracle-Datenbank herunter und führen Sie ALTER SYSTEM SWITCH LOGFILE aus. Halten Sie die AWS DMS-Aufgabe an, wenn sie keine Aktivität anzeigt.	DBA
Führen Sie die Skripts nach der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: create_foreign_key_constraint.sql und create_triggers.sql.	DBA
Führen Sie alle zusätzlichen Schritte von Amazon RDS für PostgreSQL aus.	Inkrementieren Sie Sequenzen, die bei Bedarf mit Oracle übereinstimmen, führen Sie VACUUM und ANALYZE aus und erstellen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie einen Snapshot, um die Compliance zu gewährleisten.	
Öffnen Sie die Verbindungen zu Amazon RDS for PostgreSQL .	Entfernen Sie die AWS DMS-Sicherheitsgruppen aus Amazon RDS for PostgreSQL, fügen Sie Produktionssicherheitsgruppen hinzu und verweisen Sie Ihre Anwendungen auf die neue Datenbank.	DBA
Bereinigen Sie AWS DMS-Ressourcen.	Entfernen Sie die Endpunkte, Replikationsaufgaben, Replikations-Instances und die EC2-Instance.	SysAdmin, DBA

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Amazon RDS für PostgreSQL – Preise
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS
- Quest- SharePlex Dokumentation

Migrieren Sie von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mithilfe materialisierter Ansichten und AWS DMS

Erstellt von Kumar Bolbu P G (AWS) und Pragneshpatel (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle 8i oder 9i	Ziel: Amazon RDS für PostgreSQL oder Aurora PostgreSQL – kompatibel
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS; Amazon Aurora		

Übersicht

Dieses Muster beschreibt, wie Sie eine Legacy-Datenbank von Oracle 8i oder 9i vor Ort zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL - kompatible Edition migrieren.

AWS Database Migration Service (AWS DMS) unterstützt Oracle 8i oder 9i nicht als Quelle, daher verwendet dieses Muster eine mit AWS DMS kompatible Oracle-Zwischendatenbank-Instance, z. B. Oracle 10g oder 11g. Es verwendet auch die Funktion für materialisierte Ansichten, um Daten von der Oracle 8i/9i-Quell-Instance zur Oracle 10g/11g-Zwischen-Instance zu migrieren.

AWS Schema Conversion Tool (AWS SCT) konvertiert das Datenbankschema und AWS DMS migriert die Daten zur PostgreSQL-Zieldatenbank.

Dieses Muster hilft Benutzern, die mit minimaler Datenbankausfallzeit von älteren Oracle-Datenbanken migrieren möchten. In dieser Implementierung wäre die Ausfallzeit auf die Zeit beschränkt, die benötigt wird, um alle Fremdschlüssel, Auslöser und Sequenzen in der Zieldatenbank zu erstellen oder zu validieren.

Das Muster verwendet Amazon Elastic Compute Cloud (Amazon EC2)-Instances mit installierter Oracle 10g/11g-Datenbank, um AWS DMS beim Streamen der Daten zu unterstützen. Sie können die Streaming-Replikation von der lokalen Oracle-Datenbank zur zwischengeschalteten Oracle-Instance vorübergehend anhalten, damit AWS DMS die Datenvalidierung aufholt oder ein anderes

Datenvalidierungstool verwendet. Die PostgreSQL-DB-Instance und die Oracle-Zwischendatenbank haben dieselben Daten, wenn AWS DMS die Migration aktueller Änderungen abgeschlossen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle 8i- oder 9i-Quelldatenbank in einem On-Premises-Rechenzentrum
- AWS Direct Connect zwischen dem On-Premises-Rechenzentrum und AWS konfiguriert
- Java Database Connectivity (JDBC)-Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder auf der EC2-Instance installiert sind, auf der AWS SCT installiert ist
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als AWS DMS-Quelle
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als AWS DMS-Ziel

Einschränkungen

- Die Datenbankgrößenbeschränkung beträgt 64 TB

Produktversionen

- Oracle 8i oder 9i für die Quelldatenbank
- Oracle 10g oder 11g für die Zwischendatenbank
- PostgreSQL 10.17 oder höher

Architektur

Quelltechnologie-Stack

- Oracle 8i- oder 9i-Datenbank

Zieltechnologie-Stack

- Amazon RDS für PostgreSQL oder Aurora PostgreSQL – kompatibel

Zielarchitektur

Tools

- AWS DMS hilft bei der schnellen und sicheren Migration von Datenbanken. Die Quelldatenbank bleibt während der Migration voll funktionsfähig und minimiert Ausfallzeiten für Anwendungen, die auf der Datenbank basieren. AWS DMS kann Ihre Daten zu und von den gängigsten kommerziellen und Open-Source-Datenbanken migrieren.
- AWS SCT konvertiert das Quelldatenbankschema und die meisten Datenbankcodeobjekte, einschließlich Ansichten, gespeicherter Prozeduren und Funktionen, automatisch in ein mit der Zieldatenbank kompatibles Format. Objekte, die nicht automatisch konvertiert werden können, sind deutlich markiert, sodass sie manuell konvertiert werden können, um die Migration abzuschließen. AWS SCT kann Ihren Anwendungsquellcode auch nach eingebetteten SQL-Anweisungen scannen und sie im Rahmen eines Datenbankschemakonvertierungsprojekts konvertieren. Während dieses Prozesses führt AWS SCT eine cloudnative Codeoptimierung durch, indem ältere Oracle- und SQL Server-Funktionen in ihre AWS-Entsprechungen konvertiert werden, um Sie bei der Modernisierung Ihrer Anwendungen bei der Migration Ihrer Datenbanken zu unterstützen. Wenn die Schemakonvertierung abgeschlossen ist, kann AWS SCT mithilfe von integrierten Datenmigrationsagenten bei der Migration von Daten aus einer Reihe von Data Warehouses zu Amazon Redshift helfen.

Bewährte Methoden

Bewährte Methoden für die Aktualisierung materialisierter Ansichten finden Sie in der folgenden Oracle-Dokumentation:

- Aktualisieren materialisierter Ansichten
- Schnelle Aktualisierung für materialisierte Ansichten

Polen

Installieren von Oracle auf einer EC2-Instance und Erstellen materialisierter Ansichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Netzwerk für die EC2-Instance ein.	Erstellen Sie die Virtual Private Cloud (VPC),	AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Subnetze, Internet-Gateway, Routing-Tabellen und Sicherheitsgruppen.	
Erstellen Sie die EC2-Instance.	Wählen Sie das Amazon Machine Image (AMI) für die EC2-Instance aus. Wählen Sie die Instance-Größe aus und konfigurieren Sie Instance-Details: die Anzahl der Instances (1), die VPC und das Subnetz aus dem vorherigen Schritt, weisen Sie die öffentliche IP automatisch zu und andere Optionen. Fügen Sie Speicher hinzu, konfigurieren Sie Sicherheitsgruppen und starten Sie die Instance. Wenn Sie dazu aufgefordert werden, erstellen und speichern Sie ein Schlüsselpaar für den nächsten Schritt.	AWS SysAdmin
Installieren Sie Oracle auf der EC2-Instance.	Erlangen Sie die Lizenzen und die erforderlichen Oracle-Binärdateien und installieren Sie Oracle 10g oder 11g auf der EC2-Instance.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Oracle-Netzwerke.	Ändern oder fügen Sie Einträge in hinzu`listener.ora` , um eine Verbindung mit der lokalen Oracle 8i/9i-Quelldatenbank herzustellen, und erstellen Sie dann die Datenbanklinks.	DBA
Erstellen Sie materialisierte Ansichten.	Identifizieren Sie die Datenbankobjekte, die in der Oracle 8i/9i-Quelldatenbank repliziert werden sollen, und erstellen Sie dann materialisierte Ansichten für alle Objekte mithilfe des Datenbanklinks.	DBA
Stellen Sie Skripts bereit, um materialisierte Ansichten in erforderlichen Intervallen zu aktualisieren.	Entwickeln und stellen Sie Skripts bereit, um materialisierte Ansichten in erforderlichen Intervallen auf der Amazon EC2 Oracle 10g/11g-Instance zu aktualisieren. Verwenden Sie die Option für die inkrementelle Aktualisierung, um materialisierte Ansichten zu aktualisieren.	DBA

Konvertieren des Oracle-Datenbankschemas in PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Erstellen Sie einen neuen Bericht und stellen Sie dann	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine Verbindung zu Oracle als Quelle und PostgreSQL als Ziel her. Öffnen Sie in den Projekteinstellungen die Registerkarte SQL Scripting. Ändern Sie das Ziel-SQL-Skript in Mehrere Dateien. (AWS SCT unterstützt keine Oracle 8i/9i-Datenbanken, daher müssen Sie den reinen Schema-Dump auf der Oracle 10g/11g-Zwischen-Instance wiederherstellen und als Quelle für AWS SCT verwenden.)	
Konvertieren Sie das Oracle-Datenbankschema.	Wählen Sie auf der Registerkarte Aktion die Option Bericht generieren, Schema konvertieren und dann Als SQL speichern aus.	DBA
Ändern Sie die SQL-Skripts.	Nehmen Sie Änderungen basierend auf bewährten Methoden vor. Wechseln Sie beispielsweise zu geeignete n Datentypen und entwickeln Sie PostgreSQL-Äquivalente für Oracle-spezifische Funktionen.	DBA, DevDBA

Erstellen und Konfigurieren der Amazon RDS-DB-Instance zum Hosten der konvertierten Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-DB-Instance.	Erstellen Sie in der Amazon-RDS-Konsole eine neue PostgreSQL-DB-Instance.	AWS SysAdmin, DBA
Konfigurieren Sie die DB-Instance.	Geben Sie die DB-Engine -Version, die DB-Instan ce-Klasse, die Multi-AZ-Bereitstellung, den Speichert yp und den zugewiesenen Speicher an. Geben Sie die DB-Instance-Kennung, einen Masterbenutzernamen und ein Masterpasswort ein.	AWS SysAdmin, DBA
Konfigurieren Sie Netzwerk und Sicherheit.	Geben Sie die VPC, die Subnetzgruppe, die öffentliche Zugänglichkeit, die Availabil ity Zone-Präferenz und die Sicherheitsgruppen an.	DBA, SysAdmin
Konfigurieren Sie Datenbank optionen.	Geben Sie den Datenbank namen, den Port, die Parametergruppe, die Verschlüsselung und den Masterschlüssel an.	DBA, AWS SysAdmin
Konfigurieren Sie die Sicherungen.	Geben Sie den Aufbewahr ungszeitraum für Backups, das Backup-Fenster, die Startzeit, die Dauer und die Frage an, ob Tags in Snapshots kopiert werden sollen.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Überwachungsoptionen.	Aktivieren oder deaktivieren Sie erweiterte Überwachung und Leistungseinblicke.	AWS SysAdmin, DBA
Konfigurieren Sie die Wartungsoptionen.	Geben Sie das automatische Upgrade der Nebenversion, das Wartungsfenster sowie den Starttag, die Uhrzeit und die Dauer an.	AWS SysAdmin, DBA
Führen Sie die Vormigrationsskripts von AWS SCT aus.	Erstellen Sie auf der Amazon RDS for PostgreSQL-Ziel-Instance das Datenbankschema, indem Sie die SQL-Skripte von AWS SCT mit anderen Änderungen verwenden. Dazu gehören die Ausführung mehrerer Skripts und einschließlich Benutzererstellung, Datenbankerstellung, Schemaerstellung, Tabellen, Ansichten, Funktionen und anderer Codeobjekte.	AWS SysAdmin, DBA

Migrieren von Daten mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikations-Instance in AWS DMS.	Füllen Sie die Felder für den Namen, die Instance-Klasse, die VPC (wie bei der EC2-Instance), Multi-AZ und den öffentlichen Zugriff aus. Geben Sie im Abschnitt Erweiterte	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konfiguration den zugewiesenen Speicher, die Subnetzgruppe, die Availability Zone, die VPC-Sicherheitsgruppen und den AWS Key Management Service (AWS KMS)-Schlüssel an.	
Erstellen Sie den Endpunkt der Quelldatenbank.	Geben Sie den Endpunktnamen, den Typ, die Quell-Engine (Oracle), den Servernamen (den privaten DNS-Namen der EC2-Instance), den Port, den SSL-Modus, den Benutzernamen, das Passwort, die SID, die VPC (angeben der VPC mit der Replikations-Instance) und die Replikations-Instance an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDataTypeSkalieren von .	AWS SysAdmin, DBA
Verbinden Sie AWS DMS mit Amazon RDS for PostgreSQL .	Erstellen Sie eine Migrationssicherheitsgruppe für Verbindungen zwischen VPCs, wenn sich Ihre PostgreSQL-Datenbank in einer anderen VPC befindet.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Zieldaten bank-Endpunkt.	Geben Sie den Endpunktn amen, den Typ, die Quell-Engine (PostgreSQL), den Servernamen (Amazon-RDS-Endpunkt), den Port, den SSL-Modus, den Benutzernamen, das Passwort, den Datenbank namen, die VPC (geben Sie die VPC an, die über die Replikations-Instance verfügt) und die Replikations-Insta nce an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDataTypeSkal ieren von .	AWS SysAdmin, DBA
Erstellen Sie die AWS DMS-Replikationsaufgabe.	Geben Sie den Aufgabenn amen, die Replikations-Insta nce, die Quell- und Zielendpu nkte sowie die Replikations-Instance an. Wählen Sie für Migrationstyp die Option Vorhandene Daten migrieren und laufende Änderungen replizieren aus. Deaktivie ren Sie das Kontrollkästchen Aufgabe beim Erstellen starten.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS DMS-Replikationsaufgabeneinstellungen.	Wählen Sie für den Vorbereitungsmodus der Zieltabelle die Option Nichts tun aus. Halten Sie die Aufgabe an, nachdem der vollständige Ladevorgang abgeschlossen ist (um Primärschlüssel zu erstellen). Geben Sie den eingeschränkten oder vollständigen LOB-Modus an und aktivieren Sie die Steuertabellen. Optional können Sie die CommitRate erweiterte Einstellung konfigurieren.	DBA
Konfigurieren Sie die Tabellenzuordnungen.	Erstellen Sie im Abschnitt Tabellenzuordnungen eine Einschließen-Regel für alle Tabellen in allen Schemata, die in der Migration enthalten sind, und erstellen Sie dann eine Ausschließen-Regel. Fügen Sie drei Transformationsregeln hinzu, um Schema-, Tabellen- und Spaltennamen in Kleinbuchstaben zu konvertieren, und fügen Sie alle anderen Regeln hinzu, die Sie für diese spezifische Migration benötigen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe.	Starten Sie die Replikati onsaufgabe. Stellen Sie sicher, dass der vollständ ige Ladevorgang ausgeführ t wird. Führen Sie `ALTER SYSTEM SWITCH LOGFILE` in der primären Oracle-Da tenbank aus, um die Aufgabe zu starten.	DBA
Führen Sie die Skripts für die mittlere Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: `create_in dex.sql` und `create_co nstraint.sql` (wenn das vollständige Schema nicht ursprünglich erstellt wurde).	DBA
Setzen Sie die Aufgabe fort, um die Erfassung von Datenänderungen (Change Data Capture, CDC) fortzuset zen.	Führen Sie `VACUUM` auf der Amazon RDS for PostgreSQ L-DB-Instance aus und starten Sie die AWS DMS-Aufgabe neu, um zwischeng espeicherte CDC-Änderungen anzuwenden.	DBA

Umstellung auf die PostgreSQL-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS DMS-Protokolle und -Validier ungstabellen.	Überprüfen und beheben Sie Replikations- oder Validieru ngsfehler.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Verwendung der lokalen Oracle-Datenbank und ihrer Abhängigkeiten.	Halten Sie alle Oracle-Abhängigkeiten an, fahren Sie Listener in der Oracle-Datenbank herunter und führen Sie aus`ALTER SYSTEM SWITCH LOGFILE`. Halten Sie die AWS DMS-Aufgabe an, wenn sie keine Aktivität anzeigt.	DBA
Führen Sie die Skripts nach der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: `create_foreign_key_constraint.sql and create_triggers.sql` . Stellen Sie sicher, dass die Sequenzen auf dem neuesten Stand sind.	DBA
Führen Sie zusätzliche Schritte von Amazon RDS für PostgreSQL aus.	Inkrementieren Sie Sequenzen, die bei Bedarf mit Oracle übereinstimmen, führen Sie `VACUUM` und aus `ANALYZE`und erstellen Sie einen Snapshot, um die Compliance zu gewährleisten.	DBA
Öffnen Sie die Verbindungen zu Amazon RDS for PostgreSQL .	Entfernen Sie die AWS DMS-Sicherheitsgruppen aus Amazon RDS for PostgreSQL, fügen Sie Produktionssicherheitsgruppen hinzu und verweisen Sie Ihre Anwendungen auf die neue Datenbank.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die AWS DMS-Objekte.	Entfernen Sie die Endpunkte , Replikationsaufgaben, Replikations-Instances und die EC2-Instance.	SysAdmin, DBA

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Amazon RDS für PostgreSQL – Preise
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS

Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL

Erstellt von Anil Kunapareddy (AWS) und Harshad Gohil

Umgebung: PoC oder Pilot	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for MySQL
R-Typ: Re-Architect	Arbeitslast: Oracle	Technologien: Migration; Datenbanken
AWS-Dienste: Amazon RDS		

Übersicht

Die Verwaltung von Oracle-Datenbanken auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances erfordert Ressourcen und kann kostspielig sein. Das Verschieben dieser Datenbanken in eine Amazon Relational Database Service (Amazon RDS) für MySQL-DB-Instance erleichtert Ihnen die Arbeit, da das gesamte IT-Budget optimiert wird. Amazon RDS for MySQL bietet auch Funktionen wie Multi-AZ, Skalierbarkeit und automatische Backups.

Dieses Muster führt Sie durch die Migration einer Oracle-Quelldatenbank auf Amazon EC2 zu einer Amazon RDS for MySQL MySQL-DB-Zielinstanz. Es verwendet AWS Database Migration Service (AWS DMS), um die Daten zu migrieren, und das AWS Schema Conversion Tool (AWS SCT), um das Quelldatenbankschema und die Objekte in ein Format zu konvertieren, das mit Amazon RDS for MySQL kompatibel ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Quelldatenbank mit laufenden Instance- und Listener-Services im ARCHIVELOG-Modus
- Eine Amazon RDS for MySQL MySQL-Zieldatenbank mit ausreichend Speicherplatz für die Datenmigration

Einschränkungen

- AWS DMS erstellt kein Schema in der Zieldatenbank; das müssen Sie tun. Der Schemaname muss für das Ziel bereits vorhanden sein. Tabellen aus dem Quellschema werden in den Benutzer/das Schema importiert, das AWS DMS verwendet, um eine Verbindung mit der Zielinstanz herzustellen. Zum Migrieren von mehreren Schemata müssen Sie mehrere Replikationsaufgaben erstellen.

Produktversionen

- Alle Oracle-Datenbankeditionen für die Versionen 10.2 und höher, 11g und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Oracle-Datenbankversionen finden Sie in der AWS SCT-Dokumentation.
- AWS DMS unterstützt die Versionen 5.5, 5.6 und 5.7 von MySQL.

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank auf einer EC2-Instance

Zieltechnologie-Stack

- Amazon RDS for MySQL MySQL-DB-Instance

Architektur der Datenmigration

Quell- und Zielarchitektur

Tools

- AWS DMS — AWS Database Migration Service (AWS DMS) ist ein Webservice, mit dem Sie Daten aus Ihrer lokalen Datenbank, auf einer Amazon RDS-DB-Instance oder in einer Datenbank

auf einer EC2-Instance in eine Datenbank in einem AWS-Service wie Amazon RDS for MySQL oder einer EC2-Instance migrieren können. Sie können eine Datenbank auch von einem AWS-Service zu einer lokalen Datenbank migrieren. Sie können Daten zwischen heterogenen oder homogenen Datenbank-Engines migrieren.

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) macht heterogene Datenbankmigrationen vorhersehbar, indem das Quelldatenbankschema und ein Großteil der Datenbankcode-Objekte, einschließlich Ansichten, gespeicherten Prozeduren und Funktionen, automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Nachdem Sie Ihr Datenbankschema und Ihre Codeobjekte mit AWS SCT konvertiert haben, können Sie AWS DMS verwenden, um Daten von der Quelldatenbank in die Zieldatenbank zu migrieren, um Ihre Migrationsprojekte abzuschließen.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA/Entwickler
Identifizieren Sie die DMS-Replikationsinstanz.		DBA/Entwickler
Identifizieren Sie Speichera nforderungen wie Speichertyp und Kapazität.		DBA/Entwickler
Identifizieren Sie Netzwerka nforderungen wie Latenz und Bandbreite.		DBA/Entwickler
Identifizieren Sie die Hardwareanforderungen für die Quell- und Zielserve rinstanzen (basierend auf der Oracle-Kompatibilitätsliste		DBA/Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
und den Kapazitätsanforder ungen).		
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA/Entwickler
Installieren Sie die AWS SCT- und Oracle-Treiber.		DBA/Entwickler
Legen Sie eine Backup-St rategie fest.		DBA/Entwickler
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA/Entwickler
Identifizieren Sie die Strategie für Anwendungsmigration und Umstellung.		DBA/Entwickler
Wählen Sie den richtigen DB-Instance-Typ auf der Grundlage von Kapazität , Speicher und Netzwerkf unktionen aus.		DBA/Entwickler

Konfigurieren Sie die Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC). Die Quell-, Ziel- und Replikationsinstan z sollten sich in derselben VPC befinden. Es ist auch gut,		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
diese in derselben Availability Zone zu haben.		
Erstellen Sie die erforderlichen Sicherheitsgruppen für den Datenbankzugriff.		Developer
Generieren und konfigurieren Sie ein key pair.		Developer
Konfigurieren Sie Subnetze, Availability Zones und CIDR-Blöcke.		Developer

Konfigurieren Sie die Quelle: Oracle-Datenbank auf der EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle Database auf Amazon EC2 mit den erforderlichen Benutzern und Rollen.		DBA
Führen Sie die drei Schritte in der nächsten Spalte aus, um von außerhalb der EC2-Instance auf Oracle zuzugreifen.	1. Ändern Sie den lokalen Host in `tnsnames` das öffentliche DNS von Amazon EC2. 2. Ändern Sie den lokalen Host in `listener` das öffentliche DNS von Amazon EC2. 3. Stoppen Sie den Listener und starten Sie ihn neu.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenn Amazon EC2 neu gestartet wird, ändert sich das öffentliche DNS. Stellen Sie sicher, dass Sie das öffentlic he DNS von Amazon EC2 in „tnsnames“ und „listener“ aktualisieren oder eine Elastic IP-Adresse verwenden.		DBA/Entwickler
Konfigurieren Sie die EC2-Instanz-Sicherheitsgruppe so, dass die Replikationsinstan z und die erforderlichen Clients auf die Quelldatenbank zugreifen können.		DBA/Entwickler

Konfigurieren Sie das Ziel: Amazon RDS for MySQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie die Amazon RDS for MySQL MySQL-DB-Instance.		Developer
Erstellen Sie den erforderl ichen Tablespace in der Amazon RDS for MySQL MySQL-DB-Instance.		DBA
Konfigurieren Sie die Sicherheitsgruppe so, dass die Replikationsinstanz und die erforderlichen Clients auf		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
die Zieldatenbank zugreifen können.		

AWS SCT konfigurieren und ein Schema in der Zieldatenbank erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die AWS SCT- und Oracle-Treiber.		Developer
Geben Sie die entsprech enden Parameter ein und stellen Sie eine Verbindung zur Quelle und zum Ziel her.		Developer
Generieren Sie einen Bericht zur Schemakonvertierung.		Developer
Korrigieren Sie den Code und das Schema nach Bedarf, insbesondere Tablespaces und Anführungszeichen, und führen Sie die Ausführung in der Zieldatenbank aus.		Developer
Überprüfen Sie das Schema auf Quelle und Ziel, bevor Sie Daten migrieren.		Developer

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Für Full-Load and Change Data Capture (CDC) oder nur		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
CDC müssen Sie ein zusätzlic hes Verbindungsattribut festlegen.		
Dem in den Definitionen der AWS DMS-Oracle-Quellda tenbank angegebenen Benutzer müssen alle erforderl ichen Rechte gewährt werden. Eine vollständige Liste finden Sie unter https://docs.aws.a mazon.com/dms/latest/usergu ide/CHAP_Source.Oracle.html #CHAP_Source.Oracle.Self-Managed.		DBA/Entwickler
Aktivieren Sie die zusätzlic he Protokollierung in der Quelldatenbank.		DBA/Entwickler
Für Full-Load and Change Data Capture (CDC) oder nur CDC aktivieren Sie den ARCHIVELOG-Modus in der Quelldatenbank.		DBA
Erstellen Sie Quell- und Zielendpunkte und testen Sie die Verbindungen.		Developer
Wenn die Endpunkte erfolgrei ch verbunden wurden, erstellen Sie eine Replizier ungsaufgabe.		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie in der Aufgabe nur CDC (oder) Volllast plus CDC aus, um Änderungen nur für die kontinuierliche Replikati on zu erfassen (oder) Volllast plus laufende Änderungen.		Developer
Führen Sie die Replikati onsaufgabe aus und überwachen Sie die CloudWatch Amazon-Pr otokolle.		Developer
Überprüfen Sie die Daten in den Quell- und Zieldaten banken.		Developer

Migrieren Sie Ihre Anwendung und wechseln Sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie den Schritten für Ihre Strategie zur Anwendung smigration.		DBA, Entwickler, App-Besitzer
Folgen Sie den Schritten für Ihre Strategie zur Umstellun g und Umstellung von Anwendungen.		DBA, Entwickler, App-Besitzer

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das Schema und die Daten in Quell- und Zieldatenbanken.		DBA/Entwickler
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Änderungen im Vergleich zu Tools, zu Kosteneinsparungen usw.		DBA/Entwickler/ AppOwner
Überprüfen Sie die Projektdo kumente und Artefakte.		DBA/Entwickler/ AppOwner
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA/Entwickler
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA/Entwickler/ AppOwner

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS DMS-Webseite
- AWS DMS-Blogbeiträge
- Strategien für die Migration von Oracle Database in AWS
- Häufig gestellte Fragen zu Amazon RDS for Oracle
- Häufig gestellte Fragen zu Oracle
- Amazon EC2
- Häufig gestellte Fragen zu Amazon EC2
- Lizenzierung von Oracle-Software in der Cloud-Computing-Umgebung

Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB

R-Typ: Re-Architect	Quelle: Datenbanken: Relational	Ziel: Amazon DocumentDB
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: Oracle	AWS-Dienste: Amazon DocumentDB	

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Oracle-Datenbank zu einer Amazon DocumentDB DocumentDB-Datenbank (mit MongoDB-Kompatibilität) mithilfe von AWS Database Migration Service (AWS DMS). Dieser Ansatz kann sowohl auf eine lokale Oracle-Quelldatenbank als auch auf eine Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance angewendet werden. Dieses Muster verwendet eine Amazon RDS Oracle DB-Quell-Instance als Beispiel.

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein vollständig verwalteter, MongoDB-kompatibler Dokumentendatenbankservice, der das Speichern, Abfragen und Indizieren von JSON-Daten vereinfacht.

Der Anwendungsfall für dieses Muster ist die one-to-one Replikation einer Oracle-Datenbanktabelle in eine Amazon DocumentDB-Sammlung. Das Muster verwendet AWS DMS-Replikationsaufgaben, um die Tabellenstruktur der Oracle-Datenbank zu lesen, die entsprechende Sammlung in Amazon DocumentDB zu erstellen und eine Volllastmigration durchzuführen. Sie können Ihre Daten in Amazon DocumentDB genau wie in MongoDB anzeigen und abfragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Vertrautheit mit der Verwendung von Oracle-Datenbanken

- Vertrautheit mit der Verwendung von Amazon DocumentDB
- Für den Oracle-Benutzer: SELECT ANY TABLE-Privileg
- Für die Verwendung von Amazon DocumentDB ist das Recht erforderlich, Daten zu speichern

Einschränkungen

Bei der Verwendung von Amazon DocumentDB als Ziel für AWS DMS gelten die folgenden Einschränkungen:

- In Amazon DocumentDB dürfen Namen für Sammlungen nicht das Dollarzeichen ($) enthalten. Darüber hinaus dürfen Datenbanknamen keine Unicode-Zeichen enthalten.
- AWS DMS unterstützt nicht die Zusammenführung mehrerer Quelltabellen zu einer einzigen Amazon DocumentDB-Sammlung.
- Wenn AWS DMS Änderungen aus einer Quelltabelle verarbeitet, die keinen Primärschlüssel hat, werden alle LOB-Spalten (Large Binary Object) in dieser Tabelle ignoriert.
- Wenn die Option Tabelle ändern aktiviert ist und AWS DMS auf eine Quellspalte mit dem Namen „_id“ stößt, wird diese Spalte in der Änderungstabelle als „__id“ (zwei Unterstriche) angezeigt.
- Wenn Sie Oracle als Quellendpunkt wählen, muss für die Oracle-Quelle die vollständige zusätzliche Protokollierung aktiviert sein. Andernfalls, wenn die Quelle Spalten enthält, die nicht geändert wurden, werden die Daten als Nullwerte in Amazon DocumentDB geladen.

Produktversionen

- Amazon RDS for Oracle Version 11.2.0.3 oder höher
- AWS DMS-Version 3.1.3 oder höher (die neuesten Versionsinformationen finden Sie unter Verwenden von Amazon DocumentDB als Ziel für AWS DMS in der AWS DMS-Dokumentation)

Architektur

Quelltechnologie-Stack

- Amazon RDS for Oracle Oracle-DB-Instance

Zieltechnologie-Stack

- Amazon DocumentDB

Quell- und Zielarchitektur

Tools

- AWS DMS — AWS Database Migration Service (AWS DMS) ist ein Webservice, mit dem Sie Daten von einem Quelldatenspeicher zu einem Zieldatenspeicher migrieren können. Das AWS DMS-Benutzerhandbuch spezifiziert die Versionen und Editionen der Oracle-Quelldatenbank, die für die Verwendung mit AWS DMS unterstützt werden. Weitere Informationen zu diesem Muster finden Sie unter Amazon DocumentDB als Ziel für AWS DMS verwenden.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Ihr Amazon DocumentDB-Cluster sollte in Ihrer standardmäßigen Virtual Private Cloud (VPC) laufen. Um mit Ihrem Amazon DocumentDB-Cluster zu interagieren, müssen Sie eine EC2-Instance in Ihrer Standard-VPC in derselben AWS-Region starten, in der Sie Ihren Amazon DocumentDB-Cluster erstellt haben. Einzelheiten finden Sie unter Starten einer Amazon EC2 EC2-Instance in der Amazon DocumentDB DocumentDB-Dokumentation.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		AWS-Administrator
Wählen Sie den richtigen Instance-Typ (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		AWS-Administrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerk-/Hostzugriff für die Quell- und Zieldatenbanken.		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Sicherheitsgruppe für ausgehenden Datenverkehr zu den Quell- und Zieldatenbanken.		AWS-Administrator
Erstellen und konfigurieren Sie eine EC2-Instance für Amazon DocumentDB.		AWS-Administrator

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC und Subnetze.		AWS-Administrator
Erstellen Sie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs).		AWS-Administrator
Konfigurieren und starten Sie die Amazon RDS for Oracle Oracle-Quell-Instance.		AWS-Administrator
Konfigurieren und starten Sie die Amazon DocumentDB DocumentDB-Instance.		AWS-Administrator

Bereiten Sie die Quelldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie anhand der Verbindungsdetails sicher,		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
dass die Oracle-Datenbank verbunden werden kann.		
Stellen Sie sicher, dass der Oracle-Benutzer über das SELECT ANY TABLE-Privileg verfügt.		AWS-Administrator

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Amazon DocumentDB-Cluster, indem Sie die richtige Instance-Klasse und Anzahl der Instances auswählen.		AWS-Administrator

Amazon EC2 konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die EC2-Instanz.	Um mit Ihrem Amazon DocumentDB-Cluster zu interagieren, müssen Sie eine EC2-Instance in Ihrer Standard-VPC in derselben AWS-Region starten, in der Sie Ihren Amazon DocumentDB-Cluster erstellt haben. Konfigurieren Sie die AWS-Region, VPCs, Availability Zones und Subnetze für die EC2-Instance.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das key pair.	Mit einem öffentlichen/privaten key pair können Sie nach dem Start eine sichere Verbindung zur EC2-Instance herstellen.	AWS-Administrator
Legen Sie die CIDR-Bereiche für den Bastion-Host fest (optional).	Legen Sie den CIDR-IP-Bereich fest, der für den externen Secure Shell (SSH) -Zugriff auf die Bastion-Host-Instanzen zulässig ist.	AWS-Administrator

Daten migrieren — Volllast

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.		AWS-Administrator
Erstellen Sie Quell- und Zielendpunkte.		AWS-Administrator
Erstellen Sie AWS DMS-Replikationsaufgaben für eine Volllast.		AWS-Administrator

Testen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über die EC2-Instance eine Connect zum Amazon DocumentDB-Cluster her.		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe der Mongo-Shell eine Connect zum Cluster her.	Anweisungen finden Sie unter den Amazon DocumentDB DocumentDB-Links im Abschnitt Referenzen und Hilfe.	AWS-Administrator
Überprüfen Sie die Ergebnisse der Migration.		AWS-Administrator

Zugehörige Ressourcen

- So funktioniert AWS DMS
- Migration zu Amazon DocumentDB
- Amazon DocumentDB als Ziel für AWS DMS verwenden
- Überblick über Amazon DocumentDB
- Greifen Sie mit der Mongo-Shell auf Ihren Amazon DocumentDB-Cluster zu und verwenden Sie ihn
- Migrieren Sie mithilfe der Offline-Methode von MongoDB zu Amazon DocumentDB (Blogbeitrag)
- So verwenden Sie Amazon DocumentDB (mit MongoDB-Kompatibilität), um skalierbare Anwendungen zu erstellen und zu verwalten (Blogbeitrag)

Migrieren einer Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB mithilfe von AWS DMS und AWS SCT

Erstellt von Veeranjaney Bol Grandhi (AWS) und vinod kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for MariaDB
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer Oracle-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance zu einer Amazon Relational Database Service (Amazon RDS) for MariaDB-DB-Instance. Das Muster verwendet AWS Data Migration Service (AWS DMS) für die Datenmigration und AWS Schema Conversion Tool (AWS SCT) für die Schemakonvertierung.

Die Verwaltung von Oracle-Datenbanken auf EC2-Instances erfordert mehr Ressourcen und ist teurer als die Verwendung einer Datenbank auf Amazon RDS. Amazon RDS erleichtert das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud. Amazon RDS bietet kostengünstige und anpassbare Kapazität und automatisiert gleichzeitig zeitaufwändige Verwaltungsaufgaben wie Hardwarebereitstellung, Datenbankeinrichtung, Patching und Backups.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Oracle-Quelldatenbank, in der Instance- und Listener-Services ausgeführt werden. Diese Datenbank sollte sich im Modus ARCHIVELOG befinden.
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS.
- Vertrautheit mit der Verwendung von Oracle als Quelle für AWS SCT.

Einschränkungen

- Datenbankgrößenbeschränkung: 64 TB

Produktversionen

- Alle Oracle-Datenbank-Editionen für die Versionen 10.2 und höher, 11g und bis 12.2 und 18c. Die neueste Liste der unterstützten Versionen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und in der AWS SCT-Versionstabelle in der AWS-Dokumentation.
- Amazon RDS unterstützt die MariaDB Server Community Server-Versionen 10.3, 10.4, 10.5 und 10.6. Die neueste Liste der unterstützten Versionen finden Sie in der Amazon-RDS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank auf einer EC2-Instance

Zieltechnologie-Stack

- Amazon RDS für MariaDB

Datenmigrationsarchitektur

Zielarchitektur

Tools

- AWS Schema Conversion Tool (AWS SCT) macht heterogene Datenbankmigrationen vorhersehbar, indem das Quelldatenbankschema und die meisten Datenbankcodeobjekte – einschließlich Ansichten, gespeicherter Prozeduren und Funktionen – automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden. Nachdem Sie Ihr Datenbankschema und Ihre Codeobjekte mit AWS SCT konvertiert haben, können Sie AWS DMS verwenden, um Daten von der Quelldatenbank zur Zieldatenbank zu migrieren, um Ihre Migrationsprojekte abzuschließen.

Weitere Informationen finden Sie unter Verwenden von Oracle als Quelle für AWS SCT in der AWS SCT-Dokumentation.

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der schnellen und sicheren Migration von Datenbanken zu AWS. Die Quelldatenbank bleibt während der Migration voll funktionsfähig und minimiert Ausfallzeiten für Anwendungen, die auf der Datenbank basieren. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren. AWS DMS unterstützt homogene Migrationen wie Oracle zu Oracle sowie heterogene Migrationen zwischen verschiedenen Datenbankplattformen wie Oracle oder Microsoft SQL Server zu Amazon Aurora. Weitere Informationen zum Migrieren von Oracle-Datenbanken finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation.

Polen

Plan für die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Versionen und Datenbank-Engines.	Identifizieren Sie die Quell- und Zieldatenbankversionen und Engines.	DBA, Entwickler
Identifizieren Sie die Replikations-Instance.	Identifizieren Sie die AWS DMS-Replikations-Instance.	DBA, Entwickler
Identifizieren Sie die Speicheranforderungen.	Identifizieren Sie Speichertyp und Kapazität.	DBA, Entwickler
Identifizieren Sie die Netzwerkanforderungen.	Identifizieren Sie Netzwerklatenz und Bandbreite.	DBA, Entwickler
Identifizieren Sie Hardwareanforderungen.	Identifizieren Sie Hardwareanforderungen für die Quell- und Zielserver-Instances (basierend auf der Oracle-Kompatibilitätsliste und den Kapazitätsanforderungen).	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Sicherhei tsanforderungen.	Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	DBA, Entwickler
Installieren Sie Treiber.	Installieren Sie die neuesten AWS SCT- und Oracle-Tr eiber.	DBA, Entwickler
Legen Sie eine Backup-St rategie fest.		DBA, Entwickler
Bestimmen Sie die Verfügbar keitsanforderungen.		DBA, Entwickler
Wählen Sie eine Strategie für die Migration/Umschaltung von Anwendungen aus.		DBA, Entwickler
Wählen Sie den -Instance-Typ aus.	Wählen Sie den richtigen Instance-Typ basierend auf Kapazität, Speicher und Netzwerkfunktionen aus.	DBA, Entwickler

Konfigurieren der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Die Quell-, Ziel- und Replikati ons-Instances sollten sich in derselben VPC und in derselben Availability Zone befinden (empfohlen).	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherhei tsgruppen.	Erstellen Sie die erforderlichen Sicherheitsgruppen für den Datenbankzugriff.	Developer
Erzeugen Sie ein Schlüssel paar.	Generieren und konfigurieren Sie ein Schlüsselpaar.	Developer
Konfigurieren Sie andere - Ressourcen.	Konfigurieren Sie Subnetze, Availability Zones und CIDR-Blöcke.	Developer

Konfigurieren der Quelle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die EC2-Instance.	Anweisungen finden Sie in der Amazon EC2-Dokumentation.	Developer
Installieren Sie die Oracle-Da tenbank.	Installieren Sie die Oracle-Datenbank auf der EC2-Insta nce mit den erforderlichen Benutzern und Rollen.	DBA
Führen Sie die Schritte in der Aufgabenbeschreibung aus, um von außerhalb der EC2-Instance auf Oracle zuzugreif en.	1. Ändern Sie den lokalen Host in `tnsnames` in das öffentliche DNS von Amazon EC2. 2. Ändern Sie den lokalen Host in `listener` in das öffentliche DNS von Amazon EC2. 3. Stoppen Sie den Listener und starten Sie ihn neu.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie das öffentlic he DNS von Amazon EC2.	Nach dem Neustart der EC2-Instance ändert sich das öffentliche DNS. Stellen Sie sicher, dass Sie das öffentlic he Amazon EC2-DNS in `tnsnames` und aktualisieren `listener`oder eine Elastic-I P-Adresse verwenden.	DBA, Entwickler
Konfigurieren Sie die EC2-Instance-Sicherheitsgruppe.	Konfigurieren Sie die EC2-Instance-Sicherheitsgruppe so, dass die Replikations-Instanz und die erforderlichen Clients auf die Quelldatenbank zugreifen können.	DBA, Entwickler

Konfigurieren der Amazon RDS for MariaDB-Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die RDS-DB-In stance.	Konfigurieren und starten Sie die DB-Instance von Amazon RDS for MariaDB.	Developer
Erstellen Sie Tablespaces.	Erstellen Sie alle erforderl ichen Tabellenbereiche in der Amazon RDS MariaDB-D atenbank.	DBA
Konfigurieren Sie eine Sicherheitsgruppe.	Konfigurieren Sie eine Sicherheitsgruppe, damit die Replikations-Instance und die erforderlichen Clients auf	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Zieldatenbank zugreifen können.	

Konfigurieren von AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Treiber.	Installieren Sie die neuesten AWS SCT- und Oracle-Tr eiber.	Developer
Connect (Verbinden).	Geben Sie die entsprech enden Parameter ein und stellen Sie dann eine Verbindung mit der Quelle und dem Ziel her.	Developer
Generieren Sie einen Schemakonvertierungsbericht.	Generieren Sie einen AWS SCT-Schemakonverti erungsbericht.	Developer
Korrigieren Sie den Code und das Schema nach Bedarf.	Nehmen Sie alle erforderl ichen Korrekturen am Code und Schema vor (insbeson dere Tabellenräume und Anführungszeichen).	DBA, Entwickler
Validieren Sie das Schema.	Validieren Sie das Schema für die Quelle im Vergleich zum Ziel, bevor Sie Daten laden.	Developer

Migrieren von Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie ein Verbindungsattribut fest.	Legen Sie für vollständiges Laden und Change Data Capture (CDC) oder nur für CDC ein zusätzliches Verbindungsattribut fest. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	Developer
Aktivieren Sie die zusätzliche Protokollierung.	Aktivieren Sie die zusätzliche Protokollierung für die Quelldatenbank.	DBA, Entwickler
Aktivieren Sie den Archivprotokollmodus.	Aktivieren Sie für Volllast und CDC (oder nur für CDC) den Archivprotokollmodus in der Quelldatenbank.	DBA
Erstellen und testen Sie Endpunkte.	Erstellen Sie Quell- und Zielendpunkte und testen Sie die Verbindungen. Weitere Informationen finden Sie in der Amazon-DMS-Dokumentation.	Developer
Erstellen Sie eine Replikationsaufgabe.	Wenn die Endpunkte erfolgreich verbunden sind, erstellen Sie eine Replikationsaufgabe. Weitere Informationen finden Sie in der Amazon-DMS-Dokumentation.	Developer
Wählen Sie Replikationstyp aus.	Wählen Sie in der Aufgabe Nur CDC oder Volllast plus CDC aus, um Änderungen nur	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für die kontinuierliche Replikation bzw. für vollständige bzw. fortlaufende Änderungen zu erfassen.	
Starten und überwachen Sie die Aufgabe.	Starten Sie die Replikationsaufgabe und überwachen Sie Amazon- CloudWatch Protokolle. Weitere Informationen finden Sie in der Amazon-DMS-Dokumentation.	Developer
Validieren Sie die Daten.	Validieren Sie die Daten in den Quell- und Zieldatenbanken.	Developer

Migrieren von Anwendungen und Umstellung auf die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewählten Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Entwickler
Folgen Sie der ausgewählten Strategie für Anwendungs-Cutover/-Umschaltung.		DBA, App-Besitzer, Entwickler

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie das Schema und die Daten.	Stellen Sie sicher, dass das Schema und die Daten vor dem Schließen des Projekts	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erfolgreich in der Quelle im Vergleich zum Ziel validiert werden.	
Erfassen Sie Metriken.	Erfassen Sie Metriken für die Zeit bis zur Migration, den Prozentsatz manueller Aufgaben im Vergleich zu Tool-Aufgaben, Kostenein sparungen und ähnliche Kriterien.	DBA, App-Besitzer, Entwickler
Überprüfen Sie die Dokumentation.	Überprüfen Sie die Projektdo kumente und Artefakte.	DBA, App-Besitzer, Entwickler
Fahren Sie Ressourcen herunter.	Fahren Sie temporäre AWS-Ressourcen herunter.	DBA, Entwickler
Schließen Sie das Projekt.	Schließen Sie das Migration sprojekt und geben Sie Feedback.	DBA, App-Besitzer, Entwickler

Zugehörige Ressourcen

- Übersicht über MariaDB Amazon RDS
- Produktdetails zu Amazon RDS for MariaDB
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Strategien für die Migration von Oracle-Datenbanken zu AWS
- Lizenzierung von Oracle-Software in der Cloud Computing-Umgebung
- Häufig FAQs zu Amazon RDS für Oracle
- AWS DMS-Übersicht
- AWS DMS-Blogbeiträge
- Übersicht über Amazon EC2
- Häufig FAQs zu Amazon EC2

- AWS SCT-Dokumentation

Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL

R-Typ: Re-Architect	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for MySQL
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: Oracle	AWS-Dienste: Amazon RDS	

Übersicht

Dieses Muster führt Sie durch die Migration einer lokalen Oracle-Datenbank zu einer Amazon Relational Database Service (Amazon RDS) für MySQL-DB-Instance. Es verwendet AWS Database Migration Service (AWS DMS), um die Daten zu migrieren, und das AWS Schema Conversion Tool (AWS SCT), um das Quelldatenbankschema und die Objekte in ein Format zu konvertieren, das mit Amazon RDS for MySQL kompatibel ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Alle Oracle-Datenbankeditionen für die Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Using an Oracle Database as a Source for AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.

Informationen zu den von AWS SCT unterstützten Oracle-Datenbankversionen finden Sie in der AWS SCT-Dokumentation.

- AWS DMS unterstützt derzeit die MySQL-Versionen 5.5, 5.6 und 5.7. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS-Dokumentation unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS.

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbank

Zieltechnologie-Stack

- Amazon RDS for MySQL MySQL-DB-Instance

Architektur der Datenmigration

Tools

- AWS DMS — AWS Database Migration Services (AWS DMS) unterstützt Sie bei der Migration von relationalen Datenbanken, Data Warehouses, NoSQL-Datenbanken und anderen Arten von Datenspeichern. Sie können AWS DMS verwenden, um Ihre Daten in die AWS Cloud, zwischen lokalen Instances (über eine AWS Cloud-Einrichtung) oder zwischen Kombinationen aus Cloud und lokalen Einrichtungen zu migrieren.
- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) wird verwendet, um Ihr Datenbankschema von einer Datenbank-Engine in eine andere zu konvertieren. Der benutzerdefinierte Code, den das Tool konvertiert, umfasst Ansichten, gespeicherte Prozeduren und Funktionen. Jeder Code, den das Tool nicht automatisch konvertieren kann, ist deutlich gekennzeichnet, sodass Sie ihn selbst konvertieren können.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie die Sicherheitsgruppen und Network Access Control Lists (ACLs).		SysAdmin
Konfigurieren und starten Sie eine Amazon RDS-DB-Instance.		DBA, SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie das Datenbankschema mithilfe von AWS SCT.		DBA
Migrieren Sie Daten mithilfe von AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS SCT, um den SQL-Code im Anwendungscode zu analysieren und zu konvertieren.	Weitere Informationen finden Sie unter https://docs.aws.amazon.com/ SchemaConversion tool/latest/UserGuide/chap_Converting.app.html.	Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Daten im Vergleich zu Tools, zu Kosteneinsparungen usw.		DBA, SysAdmin
Schließen Sie das Projekt ab und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Amazon RDS — Preisgestaltung

Tutorial und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS DMS (Video)
- Amazon RDS (Video)

Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe eines Oracle-Bystanders und AWS DMS

Erstellt von Cady Motyka (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS für PostgreSQL/Amazon Aurora PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster beschreibt, wie Sie eine lokale Oracle-Datenbank mit minimalen Ausfallzeiten zu einem der folgenden mit PostgreSQL kompatiblen AWS-Datenbankservices migrieren können:

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

Die Lösung verwendet AWS Database Migration Service (AWS DMS), um die Daten zu migrieren, AWS Schema Conversion Tool (AWS SCT), um das Datenbankschema zu konvertieren, und eine Oracle-Bystander-Datenbank, um die Migration zu verwalten. In dieser Implementierung ist die Ausfallzeit auf die Dauer beschränkt, die benötigt wird, um alle Fremdschlüssel in der Datenbank zu erstellen oder zu validieren.

Die Lösung verwendet auch Amazon Elastic Compute Cloud (Amazon EC2)-Instances mit einer Oracle-Bystander-Datenbank, um den Datenstrom über AWS DMS zu steuern. Sie können die Streaming-Replikation von der On-Premises-Oracle-Datenbank zum Oracle-Bystander vorübergehend anhalten, um AWS DMS zu aktivieren, um die Datenvalidierung aufrechtzuerhalten oder ein anderes Datenvalidierungstool zu verwenden. Die Amazon RDS for PostgreSQL-DB-Instance oder Aurora PostgreSQL -kompatible DB-Instance und die Bystander-Datenbank haben dieselben Daten, wenn AWS DMS die Migration aktueller Änderungen abgeschlossen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem On-Premises-Rechenzentrum mit konfigurierter Active Data Guard-Standby-Datenbank
- AWS Direct Connect, konfiguriert zwischen dem On-Premises-Rechenzentrum und AWS Secrets Manager zum Speichern der Datenbank-Secrets
- Java Database Connectivity (JDBC)-Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder auf der EC2-Instance installiert sind, auf der AWS SCT installiert ist
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als Ziel für AWS DMS

Einschränkungen

- Datenbankgrößenbeschränkung: 64 TB

Produktversionen

- AWS DMS unterstützt alle Oracle-Datenbank-Editionen für die Versionen 10.2 und höher (für die Versionen 10.x), 11g und bis zu 12.2, 18c und 19c. Die neueste Liste der unterstützten Versionen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden. Informationen zu Oracle-Datenbankversionen, die von AWS SCT unterstützt werden, finden Sie in der AWS SCT-Dokumentation.
- AWS DMS unterstützt die PostgreSQL-Versionen 9.4 und höher (für die Versionen 9.x), 10.x, 11.x, 12.x und 13.x. Die neuesten Informationen finden Sie unterVerwenden einer PostgreSQL-Datenbank als Ziel für AWS DMSin der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Oracle-Datenbank
- Eine EC2-Instance, die einen Bystander für die Oracle-Datenbank enthält

Zieltechnologie-Stack

- Amazon-RDS-for-PostgreSQL- oder Aurora-PostgreSQL-Instance, PostgreSQL 9.3 und höher

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Migration einer Oracle-Datenbank zu einer PostgreSQL-kompatiblen AWS-Datenbank mithilfe von AWS DMS und einem Oracle-Bystander:

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.

Polen

Konvertieren des Oracle-Datenbankschemas in PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Erstellen Sie einen neuen Bericht und stellen Sie eine Verbindung zu Oracle als Quelle und PostgreSQL als Ziel her. Gehen Sie unter Projekteinstellungen zur Registerkarte SQL-Skrip terstellung. Ändern Sie das Ziel-SQL-Skript in mehrere	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dateien. Diese Dateien werden später verwendet und wie folgt benannt: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	
Konvertieren Sie das Oracle-Datenbankschema.	Wählen Sie auf der Registerkarte Aktion die Option Bericht generieren aus. Wählen Sie dann Schema konvertieren und dann Als SQL speichern aus.	DBA
Ändern Sie die Skripts.	Sie können das Skript beispielsweise ändern, wenn eine Zahl im Quellschema in PostgreSQL in ein numerisches Format konvertiert wurde, Sie aber stattdessen BIGINT für eine bessere Leistung verwenden möchten.	DBA

Erstellen und Konfigurieren der Amazon RDS-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-DB-Instance.	Erstellen Sie in der richtigen AWS-Region eine neue PostgreSQL-DB-Instance. Weitere Informationen finden	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie unter Erstellen einer PostgreSQL-DB-Instance und Herstellen einer Verbindung mit einer Datenbank auf einer PostgreSQL-DB-Instance in der Amazon-RDS-Dokumentation.	
Konfigurieren Sie DB-Instance-Spezifikationen.	Geben Sie die DB-Engine-Version, die DB-Instance-Klasse, die Multi-AZ-Bereitstellung, den Speichertyp und den zugewiesenen Speicher an. Geben Sie die DB-Instance-Kennung, einen primären Benutzernamen und ein primäres Passwort ein.	AWS SysAdmin, DBA
Konfigurieren Sie Netzwerk und Sicherheit.	Geben Sie die Virtual Private Cloud (VPC), die Subnetzgruppe, die öffentliche Zugänglichkeit, die Availability-Zone-Präferenz und die Sicherheitsgruppen an.	DBA, SysAdmin
Konfigurieren Sie Datenbankoptionen.	Geben Sie den Datenbanknamen, den Port, die Parametergruppe, die Verschlüsselung und den KMS-Schlüssel an.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Sicherungen.	Geben Sie den Aufbewahrungszeitraum für Backups, das Backup-Fenster, die Startzeit, die Dauer und die Frage an, ob Tags in Snapshots kopiert werden sollen.	AWS SysAdmin, DBA
Konfigurieren Sie Überwachungsoptionen.	Aktivieren oder deaktivieren Sie erweiterte Überwachung und Leistungseinblicke.	AWS SysAdmin, DBA
Konfigurieren Sie die Wartungsoptionen.	Geben Sie das automatische Upgrade der Nebenversion, das Wartungsfenster und den Starttag, die Uhrzeit und die Dauer an.	AWS SysAdmin, DBA
Führen Sie die Vormigrationsskripts von AWS SCT aus.	Führen Sie auf der Amazon RDS-Instance die folgenden von AWS SCT generierten Skripts aus: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	AWS SysAdmin, DBA

Konfigurieren des Oracle-Bystanders in Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Netzwerk für Amazon EC2 ein.	Erstellen Sie die neue VPC, Subnetze, das Internet-Gateway, Routing-Tabellen und Sicherheitsgruppen.	AWS SysAdmin
Erstellen Sie die EC2-Instance.	Erstellen Sie in der entsprechenden AWS-Region eine neue EC2-Instance. Wählen Sie das Amazon Machine Image (AMI), wählen Sie die Instance-Größe aus und konfigurieren Sie Instance-Details: Anzahl der Instances (1), die VPC und das Subnetz, die Sie in der vorherigen Aufgabe erstellt haben, weisen Sie öffentliche IP und andere Optionen automatisch zu. Fügen Sie Speicher hinzu, konfigurieren Sie Sicherheitsgruppen und starten Sie sie. Wenn Sie dazu aufgefordert werden, erstellen und speichern Sie ein Schlüsselpaar für den nächsten Schritt.	AWS SysAdmin
Verbinden Sie die Oracle-Quelldatenbank mit der EC2-Instance.	Kopieren Sie die öffentliche IPv4-IP-Adresse und das DNS in eine Textdatei und stellen Sie eine Verbindung mithilfe von SSH wie folgt her: ssh -i "your_file.pem" ec2-user@	AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<your-IP--address-or-public-DNS>.	
Richten Sie den anfänglichen Host für einen Bystander in Amazon EC2 ein.	Richten Sie SSH-Schlüssel, Bash-Profil, ORATAB und symbolische Links ein. Erstellen Sie Oracle-Verzeichnisse.	AWS SysAdmin, Linux-Admin
Einrichten der Datenbankkopie für einen Bystander in Amazon EC2	Verwenden Sie RMAN, um eine Datenbankkopie zu erstellen, die zusätzliche Protokollierung zu aktivieren und die Standby-Steuerungsdatei zu erstellen. Nachdem das Kopieren abgeschlossen ist, versetzen Sie die Datenbank in den Wiederherstellungsmodus.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Oracle Data Guard ein.	Ändern Sie Ihre Datei listener.ora und starten Sie den Listener. Richten Sie ein neues Archivzie l ein. Platzieren Sie den Bystander im Wiederher stellungsmodus, ersetzen Sie temporäre Dateien, um zukünftige Beschädigungen zu vermeiden, installieren Sie bei Bedarf eine Crontab, um zu verhindern, dass dem Archivverzeichnis der Speicherplatz ausgeht, und bearbeiten Sie die manage-tr clog-files-oracle.cfg-Datei für die Quelle und den Standby-M odus.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Oracle-Datenbank für die Synchronisierung des Versands vor.	Fügen Sie die Standby-Protokolldateien hinzu und ändern Sie den Wiederherstellungsmodus. Ändern Sie den Versand von Protokollen in SYNC AFFIRM sowohl auf der primären Quelle als auch auf der Standby-Quelle. Wechseln Sie die Protokolle auf der primären Instance, bestätigen Sie über das Amazon EC2-Bystander-Warnprotokoll, dass Sie die Standby-Protokolldateien verwenden, und vergewissern Sie sich, dass der Redo-Stream in SYNC fließt.	AWS SysAdmin, DBA

Migrieren von Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikations-Instance in AWS DMS.	Füllen Sie die Felder für den Namen, die Instance-Klasse, die VPC (wie die Amazon EC2-Instance), Multi-AZ und den öffentlichen Zugriff aus. Geben Sie unter Advance den zugewiesenen Speicher, die Subnetzgruppe, die Availability Zone, die VPC-Sicherheitsgruppen und den AWS Key Management Service (AWS KMS)-Schlüssel an.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Endpunkt der Quelldatenbank.	Geben Sie den Endpunktn amen, den Typ, die Quell-Eng ine (Oracle), den Servernam en (Amazon EC2-DNS-N amen), den Port, den SSL-Modus, den Benutzernamen, das Passwort, die SID, die VPC (geben Sie die VPC an, die über die Replikations-Instance verfügt) und die Replikations-Instance an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDat aTypeSkalieren von .	AWS SysAdmin, DBA
Verbinden Sie AWS DMS mit Amazon RDS for PostgreSQ L .	Erstellen Sie eine Migration ssicherheitsgruppe für Verbindungen zwischen VPCs.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Zieldaten bank-Endpunkt.	Geben Sie den Endpunktn amen, den Typ, die Quell-Engine (PostgreSQL), den Servernamen (Amazon-RDS-Endpunkt), den Port, den SSL-Modus, den Benutzernamen, das Passwort, den Datenbank namen, die VPC (geben Sie die VPC an, die die Replikati ons-Instance enthält) und die Replikations-Instance an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDat aTypeSkalieren.	AWS SysAdmin, DBA
Erstellen Sie die AWS DMS-Replikationsaufgabe.	Geben Sie den Aufgabenn amen, die Replikations-Insta nce, die Quell- und Zielendpu nkte sowie die Replikations-Instance an. Wählen Sie für Migrationstyp die Option Vorhandene Daten migrieren und laufende Änderungen replizieren aus. Deaktivie ren Sie das Kontrollkästchen Aufgabe beim Erstellen starten.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS DMS-Replikationsaufgabeneinstellungen.	Wählen Sie für den Vorbereitungsmodus der Zieltabelle die Option Nichts tun aus. Beenden Sie die Aufgabe nach Abschluss des vollständigen Ladevorgangs (um Primärschlüssel zu erstellen). Geben Sie den eingeschränkten oder vollständigen LOB-Modus an und aktivieren Sie die Steuertabellen. Optional können Sie die CommitRate Voreinstellungen konfigurieren.	DBA
Konfigurieren Sie Tabellenzuordnungen.	Erstellen Sie im Abschnitt Tabellenzuordnungen eine Einschließen-Regel für alle Tabellen in allen Schemata, die in der Migration enthalten sind, und erstellen Sie dann eine Ausschließen-Regel. Fügen Sie drei Transformationsregeln hinzu, um Schema-, Tabellen- und Spaltennamen in Kleinbuchstaben zu konvertieren, und fügen Sie alle anderen Regeln hinzu, die für diese spezifische Migration erforderlich sind.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe.	Starten Sie die Replikati onsaufgabe. Stellen Sie sicher, dass der volle Ladevorgang ausgeführ t wird. Führen Sie ALTER SYSTEM SWITCH LOGFILE in der primären Oracle-Da tenbank aus, um die Aufgabe zu starten.	DBA
Führen Sie die Skripts zur mittleren Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden von AWS SCT generierten Skripts aus: • create_index.sql • create_constraint.sql	DBA
Starten Sie die Aufgabe neu, um die Erfassung von Datenänderungen (Change Data Capture, CDC) fortzuset zen.	Führen Sie VACUUM auf der Amazon RDS for PostgreSQ L-DB-Instance aus und starten Sie die AWS DMS-Aufgabe neu, um zwischeng espeicherte CDC-Änderungen anzuwenden.	DBA

Umstellung auf die PostgreSQL-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS DMS-Protokolle und Validieru ngstabellen auf Fehler.	Überprüfen und beheben Sie Replikations- oder Validieru ngsfehler.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie alle Oracle-Abhängigkeiten an.	Halten Sie alle Oracle-Abhängigkeiten an, fahren Sie Listener in der Oracle-Datenbank herunter und führen Sie ALTER SYSTEM SWITCH LOGFILE aus. Halten Sie die AWS DMS-Aufgabe an, wenn sie keine Aktivität anzeigt.	DBA
Führen Sie die Skripts nach der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden von AWS SCT generierten Skripts aus: • create_foreign_key_constraint.sql • create_triggers.sql	DBA
Führen Sie zusätzliche Schritte von Amazon RDS für PostgreSQL aus.	Inkrementelle Sequenzen, die bei Bedarf mit Oracle übereinstimmen, führen VACUUM und ANALYZE aus und erstellen einen Snapshot, um die Compliance zu gewährleisten.	DBA
Öffnen Sie die Verbindungen zu Amazon RDS for PostgreSQL .	Entfernen Sie die AWS DMS-Sicherheitsgruppen aus Amazon RDS for PostgreSQL, fügen Sie Produktionssicherheitsgruppen hinzu und verweisen Sie Ihre Anwendungen auf die neue Datenbank.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie AWS DMS-Objekte.	Entfernen Sie die Endpunkte , Replikationsaufgaben, Replikations-Instances und die EC2-Instance.	SysAdmin, DBA

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Amazon RDS für PostgreSQL – Preise

Migrieren von Oracle Database zu Amazon RDS for PostgreSQL mithilfe von Oracle GoldenGate

Erstellt von Dhairya Jindani (AWS), Rajeshkumar Sabankar (AWS) und Sindhusha Paturu (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS für PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster zeigt, wie eine Oracle-Datenbank mithilfe der Oracle Cloud Infrastructure (OCI) zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL migriert wird GoldenGate.

Mit Oracle können GoldenGateSie Daten zwischen Ihrer Quelldatenbank und einer oder mehreren Zieldatenbanken mit minimalen Ausfallzeiten replizieren.

Hinweis: Die Oracle-Quelldatenbank kann entweder On-Premises oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance sein. Sie können ein ähnliches Verfahren verwenden, wenn Sie On-Premises-Replikationstools verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle- GoldenGate Lizenz
- Java Database Connectivity (JDBC)-Treiber zum Herstellen einer Verbindung mit der PostgreSQL-Datenbank
- Schema und Tabellen, die mit dem AWS Schema Conversion Tool (AWS SCT) in der Amazon RDS for PostgreSQL-Zieldatenbank erstellt wurden

Einschränkungen

- Oracle GoldenGate kann vorhandene Tabellendaten (anfängliches Laden) und laufende Änderungen (Erfassung von Änderungsdaten) nur replizieren

Produktversionen

- Oracle Database Enterprise Edition 10g oder neuere Versionen
- Oracle GoldenGate12.2.0.1.1 für Oracle oder neuere Versionen
- Oracle GoldenGate12.2.0.1.1 für PostgreSQL oder neuere Versionen

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Migration einer Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe von Oracle GoldenGate:

Das Diagramm zeigt den folgenden Workflow:

1. Der Oracle GoldenGate Extract-Prozess wird für die Quelldatenbank ausgeführt, um Daten zu extrahieren.
2. Der Oracle GoldenGate Replicat-Prozess liefert die extrahierten Daten an die Amazon RDS for PostgreSQL-Zieldatenbank.

Tools

- Oracle GoldenGate unterstützt Sie beim Entwerfen, Ausführen, Orchestrieren und Überwachen Ihrer Datenreplikations- und Stream-Datenverarbeitungslösungen in der Oracle Cloud Infrastructure.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.

Polen

Oracle herunterladen und installieren GoldenGate

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Oracle herunter GoldenGate.	Laden Sie die folgenden Versionen von Oracle herunter GoldenGate: • Oracle GoldenGate12.2.0.1 .1 für Oracle oder eine neuere Version • Oracle GoldenGate12.2.0.1 .1 für PostgreSQL oder eine neuere Version Informationen zum Herunterl aden der Software finden Sie unter Oracle GoldenGate Downloads auf der Oracle-We bsite.	DBA
Installieren Sie Oracle GoldenGate für Oracle auf dem Oracle-Datenbank-Q uellserver.	Anweisungen finden Sie in der Oracle- GoldenGate Dokumentation.	DBA
Installieren Sie die Oracle GoldenGate for PostgreSQL-Datenbank auf der Amazon EC2-Instance.	Anweisungen finden Sie in der Oracle- GoldenGate Dokumentation.	DBA

Konfigurieren von Oracle GoldenGate für die Quell- und Zieldatenbanken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Oracle GoldenGate für Oracle Database in der Quelldatenbank ein.	Anweisungen finden Sie in der Oracle- GoldenGate Dokumentation. Stellen Sie sicher, dass Sie Folgendes konfigurieren: • Zusätzliche Protokollierung • Oracle- GoldenGate Benutzer • Alle erforderlichen Erteilungen und Berechtigungen • Parameterdateien • Manager-Prozess • Verzeichnis • GLOBALS-Dateien • Oracle Wallet	DBA
Richten Sie Oracle GoldenGate für PostgreSQL in der Zieldatenbank ein.	Anweisungen finden Sie unter Teil VI mit Oracle GoldenGate für PostgreSQL auf der Oracle-Website. Stellen Sie sicher, dass Sie Folgendes konfigurieren: • Manager-Prozess • GLOBALS-Dateien • Oracle Wallet	DBA

Konfigurieren der Datenerfassung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Prozess Extract in der Quelldatenbank ein.	Erstellen Sie in der Oracle-Quelldatenbank eine -Extraktionsdatei, um Daten zu extrahieren. Anweisungen finden Sie unter ADD EXTRACT in der Oracle-Dokumentation. Hinweis: Die Extract-Datei beinhaltet die Erstellung der Extract-Parameterdatei und des Trail-Dateiverzeichnisses.	DBA
Richten Sie einen Datenstrom ein, um die Trail-Datei von der Quelle in die Zieldatenbank zu übertragen.	Erstellen Sie eine EXTRACT-Parameterdatei und ein Trail-Dateiverzeichnis, indem Sie den Anweisungen unter PARFILE in Database Utilities auf der Oracle-Website folgen. Weitere Informationen finden Sie unter Was ist ein Trail? in Fusion Middleware Understanding Oracle GoldenGate auf der Oracle-Website.	DBA
Richten Sie die Replikation auf der Amazon EC2 ein.	Erstellen Sie eine Replikationsparameterdatei und ein Trail-Dateiverzeichnis. Weitere Informationen zum Erstellen von Replikationsparameterdateien finden Sie in Abschnitt 3.5 Validiere	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n einer Parameterdatei in der Oracle Database-Dokumentation. Weitere Informationen zum Erstellen eines Trail-Dateiverzeichnisses finden Sie unter Erstellen eines Trails in der Oracle Cloud-Dokumentation. Wichtig: Stellen Sie sicher, dass Sie einen Checkpoint-Tabelleneintrag in der Datei GLOBALS am Ziel hinzufügen. Weitere Informationen finden Sie unter Was ist ein Replikat? in Fusion Middleware Understanding Oracle GoldenGate auf der Oracle-Website.	

Konfigurieren der Datenreplikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie in der Quelldatenbank eine Parameterdatei, um Daten für den ersten Ladevorgang zu extrahieren.	Folgen Sie den Anweisungen unter Erstellen einer Parameterdatei in GGSCI in der Oracle Cloud-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Stellen Sie sicher, dass der Manager auf dem Ziel ausgeführt wird.	
Erstellen Sie in der Zieldaten bank eine Parameterdatei, um Daten für den ersten Ladevorgang zu replizieren.	Folgen Sie den Anweisung en unter Erstellen einer Parameterdatei in GGSCI in der Oracle Cloud-Dok umentation. Wichtig: Stellen Sie sicher, dass Sie den Replikat-Prozess hinzufügen und starten.	DBA

Umstellung auf die Datenbank von Amazon RDS für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie den Replikat-Prozess und stellen Sie sicher, dass die Quell- und Zieldaten banken synchron sind.	Vergleichen Sie die Zeilenanz ahl zwischen der Quell- und der Zieldatenbank, um sicherzustellen, dass die Datenreplikation erfolgreich war.	DBA
Konfigurieren Sie die Unterstüt zung von Data Definition Language (DDL).	Führen Sie das DDL-Skript zum Erstellen von Auslösern, Sequenzen, Synonymen und referenziellen Schlüsseln auf PostgreSQL aus. Hinweis: Sie können jede Standard-SQL-Clien tanwendung verwenden , um eine Verbindung zu einer Datenbank in Ihrem	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DB-Cluster herzustellen. Sie können beispielsweise pgAdmin verwenden, um eine Verbindung zu Ihrer DB-Instan ce herzustellen.	

Zugehörige Ressourcen

- Amazon RDS für PostgreSQL (Amazon-RDS-Benutzerhandbuch)
- Amazon EC2-Dokumentation
- Von Oracle GoldenGate unterstützte Verarbeitungsmethoden und Datenbanken (Oracle-Dokumentation)

Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift

Quelle: Oracle	Ziel: Redshift	R-Typ: Re-Architect
Umgebung: Produktion	Technologien: Migration; Analytik; Datenbanken	Arbeitslast: Oracle
AWS-Dienste: Amazon Redshift; AWS DMS		

Übersicht

Dieses Muster bietet Anleitungen für die Migration von Oracle-Datenbanken zu einem Amazon Redshift Cloud Data Warehouse in der Amazon Web Services (AWS) -Cloud mithilfe von AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT). Das Muster deckt Oracle-Quelldatenbanken ab, die lokal installiert oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance installiert sind. Es behandelt auch Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Datenbank, die in einem lokalen Rechenzentrum oder in der AWS-Cloud läuft
- Ein aktives AWS-Konto
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer Amazon Redshift Redshift-Datenbank als Ziel für AWS DMS
- Kenntnisse über Amazon RDS, Amazon Redshift, die anwendbaren Datenbanktechnologien und SQL
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Konnektoren, auf denen AWS SCT installiert ist

Produktversionen

- Für selbstverwaltete Oracle-Datenbanken unterstützt AWS DMS alle Oracle-Datenbankeditionen für Versionen 10.2 und höher (für Versionen 10. x), 11g und bis zu 12.2, 18c und 19c. Für Amazon RDS for Oracle Oracle-Datenbanken, die AWS verwaltet, unterstützt AWS DMS alle Oracle-Datenbankeditionen für die Versionen 11g (Versionen 11.2.0.4 und höher) und bis zu 12.2, 18c und 19c. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Oracle-Datenbank
- Eine Oracle-Datenbank auf einer EC2-Instance
- Eine Amazon RDS for Oracle Oracle-DB-Instance

Zieltechnologie-Stack

- Amazon-Redshift

Zielarchitektur

Von einer Oracle-Datenbank, die in der AWS-Cloud läuft, zu Amazon Redshift:

Von einer Oracle-Datenbank, die in einem lokalen Rechenzentrum läuft, zu Amazon Redshift:

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) hilft Ihnen, Datenbanken schnell und sicher zu AWS zu migrieren. Die Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch Ausfallzeiten für Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren.

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) kann verwendet werden, um Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere zu konvertieren. Es unterstützt verschiedene Datenbank-Engines, darunter Oracle, SQL Server und PostgresSQL, als Quellen.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenbank versionen.	Überprüfen Sie die Quell- und Zieldatenbankversionen und stellen Sie sicher, dass sie von AWS DMS unterstützt werden. Informationen zu unterstützten Oracle-Datenbankversionen finden Sie unter Eine Oracle-Datenbank als Quelle für AWS DMS verwenden. Informationen zur Verwendung von Amazon Redshift als Ziel finden Sie unter Verwenden einer Amazon Redshift Redshift-Datenbank als Ziel für AWS DMS.	DBA
Erstellen Sie eine VPC und eine Sicherheitsgruppe.	Erstellen Sie in Ihrem AWS-Konto eine Virtual Private Cloud (VPC), falls diese nicht existiert. Erstellen Sie eine Sicherheitsgruppe für ausgehenden Datenverkehr zu Quell- und Zieldatenbanken. Weitere Informationen finden Sie in der Dokumentation zu	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Virtual Private Cloud (Amazon VPC).	
Installieren Sie AWS SCT.	Laden Sie die neueste Version von AWS SCT und die entsprechenden Treiber herunter und installieren Sie sie. Weitere Informationen finden Sie unter Installation, Überprüfung und Aktualisierung des AWS SCT.	DBA
Erstellen Sie einen Benutzer für die AWS DMS-Aufgabe.	Erstellen Sie einen AWS DMS-Benutzer in der Quelldatenbank und gewähren Sie ihm READ-Rechte. Dieser Benutzer wird sowohl von AWS SCT als auch von AWS DMS verwendet.	DBA
Testen Sie die DB-Konnektivität.	Testen Sie die Konnektivität zur Oracle-DB-Instance.	DBA
Erstellen Sie ein neues Projekt in AWS-SCT.	Öffnen Sie das AWS SCT-Tool und erstellen Sie ein neues Projekt.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie das zu migrierende Oracle-Schema.	Verwenden Sie AWS SCT, um das zu migrierende Schema zu analysieren und einen Bewertungsbericht zur Datenbankmigration zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Bewertungsberichts zur Datenbankmigration in der AWS SCT-Dokumentation.	DBA
Überprüfen Sie den Bewertungsbericht.	Überprüfen Sie den Bericht auf die Durchführbarkeit der Migration. Einige DB-Objekte müssen möglicherweise manuell konvertiert werden. Weitere Informationen zum Bericht finden Sie unter Bewertungsbericht anzeigen in der AWS SCT-Dokumentation.	DBA

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon Redshift Redshift-Cluster.	Erstellen Sie einen Amazon Redshift Redshift-Cluster in der VPC, die Sie zuvor erstellt haben. Weitere Informationen finden Sie unter Amazon Redshift Redshift-Cluster in der Amazon Redshift Redshift-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Datenbankbenutzer erstellen.	Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Oracle-Quelldatenbank. Erstellen Sie Benutzer in der Amazon Redshift Redshift-Zieldatenbank und wenden Sie die Rollen aus dem vorherigen Schritt an.	DBA
Evaluieren Sie Datenbank parameter.	Überprüfen Sie die Datenbank optionen, Parameter , Netzwerkdateien und Datenbank-Links aus der Oracle-Quelldatenbank und bewerten Sie deren Anwendbarkeit auf das Ziel.	DBA
Wenden Sie alle relevanten Einstellungen auf das Ziel an.	Weitere Informationen zu diesem Schritt finden Sie unter Konfigurationsreferenz in der Amazon Redshift Redshift-Dokumentation.	DBA

Objekte in der Zieldatenbank erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS DMS-Benutzer in der Zieldatenbank.	Erstellen Sie einen AWS DMS-Benutzer in der Zieldatenbank und gewähren Sie ihm Lese- und Schreibbe rechtigungen. Überprüfen Sie	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Konnektivität von AWS SCT.	
Konvertieren Sie das Schema, überprüfen Sie den SQL-Bericht und speichern Sie alle Fehler oder Warnungen.	Weitere Informationen finden Sie unter Konvertieren von Datenbankschemas mithilfe von AWS SCT in der AWS SCT-Dokumentation.	DBA
Wenden Sie die Schemaänd erungen auf die Zieldaten bank an oder speichern Sie sie als.sql-Datei.	Anweisungen finden Sie unter Speichern und Anwenden Ihres konvertierten Schemas im AWS SCT in der AWS SCT-Dokumentation.	DBA
Validieren Sie die Objekte in der Zieldatenbank.	Validieren Sie die Objekte, die im vorherigen Schritt in der Zieldatenbank erstellt wurden. Schreiben Sie alle Objekte, die nicht erfolgreich konvertie rt wurden, neu oder entwerfen Sie sie neu.	DBA
Deaktivieren Sie Fremdschl üssel und Trigger.	Deaktivieren Sie alle Fremdschlüssel und Trigger. Diese können zu Problemen beim Laden von Daten während des Vollladevorgangs führen, wenn AWS DMS ausgeführt wird.	DBA

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS DMS-Konsole. Wählen Sie im Navigationsbereich Replikationsinstanzen, Replikationsinstanz erstellen aus. Eine ausführliche Anleitung finden Sie in Schritt 1 unter Erste Schritte mit AWS DMS in der AWS DMS-Dokumentation.	DBA
Erstellen Sie Quell- und Zielendpunkte.	Erstellen Sie Quell- und Zielendpunkte und testen Sie die Verbindung zwischen der Replikationsinstanz und den Quell- und Zielendpunkten. Eine ausführliche Anleitung finden Sie in Schritt 2 unter Erste Schritte mit AWS DMS in der AWS DMS-Dokumentation.	DBA
Erstellen Sie eine Replikationsaufgabe.	Erstellen Sie eine Replikationsaufgabe und wählen Sie die entsprechende Migrationsmethode aus. Eine ausführliche Anleitung finden Sie in Schritt 3 unter Erste Schritte mit AWS DMS in der AWS DMS-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Datenrepl ikation.	Starten Sie die Replikati onsaufgabe und überwachen Sie die Protokolle auf Fehler.	DBA

Migrieren Sie Ihre Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Anwendungsserver erstellen.	Erstellen Sie die neuen Anwendungsserver auf AWS.	Besitzer der Anwendung
Migrieren Sie den Anwendung scode.	Migrieren Sie den Anwendung scode auf die neuen Server.	Besitzer der Anwendung
Konfigurieren Sie den Anwendungsserver.	Konfigurieren Sie den Anwendungsserver für die Zieldatenbank und die Treiber.	Besitzer der Anwendung
Optimieren Sie den Anwendungscode.	Optimieren Sie den Anwendungscode für die Ziel-Engine.	Besitzer der Anwendung

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Benutzer validieren.	Validieren Sie Benutzer in der Amazon Redshift Redshift-Zieldatenbank und gewähren Sie ihnen Rollen und Rechte.	DBA
Stellen Sie sicher, dass die Anwendung gesperrt ist.	Stellen Sie sicher, dass die Anwendung gesperrt ist,	Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um weitere Änderungen zu verhindern.	
Validieren Sie die Daten.	Überprüfen Sie die Daten in der Amazon Redshift Redshift-Zieldatenbank.	DBA
Aktivieren Sie Fremdschlüssel und Trigger.	Aktivieren Sie Fremdschlüssel und Trigger in der Amazon Redshift Redshift-Zieldaten bank.	DBA
Connect der neuen Datenbank her.	Konfigurieren Sie die Anwendung für die Verbindun g mit der neuen Amazon Redshift Redshift-Datenbank.	Besitzer der Anwendung
Führen Sie die letzten Prüfungen durch.	Führen Sie vor der Inbetrieb nahme eine letzte, umfassend e Systemüberprüfung durch.	DBA, Besitzer der Anwendung
Geh live.	Gehen Sie mit der Amazon Redshift Redshift-Zieldaten bank live.	DBA

Schließen Sie das Migrationsprojekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.	Fahren Sie temporäre AWS-Ressourcen wie die AWS DMS-Replikationsinstanz und die für AWS SCT verwendete EC2-Instance herunter.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumente überprüfen.	Überprüfen und validieren Sie die Dokumente des Migration sprojekts.	DBA, Systemadministrator
Sammeln Sie Metriken.	Sammeln Sie Informationen über das Migrationsprojekt, z. B. die Zeit für die Migration , den Prozentsatz manueller Aufgaben im Vergleich zu den Toolaufgaben und die Gesamtkosteneinsparungen.	DBA, Systemadministrator
Schließt das Projekt ab.	Schließen Sie das Projekt ab und geben Sie Feedback.	DBA, Systemadministrator

Zugehörige Ressourcen

Referenzen

- AWS DMS-Benutzerhandbuch
- AWS SCT-Benutzerhandbuch
- Leitfaden „Erste Schritte“ mit Amazon Redshift

Tutorials und Videos

- Tauchen Sie tief in AWS SCT und AWS DMS ein (Präsentation von AWS re:Invent 2019)
- Erste Schritte mit dem AWS Database Migration Service

Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mit AWS DMS und AWS SCT

Erstellt von Senthil Ramasamy (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: Amazon Aurora PostgreSQL – kompatibel
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora		

Übersicht

Dieses Muster beschreibt, wie eine Oracle-Datenbank mithilfe von AWS Data Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT) zu Amazon Aurora PostgreSQL kompatible Edition migriert wird.

Das Muster deckt Oracle-Quelldatenbanken ab, die On-Premises sind, Oracle-Datenbanken, die auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances installiert sind, und Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken. Das Muster konvertiert diese Datenbanken in Aurora PostgreSQL – kompatibel.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Oracle-Datenbank in einem On-Premises-Rechenzentrum oder in der AWS Cloud.
- SQL-Clients, die entweder auf einem lokalen Computer oder auf einer EC2-Instance installiert sind.
- Java Database Connectivity (JDBC)-Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder einer EC2-Instance installiert sind, auf der AWS SCT installiert ist.

Einschränkungen

- Datenbankgrößenbeschränkung: 128 TB
- Wenn die Quelldatenbank eine kommerzielle off-the-shelf (COTS)-Anwendung unterstützt oder herstellerspezifisch ist, können Sie sie möglicherweise nicht in eine andere Datenbank-Engine konvertieren. Bevor Sie dieses Muster verwenden, vergewissern Sie sich, dass die Anwendung Aurora PostgreSQL -kompatibel unterstützt.

Produktversionen

- Für selbstverwaltete Oracle-Datenbanken unterstützt AWS DMS alle Oracle-Datenbank-Editionen für die Versionen 10.2 und höher (für die Versionen 10.x), 11g und bis zu 12.2, 18c und 19c. Die neueste Liste der unterstützten Oracle-Datenbankversionen (sowohl selbstverwaltet als auch Amazon RDS für Oracle) finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS.
- Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden. Informationen zu Oracle-Datenbankversionen, die von AWS SCT unterstützt werden, finden Sie in der AWS SCT-Dokumentation.
- Aurora unterstützt die PostgreSQL-Versionen, die in Amazon-Aurora-PostgreSQL-Versionen und Engine-Versionen aufgeführt sind.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Oracle-Datenbank
- Eine Oracle-Datenbank auf einer EC2-Instance
- Eine DB-Instance von Amazon RDS für Oracle

Zieltechnologie-Stack

- Aurora PostgreSQL – kompatibel

Zielarchitektur

Datenmigrationsarchitektur

- Von einer Oracle-Datenbank, die in der AWS Cloud ausgeführt wird

- Von einer Oracle-Datenbank, die in einem On-Premises-Rechenzentrum ausgeführt wird

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Polen

Vorbereiten der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbank vor.	Informationen zur Vorbereitung der Quelldatenbank finden Sie unter Verwenden von Oracle Database als Quelle für AWS SCT in der AWS SCT-Dokumentation.	DBA
Erstellen Sie eine EC2-Instance für AWS SCT.	Erstellen und konfigurieren Sie bei Bedarf eine EC2-Instance für AWS SCT.	DBA
Laden Sie AWS SCT herunter.	Laden Sie die neueste Version von AWS SCT und die zugehörigen Treiber	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	herunter. Weitere Informationen finden Sie unter Installieren, Überprüfen und Aktualisieren von AWS SCT in der AWS SCT-Dokumentation.	
Fügen Sie Benutzer und Berechtigungen hinzu.	Fügen Sie die erforderlichen Benutzer und Berechtigungen in der Quelldatenbank hinzu und validieren Sie sie.	DBA
Erstellen Sie ein AWS SCT-Projekt.	Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindung mit der Quelldatenbank her. Anweisungen finden Sie unter Erstellen eines AWS SCT-Projekts und Hinzufügen von Datenbankservern in der AWS SCT-Dokumentation.	DBA
Bewerten Sie die Durchführbarkeit.	Generieren Sie einen Bewertungsbericht, der Aktionselemente für Schemata zusammenfasst, die nicht automatisch konvertiert werden können, und Schätzungen für manuelle Konvertierungsbemühungen liefert. Weitere Informationen finden Sie unter Erstellen und Überprüfen des Bewertungsberichts zur Datenbankmigration in der AWS SCT-Dokumentation.	DBA

Vorbereiten der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS-DB-Ziel-Instance.	Erstellen Sie eine Amazon RDS-DB-Ziel-Instance mit Amazon Aurora als Datenbank -Engine. Anweisungen finden Sie unter Erstellen einer Amazon-RDS-DB-Instance in der Amazon-RDS-Dokumen tation.	DBA
Extrahieren Sie Benutzer, Rollen und Berechtigungen.	Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Quelldatenbank.	DBA
Benutzer zuordnen.	Ordnen Sie die vorhanden en Datenbankbenutzer den neuen Datenbankbenutzern zu.	App-Besitzer
Erstellen Sie Benutzer.	Erstellen Sie Benutzer in der Zieldatenbank.	DBA, App-Besitzer
Wenden Sie Rollen an.	Wenden Sie Rollen aus dem vorherigen Schritt auf die Zieldatenbank an.	DBA
Überprüfen Sie Optionen, Parameter, Netzwerkdateien und Datenbanklinks.	Überprüfen Sie die Quelldate nbank auf Optionen, Parameter, Netzwerkdateien und Datenbanklinks und bewerten Sie dann deren Anwendbarkeit auf die Zieldatenbank.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie die Einstellungen an.	Wenden Sie alle relevanten Einstellungen auf die Zieldaten bank an.	DBA

Übertragen von Objekten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS SCT-Konnektivität.	Konfigurieren Sie die AWS SCT-Konnektivität zur Zieldatenbank.	DBA
Konvertieren Sie das Schema mit AWS SCT.	AWS SCT konvertiert das Quelldatenbankschema und den größten Teil des benutzerdefinierten Codes automatisch in ein Format, das mit der Zieldatenbank kompatibel ist. Jeder Code, den das Tool nicht automatis ch konvertieren kann, ist deutlich markiert, sodass Sie ihn manuell konvertieren können.	DBA
Überprüfen Sie den Bericht.	Überprüfen Sie den generiert en SQL-Bericht und speichern Sie alle Fehler und Warnungen.	DBA
Wenden Sie automatisierte Schemaänderungen an.	Wenden Sie automatisierte Schemaänderungen auf die Zieldatenbank an oder	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	speichern Sie sie als SQL-Datei.	
Validieren Sie Objekte.	Überprüfen Sie, ob AWS SCT die Objekte auf dem Ziel erstellt hat.	DBA
Verarbeiten Sie Elemente, die nicht konvertiert wurden.	Manuelles Umschreiben, Ablehnen oder Umdesigne n von Elementen, die nicht automatisch konvertiert werden konnten.	DBA, App-Besitzer
Wenden Sie Rollen- und Benutzerberechtigungen an.	Wenden Sie die generiert en Rollen- und Benutzerb erechtigungen an und überprüfen Sie alle Ausnahmen.	DBA

Migrieren der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie die -Methode.	Bestimmen Sie die Methode für die Migration von Daten.	DBA
Erstellen Sie eine Replikati ons-Instance.	Erstellen Sie eine Replikati ons-Instance über die AWS DMS-Konsole. Weitere Informationen finden Sie unter Arbeiten mit einer AWS DMS-Replikations-Instance in der AWS DMS-Dokumentation.	DBA
Erstellen Sie die Quell- und Zielendpunkte.	Um Endpunkte zu erstellen, folgen Sie den Anweisungen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Erstellen von Quell- und Zielendpunkten in der AWS DMS-Dokumentation.	
Erstellen Sie eine Replikationsaufgabe.	Informationen zum Erstellen einer Aufgabe finden Sie unter Arbeiten mit AWS DMS-Aufgaben in der AWS DMS-Dokumentation.	DBA
Starten Sie die Replikationsaufgabe und überwachen Sie die Protokolle.	Weitere Informationen zu diesem Schritt finden Sie unter Überwachung von AWS DMS-Aufgaben in der AWS DMS-Dokumentation.	DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren und konvertieren Sie SQL-Elemente im Anwendungscode.	Verwenden Sie AWS SCT, um die SQL-Elemente im Anwendungscode zu analysieren und zu konvertieren. Wenn Sie Ihr Datenbankschema von einer Engine in eine andere konvertieren, müssen Sie auch den SQL-Code in Ihren Anwendungen aktualisieren, damit diese mit der neuen Datenbank-Engine anstelle der alten interagieren. Sie können den konvertierten SQL-Code anzeigen, analysieren, bearbeiten und speichern.	App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Anwendung sserver.	Erstellen Sie die neuen Anwendungsserver auf AWS.	App-Besitzer
Migrieren Sie den Anwendung scode.	Migrieren Sie den Anwendung scode zu den neuen Servern.	App-Besitzer
Konfigurieren Sie die Anwendungsserver.	Konfigurieren Sie die Anwendungsserver für die Zieldatenbank und Treiber.	App-Besitzer
Code wurde korrigiert.	Korrigieren Sie jeden Code, der für die Quelldatenbank-Engine in Ihrer Anwendung spezifisch ist.	App-Besitzer
Code optimieren.	Optimieren Sie Ihren Anwendungscode für die Zieldatenbank-Engine.	App-Besitzer

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zur Zieldaten bank.	Führen Sie den Cutover für die neue Datenbank durch.	DBA
Sperren Sie die Anwendung.	Sperren Sie die Anwendung vor weiteren Änderungen.	App-Besitzer
Änderungen validieren.	Überprüfen Sie, ob alle Änderungen an die Zieldaten bank weitergegeben wurden.	DBA
Umleiten auf die Zieldaten bank.	Verweisen Sie die neuen Anwendungsserver auf die Zieldatenbank.	App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie alles.	Führen Sie eine abschließende, umfassende Systemprüfung durch.	App-Besitzer
Go-Live.	Schließen Sie die letzten Cutover-Aufgaben ab.	App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre Ressourcen herunter.	Fahren Sie die temporären AWS-Ressourcen wie die AWS DMS-Replikations-Instance und die für AWS SCT verwendete EC2-Instance herunter.	DBA, App-Besitzer
Feedback aktualisieren.	Aktualisieren Sie das Feedback zum AWS DMS-Prozess für interne Teams.	DBA, App-Besitzer
Überarbeiten Sie Prozess und Vorlagen.	Überarbeiten Sie den AWS DMS-Prozess und verbessern Sie die Vorlage bei Bedarf.	DBA, App-Besitzer
Validieren Sie Dokumente.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer
Erfassen Sie Metriken.	Erfassen Sie Metriken, um die Zeit für die Migration, den Prozentsatz der manuellen Kosteneinsparungen im Vergleich zu Tools usw. zu bewerten.	DBA, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie das Projekt.	Schließen Sie das Migration sprojekt und geben Sie den Stakeholdern Feedback.	DBA, App-Besitzer

Zugehörige Ressourcen

Referenzen

- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS Database Migration Service
- Oracle Database 11g/12c zu Amazon Aurora mit PostgreSQL-Kompatibilität (9.6.x) Migration Playbook
- Oracle Database 19c zu Amazon Aurora mit PostgreSQL-Kompatibilität (12.4) Migrations-Playbook
- Migrieren einer Datenbank von Amazon RDS für Oracle zu Amazon Aurora PostgreSQL – Kompatible Edition
- AWS Data Migration Service
- AWS Schema Conversion Tool
- Migrieren von Oracle zu Amazon Aurora
- Amazon-RDS-Preise

Tutorials und Videos

- Schrittweise Anleitungen zur Datenbankmigration
- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS Data Migration Service (Video)
- Migrieren einer Oracle-Datenbank zu PostgreSQL (Video)

Zusätzliche Informationen

.

Migrieren von Daten aus einer lokalen Oracle-Datenbank zu Aurora PostgreSQL

Erstellt von Bolle Deng (AWS) und Shunan Xiang (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora; AWS DMS; AWS SCT		

Übersicht

Dieses Muster bietet Anleitungen für die Datenmigration von einer On-Premises-Oracle-Datenbank zu Amazon Aurora PostgreSQL – kompatible Edition. Es zielt auf eine Strategie zur Online-Datenmigration mit minimaler Ausfallzeit für Oracle-Datenbanken mit mehreren Terabyte ab, die große Tabellen mit Aktivitäten mit hoher Datenmanipulationssprache (DML) enthalten. Eine Standby-Datenbank von Oracle Active Data Guard wird als Quelle verwendet, um die Datenmigration von der Primärdatenbank auszulagern. Die Replikation von der Oracle-Primärdatenbank in den Standby-Modus kann während des vollständigen Ladevorgangs ausgesetzt werden, um ORA-01555-Fehler zu vermeiden.

Tabellenspalten in Primärschlüsseln (PKs) oder Fremdschlüsseln (FKs) mit dem Datentyp NUMBER werden häufig verwendet, um Ganzzahlen in Oracle zu speichern. Wir empfehlen, diese in PostgreSQL in INT oder BIGINT zu konvertieren, um die Leistung zu verbessern. Sie können das AWS Schema Conversion Tool (AWS SCT) verwenden, um die Standard-Datentypzuordnung für PK- und FK-Spalten zu ändern. (Weitere Informationen finden Sie im AWS-BlogbeitragConvert the NUMBER data type from Oracle to PostgreSQL .) Bei der Datenmigration in diesem Muster wird AWS Database Migration Service (AWS DMS) sowohl für Volllast- als auch für die Erfassung von Datenänderungen (Change Data Capture, CDC) verwendet.

Sie können dieses Muster auch verwenden, um eine lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder eine Oracle-Datenbank zu migrieren, die

in Amazon Elastic Compute Cloud (Amazon EC2) gehostet wird, entweder zu Amazon RDS für PostgreSQL oder Aurora PostgreSQL -kompatibel.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem On-Premises-Rechenzentrum mit konfiguriertem Active Data Guard-Standby
- AWS Direct Connect zwischen dem On-Premises-Rechenzentrum und der AWS Cloud konfiguriert
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als Ziel für AWS DMS

Einschränkungen

- Amazon-Aurora-Datenbank-Cluster können mit bis zu 128 TiB Speicher erstellt werden. Datenbank-Instances von Amazon RDS für PostgreSQL können mit bis zu 64 TiB Speicher erstellt werden. Die neuesten Speicherinformationen finden Sie unterAmazon Aurora-Speicher und -Zuverlässigkeit undAmazon RDS-DB-Instance-Speicher in der AWS-Dokumentation.

Produktversionen

- AWS DMS unterstützt alle Oracle-Datenbank-Editionen für die Versionen 10.2 und höher (für die Versionen 10.x), 11g und bis zu 12.2, 18c und 19c. Die neueste Liste der unterstützten Versionen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- On-Premises-Oracle-Datenbanken mit konfiguriertem Standby von Oracle Active Data Guard

Zieltechnologie-Stack

- Aurora PostgreSQL – kompatibel

Datenmigrationsarchitektur

Tools

- AWS DMS – AWS Database Migration Service (AWS DMS) unterstützt mehrere Quell- und Zieldatenbanken. Eine Liste der unterstützten Oracle-Quell- und Zieldatenbankversionen und -editionen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation. Wenn die Quelldatenbank nicht von AWS DMS unterstützt wird, müssen Sie eine andere Methode für die Migration der Daten in Phase 6 (im Abschnitt Epics) auswählen.Wichtiger Hinweis: Da es sich um eine heterogene Migration handelt, müssen Sie zunächst überprüfen, ob die Datenbank eine kommerzielle off-the-shelf (COTS)-Anwendung unterstützt. Wenn es sich bei der Anwendung um COTS handelt, wenden Sie sich an den Anbieter, um zu bestätigen, dass Aurora PostgreSQL – kompatibel unterstützt wird, bevor Sie fortfahren. Weitere Informationen finden Sie unter Schritt-für-Schritt-Anleitungen zur AWS DMS-Migration in der AWS-Dokumentation.
- AWS SCT – Das AWS Schema Conversion Tool (AWS SCT) erleichtert heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Der benutzerdefinierte Code, den das Tool konvertiert, umfasst Ansichten, gespeicherte Prozeduren und Funktionen. Jeder Code, den das Tool nicht automatisch konvertieren kann, ist deutlich markiert, sodass Sie ihn selbst konvertieren können.

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Installieren Sie AWS SCT und Treiber.		DBA
Fügen Sie die erforderlichen AWS SCT-Benutzer und die		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Grants-Source-Datenbank hinzu und validieren Sie sie.		
Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindung mit der Quelldatenbank her.		DBA
Generieren Sie einen Bewertungsbericht und bewerten Sie die Durchführ barkeit.		DBA, App-Besitzer

Vorbereiten der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora-PostgreSQL-kompatible Zieldatenbank.		DBA
Extrahieren Sie die Liste der Benutzer, Rollen und Erteilung en aus der Quelldatenbank.		DBA
Ordnen Sie die vorhanden en Datenbankbenutzer den neuen Datenbankbenutzern zu.		App-Besitzer
Erstellen Sie Benutzer in der Zieldatenbank.		DBA
Wenden Sie Rollen aus dem vorherigen Schritt auf die		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aurora PostgreSQL-kompatible Zieldatenbank an.		
Überprüfen Sie Datenbankoptionen, Parameter, Netzwerkdateien und Datenbanklinks aus der Quelldatenbank und bewerten Sie deren Anwendbarkeit auf die Zieldatenbank.		DBA, App-Besitzer
Wenden Sie alle relevanten Einstellungen auf die Zieldatenbank an.		DBA

Vorbereiten der Konvertierung von Datenbankobjektcode

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS SCT-Konnektivität zur Zieldatenbank.		DBA
Konvertieren Sie das Schema in AWS SCT und speichern Sie den konvertierten Code als SQL-Datei.		DBA, App-Besitzer
Konvertieren Sie manuell alle Datenbankobjekte, die nicht automatisch konvertiert werden konnten.		DBA, App-Besitzer
Optimieren Sie die Datenbankcodekonvertierung.		DBA, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Trennen Sie die .sql-Date i je nach Objekttyp in mehrere .sql-Dateien.		DBA, App-Besitzer
Validieren Sie die SQL-Skripts in der Zieldatenbank.		DBA, App-Besitzer

Vorbereiten der Datenmigration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.		DBA
Erstellen Sie die Quell- und Zielendpunkte.	Wenn der Datentyp der PKs und FKs von NUMBER in Oracle in BIGINT in PostgreSQL konvertiert wird, sollten Sie `numberDataTypeScale=-2` bei der Erstellung des Quellendpunkts das Verbindungsattribut angeben.	DBA

Migrieren von Daten – Volllast

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Schema und die Tabellen in der Zieldatenbank.		DBA
Erstellen Sie AWS DMS-Volllastaufgaben, indem Sie		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
entweder Tabellen gruppiere n oder eine große Tabelle basierend auf der Tabelleng röße aufteilen.		
Halten Sie die Anwendung en in den Oracle-Quelldatenb anken für einen kurzen Zeitraum an.		App-Besitzer
Stellen Sie sicher, dass die Oracle-Standby-Datenbank synchron mit der Primärdat enbank ist, und beenden Sie die Replikation von der Primärdatenbank zur Standby-Datenbank.		DBA, App-Besitzer
Starten Sie Anwendungen in der Oracle-Quelldatenbank.		App-Besitzer
Starten Sie die AWS DMS-Volllastaufgaben parallel von der Oracle-Standby-Dat enbank zur Aurora PostgreSQ L-kompatiblen Datenbank.		DBA
Erstellen Sie PKs und sekundäre Indizes, nachdem der vollständige Ladevorgang abgeschlossen ist.		DBA
Validieren Sie die Daten.		DBA

Daten migrieren – CDC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie laufende AWS DMS-Replikationsaufgaben, indem Sie eine benutzerd efinierte CDC-Startzeit oder Systemänderungsnummer (SCN) angeben, wenn die Oracle-Standby-Datenbank mit der Primärdatenbank synchronisiert wurde und bevor die Anwendungen in der vorherigen Aufgabe neu gestartet wurden.		DBA
Starten Sie parallel AWS DMS-Aufgaben, um laufende Änderungen von der Oracle-Standby-Datenbank in die Aurora PostgreSQL-kompati ble Datenbank zu replizieren.		DBA
Stellen Sie die Replikation von der Oracle-Primärdaten bank zur Standby-Datenbank wieder her.		DBA
Überwachen Sie die Protokolle und halten Sie die Anwendung en in der Oracle-Datenbank an, wenn die Aurora PostgreSQL-kompatible Zieldatenbank fast synchron mit der Oracle-Quelldatenbank ist.		DBA, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die AWS DMS-Aufgaben an, wenn das Ziel vollständig mit der Oracle-Quelldatenbank synchronisiert ist.		DBA
Erstellen Sie FKs und validieren Sie die Daten in der Zieldatenbank.		DBA
Erstellen Sie Funktionen, Ansichten, Auslöser, Sequenzen und andere Objekttypen in der Zieldatenbank.		DBA
Wenden Sie Rollengewährungen in der Zieldatenbank an.		DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS SCT, um die SQL-Anweisungen innerhalb des Anwendungscodes zu analysieren und zu konvertieren.		App-Besitzer
Erstellen Sie neue Anwendungsserver auf AWS.		App-Besitzer
Migrieren Sie den Anwendungscode zu den neuen Servern.		App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Anwendungsserver für die Zieldatenbank und Treiber.		App-Besitzer
Korrigieren Sie jeden Code, der für die Quelldatenbank-Engine in der Anwendung spezifisch ist.		App-Besitzer
Optimieren Sie den Anwendungscode für die Zieldatenbank.		App-Besitzer

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verweisen Sie den neuen Anwendungsserver auf die Zieldatenbank.		DBA, App-Besitzer
Führen Sie Sanitätsprüfungen durch.		DBA, App-Besitzer
Go-Live.		DBA, App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie Metriken für die Zeit bis zur Migration, den Prozentsatz der manuellen Verwendung im Vergleich zu Tools, Kosteneinsparungen und ähnliche Daten.		DBA, App-Besitzer
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer

Zugehörige Ressourcen

Referenzen

- Oracle Database to Aurora PostgreSQL – kompatibel: Migration Playbook
- Migrieren einer Amazon RDS for Oracle Database zu Amazon Aurora MySQL
- AWS DMS-Website
- AWS DMS-Dokumentation
- AWS SCT-Website
- AWS SCT-Dokumentation
- Migrieren von Oracle zu Amazon Aurora

Tutorials

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- Schrittweise Anleitungen zum AWS Database Migration Service

Migrieren von SAP ASE zu Amazon RDS for SQL Server mit AWS DMS

Erstellt von Amit Kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: SAP ASE	Ziel: Amazon RDS für SQL Server
R-Typ: Re-Architektur	Workload: SAP	Technologien: Migration; Datenbanken; Modernisierung
AWS-Services: Amazon RDS; AWS DMS		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer SAP Adaptive Server Enterprise (ASE)-Datenbank zu einer Amazon Relational Database Service (Amazon RDS)-DB-Instance, auf der Microsoft SQL Server ausgeführt wird. Die Quelldatenbank kann sich in einem On-Premises-Rechenzentrum oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance befinden. Das Muster verwendet AWS Database Migration Service (AWS DMS), um Daten zu migrieren, und (optional) Tools für computerunterstütztes Software-Engineering (CASE), um das Datenbankschema zu konvertieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine SAP-ASE-Datenbank in einem On-Premises-Rechenzentrum oder auf einer EC2-Instance
- Eine aktive Amazon RDS for SQL Server-Zieldatenbank

Einschränkungen

- Datenbankgrößenbeschränkung: 64 TB

Produktversionen

- Nur SAP ASE Version 15.7 oder 16.x. Die neuesten Informationen finden Sie unter Verwenden einer SAP-Datenbank als Quelle für AWS DMS.
- Für Amazon RDS-Zieldatenbanken unterstützt AWS DMS Microsoft SQL Server-Versionen auf Amazon RDS für die Editionen Enterprise, Standard, Web und Express. Die neuesten Informationen zu unterstützten Versionen finden Sie in der AWS-DMS-Dokumentation. Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden.

Architektur

Quelltechnologie-Stack

- Eine SAP-ASE-Datenbank, die sich On-Premises oder auf einer Amazon EC2 befindet

Zieltechnologie-Stack

- Eine DB-Instance von Amazon RDS für SQL Server

Quell- und Zielarchitektur

Von einer SAP-ASE-Datenbank auf Amazon EC2 zu einer Amazon-RDS-für-SQL-Server-DB-Instance:

Von einer lokalen SAP-ASE-Datenbank zu einer Amazon RDS for SQL Server-DB-Instance:

Tools

- AWS Database Migration Service (AWS DMS) ist ein Webservice, mit dem Sie Daten von Ihrer On-Premises-Datenbank, auf einer Amazon RDS-DB-Instance oder in einer Datenbank auf einer EC2-Instance zu einer Datenbank auf einem AWS-Service wie Amazon RDS für SQL Server oder einer EC2-Instance migrieren können. Sie können eine Datenbank auch von einem AWS-Service zu einer On-Premises-Datenbank migrieren. Sie können Daten zwischen heterogenen oder homogenen Datenbank-Engines migrieren.
- Für Schemakonvertierungen können Sie optional erwin Data Modeler oder SAP PowerDesigner verwenden.

Sekunden

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instance-Typ basierend auf Kapazität, Speicherfunktionen und Netzwerkfunktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie die Strategie für die Anwendungsmigration.		DBA, SysAdmin, App-Besitzer

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs).		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie eine Amazon RDS-DB-In stance.		SysAdmin

Daten migrieren – Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie das Datenbank schema manuell oder verwenden Sie ein CASE-Tool wie erwin Data Modeler oder SAP PowerDesigner.		DBA

Daten migrieren – Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.		DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, SysAdmin, App-Besitzer

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA, SysAdmin, App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin, App-Besitzer
Erfassen Sie Metriken wie die Zeit für die Migration, den Prozentsatz manueller und automatisierter Aufgaben sowie Kosteneinsparungen.		DBA, SysAdmin, App-Besitzer
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, SysAdmin, App-Besitzer

Zugehörige Ressourcen

Referenzen

- AWS DMS-Website
- Amazon RDS – Preise
- Verwenden einer SAP ASE-Datenbank als Quelle für AWS DMS
- Einschränkungen für RDS Custom für SQL Server

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS DMS (Video)
- Amazon RDS (Video)

Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mit AWS DMS

Erstellt vonelo Fernandes (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Microsoft SQL Server	Ziel: Amazon Redshift
R-Typ: Neuarchitektur	Workload: Microsoft	Technologien: Migration; Datenbanken
AWS-Services: Amazon Redshift		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS Data Migration Service (AWS DMS).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Quelldatenbank von Microsoft SQL Server in einem On-Premises-Rechenzentrum
- Erfüllte Voraussetzungen für die Verwendung einer Amazon-Redshift-Datenbank als Ziel für AWS DMS, wie in der AWS-DMS-Dokumentation beschrieben

Produktversionen

- SQL Server 2005-2019, Enterprise, Standard, Arbeitsgruppe, Entwickler und Web Editionen. Die neueste Liste der unterstützten Versionen finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS in der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Amazon Redshift

Datenmigrationsarchitektur

Tools

- AWS DMS ist ein Datenmigrationsservice, der verschiedene Arten von Quell- und Zieldatenbanken unterstützt. Informationen zu den Microsoft SQL Server-Datenbankversionen und -editionen, die für die Verwendung mit AWS DMS unterstützt werden, finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation. Wenn AWS DMS Ihre Quelldatenbank nicht unterstützt, müssen Sie eine alternative Methode für die Datenmigration auswählen.

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserver-Instance.		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie basierend auf Kapazität, Speicherfunktionen und Netzwerkfunktionen den richtigen Instance-Typ aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, Systemadministrator
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Weitere Informationen finden Sie unter Arbeiten mit einer DB-Instance in einer VPC in der AWS-Dokumentation.	Systemadministrator
Erstellen Sie Sicherheitsgruppen.		Systemadministrator
Konfigurieren und starten Sie einen Amazon-Redshift-Cluster.	Weitere Informationen finden Sie unter Erstellen eines Amazon-Redshift-Beispielclusters in der Amazon-Redshift-Dokumentation.	DBA, Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten aus der Microsoft SQL Server-Datenbank mithilfe von AWS DMS.		DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie die Anwendung sclients auf die neue Infrastru ktur.		DBA, App-Besitzer, Systemadministrator

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Erfassen Sie Metriken wie die Zeit für die Migration, den		DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Prozentsatz manueller und automatisierter Aufgaben sowie Kosteneinsparungen.		
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- AWS DMS-Dokumentation
- Amazon-Redshift-Dokumentation
- Amazon-Redshift-Preise

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon Redshift
- Verwenden einer Amazon Redshift-Datenbank als Ziel für AWS Database Migration Service
- AWS DMS (Video)

Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten

Erstellt von Neha Thakur (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Microsoft SQL Server	Ziel: Amazon Redshift
R-Typ: Neuarchitektur	Workload: Microsoft	Technologien: Migration; Datenbanken
AWS-Services: Amazon Redshift; AWS SCT		

Übersicht

Dieses Muster beschreibt die Schritte zur Migration einer lokalen Microsoft SQL Server-Quelldatenbank zu einer Amazon Redshift-Zieldatenbank mithilfe von AWS Schema Conversion Tool (AWS SCT)-Datenextraktionsagenten. Ein Agent ist ein externes Programm, das in AWS SCT integriert ist, aber die Datentransformation an anderer Stelle durchführt und in Ihrem Namen mit anderen AWS-Services interagiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Microsoft SQL Server-Quelldatenbank, die für die Data Warehouse-Workload in einem On-Premises-Rechenzentrum verwendet wird
- Ein aktives AWS-Konto

Produktversionen

- Microsoft SQL Server Version 2008 oder höher. Die neueste Liste der unterstützten Versionen finden Sie in der AWS SCT-Dokumentation.

Architektur

Quelle des Technologie-Stacks

- Eine lokale Microsoft SQL Server-Datenbank

-Technologie-Stack-Ziel

- Amazon Redshift

Datenmigrationsarchitektur

Tools

- AWS Schema Conversion Tool (AWS SCT) verarbeitet heterogene Datenbankmigrationen, indem es das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert, das mit der Zieldatenbank kompatibel ist. Wenn sich die Quell- und Zieldatenbanken stark unterscheiden, können Sie einen AWS SCT-Agenten verwenden, um eine zusätzliche Datentransformation durchzuführen. Weitere Informationen finden Sie unter Migrieren von Daten aus einem On-Premises-Data-Warehouse zu Amazon Redshift in der AWS-Dokumentation.

Bewährte Methoden

- Bewährte Methoden für AWS SCT
- Bewährte Methoden für Amazon Redshift

Polen

Vorbereiten der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen und Engines.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserver-Instance.		DBA, SysAdmin
Identifizieren Sie Speichera nforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instance-Typ aus (Kapazität, Speicherfunktionen, Netzwerkf unktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Wählen Sie eine Strategie für die Anwendungsmigration aus.		DBA, SysAdmin, App-Besitzer

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze.		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherheitsgruppen.		SysAdmin
Konfigurieren und starten Sie den Amazon-Redshift-Cluster.		SysAdmin

Migrieren von Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe der AWS SCT-Datenextraktionsagenten.		DBA

Migrieren von Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewählten Strategie zur Anwendungsmigration.		DBA, SysAdmin, App-Besitzer

Umstellung auf die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie Anwendungsclients auf die neue Infrastruktur.		DBA, SysAdmin, App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin, App-Besitzer
Erfassen Sie Metriken wie die Zeit für die Migration, den Prozentsatz manueller und automatisierter Aufgaben sowie Kosteneinsparungen.		DBA, SysAdmin, App-Besitzer
Schließen Sie das Projekt und geben Sie Feedback.		DBA, SysAdmin, App-Besitzer

Zugehörige Ressourcen

Referenzen

- AWS SCT-Benutzerhandbuch
- Verwenden von Data Extraction Agents
- Amazon Redshift – Preise

Tutorials und Videos

- Erste Schritte mit dem AWS Schema Conversion Tool
- Erste Schritte mit Amazon Redshift

Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift

R-Typ: Re-Architect	Quelle: Datenbanken: Relational	Ziel: Amazon Redshift
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
AWS-Dienste: Amazon Redshift		

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer Teradata-Datenbank, die als Data Warehouse in einem lokalen Rechenzentrum verwendet wird, zu einer Amazon Redshift Redshift-Datenbank. Das Muster verwendet Datenextraktionsagenten des AWS Schema Conversion Tool (AWS SCT). Ein Agent ist ein externes Programm, das in AWS SCT integriert ist, die Datentransformation jedoch an anderer Stelle durchführt und in Ihrem Namen mit anderen AWS-Services interagiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Teradata-Quelldatenbank in einem lokalen Rechenzentrum

Produktversionen

- Teradata Version 13 und höher. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS SCT-Dokumentation.

Architektur

Quelltechnologie-Stack

- Lokale Teradata-Datenbank

Zieltechnologie-Stack

- Amazon-Redshift-Cluster

Architektur der Datenmigration

Tools

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) verarbeitet heterogene Datenbankmigrationen, indem es das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert, das mit der Zieldatenbank kompatibel ist. Wenn sich die Quell- und Zieldatenbanken stark voneinander unterscheiden, können Sie einen AWS SCT-Agenten verwenden, um zusätzliche Datentransformationen durchzuführen. Weitere Informationen finden Sie in der AWS-Dokumentation unter Migrieren von Daten aus einem lokalen Data Warehouse zu Amazon Redshift.

Epen

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instanztyp (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Wählen Sie eine Strategie für die Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherheitsgruppen.		SysAdmin
Konfigurieren und starten Sie den Amazon Redshift Redshift-Cluster.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mithilfe von AWS SCT-Datenextraktionsagenten.	Detaillierte Informationen zur Verwendung von AWS SCT-Datenextraktionsagenten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter den Links im Abschnitt Referenzen und Hilfe.	

Anwendungen migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewähl ten Strategie zur Anwendung smigration.		DBA SysAdmin, Besitzer der App

Wechseln Sie zur Amazon Redshift Redshift-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Sammeln Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz manueller Aufgaben im Vergleich zu		DBA SysAdmin, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Toolaufgaben, zu Kostenein sparungen usw.		
Schließen Sie das Projekt und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- AWS SCT-Benutzerhandbuch
- Verwendung von Datenextraktionsagenten
- Amazon Redshift — Preise
- Konvertieren Sie die Teradata RESET WHEN-Funktion auf Amazon Redshift SQL (AWS Prescriptive Guidance)
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL (AWS Prescriptive Guidance)

Tutorials

- Erste Schritte mit dem AWS Schema Conversion Tool
- Erste Schritte mit Amazon Redshift

Migrieren Sie eine lokale Vertica-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift

R-Typ: Re-Architect	Quelle: Datenbanken: Relational	Ziel: Amazon Redshift
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
AWS-Dienste: Amazon Redshift		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen Vertica-Datenbank zu einem Amazon Redshift Redshift-Cluster mithilfe der Datenextraktionsagenten des AWS Schema Conversion Tool (AWS SCT). Ein Agent ist ein externes Programm, das in AWS SCT integriert ist, die Datentransformation jedoch an anderer Stelle durchführt und in Ihrem Namen mit anderen AWS-Services interagiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Vertica-Quelldatenbank, die für die Data Warehouse-Arbeitslast in einem lokalen Rechenzentrum verwendet wird
- Ein Amazon Redshift Redshift-Zielcluster

Produktversionen

- Vertica Version 7.2.2 und höher. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS SCT-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Vertica-Datenbank

Zieltechnologie-Stack

- Ein Amazon Redshift Redshift-Cluster

Architektur der Datenmigration

Tools

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) verarbeitet heterogene Datenbankmigrationen, indem es das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert, das mit der Zieldatenbank kompatibel ist. Wenn sich die Quell- und Zieldatenbanken stark voneinander unterscheiden, können Sie einen AWS SCT-Agenten verwenden, um zusätzliche Datentransformationen durchzuführen. Weitere Informationen finden Sie in der AWS-Dokumentation unter Migrieren von Daten aus einem lokalen Data Warehouse zu Amazon Redshift.

Epen

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instanztyp (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Wählen Sie eine Strategie für die Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherheitsgruppen.		SysAdmin
Konfigurieren und starten Sie einen Amazon Redshift Redshift-Cluster.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe der AWS SCT-Datenextraktionsagenten.	Detaillierte Informationen zur Verwendung von AWS SCT-Datenextraktionsagenten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter den Links im Abschnitt Referenzen und Hilfe.	

Anwendungen migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewähl ten Strategie zur Anwendung smigration.		DBA SysAdmin, Besitzer der App

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Sammeln Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz manueller Aufgaben im Vergleich zu		DBA SysAdmin, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Toolaufgaben, zu Kostenein sparungen usw.		
Schließen Sie das Projekt und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- AWS SCT-Benutzerhandbuch
- Verwendung von Datenextraktionsagenten
- Amazon Redshift — Preise

Tutorials und Videos

- Erste Schritte mit dem AWS Schema Conversion Tool
- Erste Schritte mit Amazon Redshift

Migrieren älterer Anwendungen von Oracle Pro*C zu ECPG

Erstellt von Sai Parthasaradhi (AWS) undesh Balumuri (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken

Übersicht

Die meisten Legacy-Anwendungen mit eingebettetem SQL-Code verwenden den Oracle Pro*C-Precompiler, um auf die Datenbank zuzugreifen. Wenn Sie diese Oracle-Datenbanken zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL - kompatible Edition migrieren, müssen Sie Ihren Anwendungscode in ein Format konvertieren, das mit dem Precompiler in PostgreSQL kompatibel ist, der als ECPG bezeichnet wird. Dieses Muster beschreibt, wie Oracle-Pro*C-Code in sein Äquivalent in PostgreSQL ECPG konvertiert wird.

Weitere Informationen zu Pro*C finden Sie in der Oracle-Dokumentation. Eine kurze Einführung in ECPG finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine mit Amazon RDS for PostgreSQL oder Aurora PostgreSQL kompatible Datenbank
- Eine Oracle-Datenbank, die On-Premises ausgeführt wird

Tools

- Die im nächsten Abschnitt aufgeführten PostgreSQL-Pakete.
- AWS CLI – Die AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS CLI-Befehle ausführen, die Funktionen implementieren, die denen entsprechen,

die von der browserbasierten AWS-Managementkonsole über eine Eingabeaufforderung bereitgestellt werden.

Polen

Festlegen der Build-Umgebung auf CentOS oder RHEL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie PostgreSQL-Pakete.	Installieren Sie die erforderlichen PostgreSQL-Pakete mithilfe der folgenden Befehle.
	`yum update -y`
	`yum install -y yum-utils`
	`rpm -ivh https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm`
	`dnf -qy module disable postgresql`
		App-Entwickler, DevOps Techniker

Installieren Sie die Header-Dateien und Bibliotheken.	Installieren Sie das`postgresql12-devel` -Paket, das Header-Dateien und Bibliotheken enthält, mithilfe der folgenden Befehle. Installieren Sie das -Paket sowohl in der Entwicklungs- als auch in der Laufzeitumgebung, um Fehler in der Laufzeitumgebung zu vermeiden. `dnf -y install postgresql12-devel`	App-Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`yum install ncompress zip ghostscript jq unzip wget git -y`
	
	Führen Sie nur für die Entwicklungsumgebung die folgenden Befehle aus.
	
	`yum install zlib-devel make -y`
	`ln -s /usr/pgsql-12/bin/ecpg /usr/bin/`	

Konfigurieren Sie die Umgebungspfadvariable.	Legen Sie den Umgebungspfad für PostgreSQL-Clientbibliotheken fest. `export PATH=$PATH:/usr/pgsql-12/bin`	App-Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie bei Bedarf zusätzliche Software.	Falls erforderlich, installieren Sie pgLoader als Ersatz für SQL*Loader in Oracle.
	`wget -O /etc/yum.repos.d/pgloader-ccl.repo https://dl.packager.io/srv/opf/pgloader-ccl/master/installer/el/7.repo`
	`yum install pgloader-ccl -y`
	`ln -s /opt/pgloader-ccl/bin/pgloader /usr/bin/`
	Wenn Sie Java-Anwendungen von Pro*C-Modulen aus aufrufen, installieren Sie Java.
	`yum install java -y`
	Installieren Sie ant, um den Java-Code zu kompilieren.
	`yum install ant -y`
		App-Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie den AWS CLI.	Installieren Sie die AWS CLI, um Befehle für die Interakti on mit AWS-Services wie AWS Secrets Manager und Amazon Simple Storage Service (Amazon S3) von Ihren Anwendungen aus auszuführen.
	`cd /tmp/`
	`curl "https://`
	`awscli.amazonaws.c`
	`om/awscli-exe-linu`
	`x-x86_64.zip" -o`
	` "awscliv2.zip"`
	`unzip awscliv2.zip`
	`./aws/install -i /usr/`
	`local/aws-cli -b /usr/`
	`local/bin --update`
		App-Entwickler, DevOps Techniker

Identifizieren Sie die Programme, die konvertiert werden sollen.	Identifizieren Sie die Anwendungen, die Sie von Pro*C in ECPG konvertieren möchten.	App-Entwickler, App-Besitzer

Pro*C-Code in ECPG konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie unerwünschte Header.	Entfernen Sie die `include` Header, die in PostgreSQL nicht erforderlich sind, z. B. `oci.horatypes`, und `sqlda`.	App-Besitzer, App-Entwickler
Aktualisieren Sie Variablen deklarationen.	Fügen Sie `EXEC SQL` Anweisungen für alle	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Variablendeklarationen hinzu, die als Hostvariablen verwendet werden. Entfernen Sie die `EXEC SQL VAR` Deklarationen wie die folgenden aus Ihrer Anwendung. `EXEC SQL VAR query IS STRING(2048);`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die ROWNUM-Funktionalität.	Die `ROWNUM` Funktion ist in PostgreSQL nicht verfügbar . Ersetzen Sie dies durch die `ROW_NUMBER` Fensterfunktion in SQL-Abfragen.
	
	Pro*C-Code:
	
	`SELECT SUBSTR(RTRIM(FILE_NAME,'.txt'),12) INTO :gcpclFileseq FROM (SELECT FILE_NAME FROM DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;`
	
	ECPG-Code:
	
	`SELECT SUBSTR(RTRIM(FILE_NAME,'.txt'),12) INTO :gcpclFileseq FROM (SELECT FILE_NAME , ROW_NUMBER() OVER (ORDER BY FILE_NAME DESC) AS ROWNUM FROM demo_schema.DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`WHERE ROWNUM <=1 ORDER BY ROWNUM;`	

Aktualisieren Sie Funktionsparameter, um Aliasvariablen zu verwenden.	In PostgreSQL können Funktionsparameter nicht als Hostvariablen verwendet werden. Überschreiben Sie sie mithilfe einer Aliasvariablen.
	
	Pro*C-Code:
	
	`int processData(int referenceId){ EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
	
	ECPG-Code:
	
	`int processData(int referenceIdParam){ EXEC SQL int referenceId = referenceIdParam; EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Strukturtypen.	Definieren Sie `struct` Typen in - `EXEC SQL BEGIN` und -`END`Blöcken mit `typedef` , wenn die `struct` Typvariablen als Hostvariablen verwendet werden. Wenn die `struct` Typen in Header-Dateien (`.h`) definiert sind, schließen Sie die Dateien mit `EXEC SQL` Include-Anweisungen ein. Pro*C-Code: Header-Datei (`demo.h`) `struct s_partition_ranges { char sc_table_group[31]; char sc_table_name[31]; char sc_range_value[10]; }; struct s_partition_ranges_ind { short ss_table_group; short ss_table_name; short ss_range_value; };` ECPG-Code:	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Header-Datei (`demo.h`)
	`EXEC SQL BEGIN DECLARE SECTION;`
	`typedef struct { char sc_table_group[31]; char sc_table_name[31]; char sc_range_value[10]; } s_partition_ranges;`
	`typedef struct { short ss_table_group; short ss_table_name; short ss_range_value; } s_partition_ranges_ind;`
	`EXEC SQL END DECLARE SECTION;`
	Pro*C-Datei (`demo.pc`)
	`#include "demo.h"`
	`struct s_partition_ranges gc_partition_data[MAX_PART_TABLE] ;`
	`struct s_partition_ranges_ind gc_partition_data_ind[MAX_PART_TABLE] ;`
	ECPG-Datei (`demo.pc`)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`exec sql include "demo.h" EXEC SQL BEGIN DECLARE SECTION; s_partition_ranges gc_partition_data[ MAX_PART_TABLE] ; s_partition_ranges_ind gc_partition_data_ ind[MAX_PART_TABLE] ; EXEC SQL END DECLARE SECTION;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Logik, um sie von Cursorn abzurufen.	Um mehrere Zeilen mithilfe von Array-Variablen von Cursorn abzurufen, ändern Sie den Code so, dass er verwendet`FETCH FORWARD`.
	
	Pro*C-Code:
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL FETCH filename_ cursor into :aPoeFile s;`
	
	ECPG-Code:
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL int fetchSize = MAX_FILES; EXEC SQL FETCH FORWARD :fetchSiz e filename_cursor into :aPoeFiles;`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie Paketaufrufe, die keine Rückgabewerte haben.	Oracle-Paketfunktionen, die keine Rückgabewerte haben, sollten mit einer Indikator variablen aufgerufen werden. Wenn Ihre Anwendung mehrere Funktionen enthält, die denselben Namen haben, oder wenn die Funktionen des unbekannten Typs Laufzeitf ehler generieren, geben Sie die Werte in die Datentypen ein.
	
	Pro*C-Code:
	
	`void ProcessData (char *data , int id) { EXEC SQL EXECUTE BEGIN pkg_demo. process_data (:data, :id); END; END-EXEC; }`
	
	ECPG-Code:
	
	`void ProcessData (char *dataParam, int idParam ) { EXEC SQL char *data = dataParam;`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>EXEC SQL int id
	= idParam;
	EXEC SQL short
	rowInd;
	EXEC SQL short
	rowInd = 0;
	EXEC SQL SELECT
	pkg_demo.process_data
	(
	
	inp_data => :data::te
	xt,
	
	inp_id => :id
	)
	INTO :rowInd;
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Schreiben Sie SQL_CURSOR-Variablen neu.	Schreiben Sie die `SQL_CURSOR` Variable und ihre Implementierung neu.
	
	Pro*C-Code:
	
	`/* SQL Cursor */`
	`SQL_CU`
	`RSOR demo_cursor;`
	`EXEC SQL`
	`ALLOCATE :demo_cursor;`
	`EXEC SQL EXECUTE`
	`BEGIN`
	`pkg_demo.`
	`get_cursor(`
	`demo_cur=`
	`>:demo_cursor`
	`);`
	`END;`
	`END-EXEC;`
	
	ECPG-Code:
	
	`EXEC SQL DECLARE`
	`demo_cursor CURSOR FOR`
	`SELECT`
	`* from`
	`pkg_demo.open_file`
	`name_rc(`
	`demo_cur=`
	`>refcursor`
	`) ;`
	`EXEC SQL char open_file`
	`name_rcInd[100];`
	`# As the below function`
	`returns cursor_name`
	`as`
	`# return we need to`
	`use char[] type as`
	`indicator.`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXEC SQL SELECT pkg_demo.get_cursor ( demo_cur=>'demo_cursor' ) INTO :open_filename_rcInd;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie gängige Migration smuster an.	• Ändern Sie SQL-Abfragen, damit sie mit PostgreSQL kompatibel sind. • Verschieben Sie anonyme Blöcke, wenn sie in ECPG nicht unterstützt werden, in die Datenbank. • Entfernen Sie die `dbms_application_info` Logik, die von PostgreSQL nicht unterstützt wird. • Verschieben Sie `EXEC SQL COMMIT` Anweisungen nach dem Schließen des Cursors. Wenn Sie Abfragen übergeben, während Sie sich in der Schleife befinden, um die Datensätze vom Cursor abzurufen, wird der Cursor geschlossen und ein Cursor ist nicht vorhanden-Fehler wird angezeigt. • Informationen zur Behandlung von Ausnahmen in ECPG und Fehlercodes finden Sie unter Fehlerbehandlung in der PostgreSQL-Dokumentation.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie bei Bedarf das Debugging.	Um das ECPG-Programm im Debug-Modus auszuführ en, fügen Sie den folgenden Befehl im Hauptfunktionsblock hinzu. `ECPGdebug(1, stderr);`	App-Entwickler, App-Besitzer

Kompilieren von ECPG-Programmen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine ausführbare Datei für ECPG.	Wenn Sie über eine eingebett ete SQL-C-Quelldatei mit dem Namen verfügen`prog1.pgc` , können Sie ein ausführba res Programm erstellen, indem Sie die folgende Befehlsse quenz verwenden.
	`ecpg prog1.pgc`
	`cc -I/usr/local/pgsql/ include -c prog1.c`
	`cc -o prog1 prog1.o -L/ usr/local/pgsql/lib - lecpg`
		App-Entwickler, App-Besitzer

Erstellen Sie eine Make-Datei für die Kompilierung.	Erstellen Sie eine Make-Datei, um das ECPG-Prog ramm zu kompilieren, wie in der folgenden Beispieldatei gezeigt.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`CFLAGS ::= $(CFLAGS) -I/usr/pgsql-12/include -g -Wall`
	`LDFLAGS ::= $(LDFLAGS) -L/usr/pgsql-12/lib -Wl,-rpath,/usr/pgsql-12/lib`
	`LDLIBS ::= $(LDLIBS) -lecpg`
	`PROGRAMS = test`
	`.PHONY: all clean`
	`%.c: %.pgc`
	`  ecpg $<`
	`all: $(PROGRAMS)`
	`clean:`
	`  rm -f $(PROGRAMS) $(PROGRAMS:%=%.c) $(PROGRAMS:%=%.o)`	

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Code.	Testen Sie den konvertierten Anwendungscode, um sicherzustellen, dass er ordnungsgemäß funktioniert.	App-Entwickler, App-Besitzer, Testingenieur

Zugehörige Ressourcen

- ECPG – Embedded SQL in C (PostgreSQL-Dokumentation)
- Fehlerbehandlung (PostgreSQL-Dokumentation)
- Warum den Oracle Pro*C/C++ Precompiler verwenden (Oracle-Dokumentation)

Zusätzliche Informationen

PostgreSQL verfügt über einen eingebetteten SQL-Precompiler, ECPG, der dem Oracle Pro*C-Precompiler entspricht. ECPG konvertiert C-Programme mit eingebetteten SQL-Anweisungen in Standard-C-Code, indem die SQL-Aufrufe durch spezielle Funktionsaufrufe ersetzt werden. Die Ausgabedateien können dann mit jeder C-Compiler-Toolkette verarbeitet werden.

Eingabe- und Ausgabedateien

ECPG konvertiert jede Eingabedatei, die Sie in der Befehlszeile angeben, in die entsprechende C-Ausgabedatei. Wenn ein Eingabedateiname keine Dateierweiterung hat, wird .pgc angenommen. Die Erweiterung der Datei wird durch ersetzt`.c`, um den Ausgabedateinamen zu erstellen. Sie können jedoch den Standardausgabedateinamen überschreiben, indem Sie die `-o` Option verwenden.

Wenn Sie einen Bindestrich (`-`) als Eingabedateinamen verwenden, liest ECPG das Programm aus der Standardeingabe und schreibt in die Standardausgabe, es sei denn, Sie überschreiben dies mit der`-o` Option .

Header-Dateien

Wenn der PostgreSQL-Compiler die vorverarbeiteten C-Codedateien kompiliert, sucht er im PostgreSQL-`include`Verzeichnis nach den ECPG-Header-Dateien. Daher müssen Sie möglicherweise die `-I` Option verwenden, um den Compiler auf das richtige Verzeichnis zu verweisen (z. B. `-I/usr/local/pgsql/include`).

Bibliotheken

Programme, die C-Code mit eingebettetem SQL verwenden, müssen mit der`libecpg` Bibliothek verknüpft werden. Sie können beispielsweise die Linker-Optionen verwenden `-L/usr/local/pgsql/lib -lecpg`.

Konvertierte ECPG-Anwendungen rufen Funktionen in der `libpq` Bibliothek über die eingebettete SQL-Bibliothek (`ecpglib`) auf und kommunizieren mit dem PostgreSQL-Server unter Verwendung des Standard-Frontend/Backend-Protokolls.

Migrieren von virtuell generierten Spalten von Oracle zu PostgreSQL

Erstellt von Veeranjaney Bol Grandhi (AWS), Rajesh Madiwale (AWS) und Ramesh Pathuri (AWS)

Umgebung: Produktion	Quelle: Oracle Database	Ziel: Amazon RDS für PostgreSQL oder Aurora PostgreSQL – kompatibel
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora; Amazon RDS; AWS DMS		

Übersicht

In Version 11 und früher bietet PostgreSQL keine Funktion, die direkt einer virtuellen Oracle-Spalte entspricht. Der Umgang mit virtuell generierten Spalten während der Migration von Oracle Database zu PostgreSQL Version 11 oder früher ist aus zwei Gründen schwierig:

- Virtuelle Spalten sind während der Migration nicht sichtbar.
- PostgreSQL unterstützt den `generate` Ausdruck vor Version 12 nicht.

Es gibt jedoch Problemumgehungen, um ähnliche Funktionen zu emulieren. Wenn Sie AWS Database Migration Service (AWS DMS) verwenden, um Daten von Oracle Database zu PostgreSQL Version 11 und früher zu migrieren, können Sie Auslöserfunktionen verwenden, um die Werte in virtuell generierten Spalten aufzufüllen. Dieses Muster enthält Beispiele für Oracle Database- und PostgreSQL-Code, den Sie für diesen Zweck verwenden können. Auf AWS können Sie Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL - kompatible Edition für Ihre PostgreSQL-Datenbank verwenden.

Ab PostgreSQL Version 12 werden generierte Spalten unterstützt. Generierte Spalten können entweder im laufenden Betrieb aus anderen Spaltenwerten berechnet oder berechnet und gespeichert werden. Von PostgreSQL generierte Spalten ähneln virtuellen Oracle-Spalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank
- Ziel-PostgreSQL-Datenbanken (auf Amazon RDS für PostgreSQL oder Aurora PostgreSQL – kompatibel)
- PL/pgSQL-Codierungswissen

Einschränkungen

- Gilt nur für PostgreSQL-Versionen vor Version 12.
- Gilt für Oracle Database Version 11g oder höher.
- Virtuelle Spalten werden in Datenmigrationstools nicht unterstützt.
- Gilt nur für Spalten, die in derselben Tabelle definiert sind.
- Wenn sich eine virtuell generierte Spalte auf eine deterministische benutzerdefinierte Funktion bezieht, kann sie nicht als Partitionierungsschlüsselspalte verwendet werden.
- Die Ausgabe des Ausdrucks muss ein skalarer Wert sein. Es kann keinen von Oracle bereitgestellten Datentyp, einen benutzerdefinierten Typ`LOB`, oder zurückgeben`LONG RAW`.
- Indizes, die anhand virtueller Spalten definiert sind, entsprechen funktionsbasierten Indizes in PostgreSQL .
- Tabellenstatistiken müssen gesammelt werden.

Tools

- pgAdmin 4 ist ein Open-Source-Verwaltungstool für PostgreSQL . Dieses Tool bietet eine grafische Oberfläche, die die Erstellung, Wartung und Verwendung von Datenbankobjekten vereinfacht.
- Oracle SQL Developer ist eine kostenlose, integrierte Entwicklungsumgebung für die Arbeit mit SQL in Oracle-Datenbanken in herkömmlichen und Cloud-Bereitstellungen.

Polen

Erstellen von Quell- und Zieldatenbanktabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Oracle-Datenbase-Quelltabelle.	Erstellen Sie in Oracle Database mithilfe der folgenden Anweisung eine Tabelle mit virtuell generierten Spalten. `CREATE TABLE test.generated_column ( CODE NUMBER, STATUS VARCHAR2(12) DEFAULT 'PreOpen', FLAG CHAR(1) GENERATED ALWAYS AS (CASE UPPER(STATUS) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) VIRTUAL VISIBLE );` In dieser Quelltabelle werden die Daten in der `STATUS` Spalte über AWS DMS zur Zieldatenbank migriert. Die `FLAG` Spalte wird jedoch mit `-generate by`Funktionen gefüllt, sodass diese Spalte während der Migration für AWS DMS nicht sichtbar ist. Um die Funktionalität von zu implementieren`generated by`, müssen Sie Auslöser und Funktionen in der Zieldatenbank verwenden, um die	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Werte in der FLAG Spalte zu füllen, wie im nächsten Epi dargestellt.	
Erstellen Sie eine PostgreSQ L-Zieltabelle in AWS.	Erstellen Sie eine PostgreSQ L-Tabelle in AWS mithilfe der folgenden Anweisung. `CREATE TABLE test.gene rated_column ( code integer not null, status character varying(12) not null , flag character(1) );` In dieser Tabelle ist die `status` Spalte eine Standardspalte. Bei der `flag` Spalte handelt es sich um eine generierte Spalte, die auf den Daten in der `status` Spalte basiert.	DBA, App-Entwickler

Erstellen einer Auslöserfunktion zur Verarbeitung der virtuellen Spalte in PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen PostgreSQ L-Auslöser.	Erstellen Sie in PostgreSQL einen Auslöser. `CREATE TRIGGER tgr_gen_c olumn`	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AFTER INSERT OR UPDATE OF status ON test.generated_column FOR EACH ROW EXECUTE FUNCTION test.tgf_gen_column();`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine PostgreSQL-Auslöserfunktion.	Erstellen Sie in PostgreSQL eine -Funktion für den -Auslöser. Diese Funktion füllt eine virtuelle Spalte aus, die von der Anwendung oder AWS DMS eingefügt oder aktualisiert wird, und validiert die Daten. `CREATE OR REPLACE FUNCTION test.tgf_gen_column() RETURNS trigger AS $VIRTUAL_COL$ BEGIN IF (TG_OP = 'INSERT') THEN IF (NEW.flag IS NOT NULL) THEN RAISE EXCEPTION 'ERROR: cannot insert into column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF (TG_OP = 'UPDATE') THEN IF (NEW.flag::VARCHAR != OLD.flag::varchar) THEN RAISE EXCEPTION 'ERROR: cannot update column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF;`	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`IF TG_OP IN ('INSERT' ,'UPDATE') THEN IF (old.flag is NULL) OR (coalesce(old.stat us,'') != coalesce(new.status,'')) THEN UPDATE test.gene rated_column SET flag = (CASE UPPER(status) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) WHERE code = new.code; END IF; END IF; RETURN NEW; END $VIRTUAL_COL$ LANGUAGE plpgsql;`	

Testen der Datenmigration mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikati ons-Instance.	Um eine Replikations-Insta nce zu erstellen, folgen Sie den Anweisungen in der AWS DMS-Dokumentation. Die Replikations-Instance sollte sich in derselben Virtual Private Cloud (VPC) wie Ihre Quell- und Zieldatenbanken befinden.	DBA, App-Entwickler
Erstellen Sie Quell- und Zielendpunkte.	Um die Endpunkte zu erstellen , folgen Sie den Anweisung	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en in der AWS DMS-Dokum entation.	
Testen Sie die Endpunktv erbindungen.	Sie können die Endpunktv erbindungen testen, indem Sie die VPC und die Replikations-Instance angeben und Test ausführen auswählen.	DBA, App-Entwickler
Erstellen und starten Sie eine Volllastaufgabe.	Anweisungen finden Sie unter Erstellen einer Aufgabe und Volllast-Aufgabene instellungen in der AWS DMS-Dokumentation.	DBA, App-Entwickler
Validieren Sie die Daten für die virtuelle Spalte.	Vergleichen Sie die Daten in der virtuellen Spalte in den Quell- und Zieldatenbanken. Sie können die Daten manuell validieren oder ein Skript für diesen Schritt schreiben.	DBA, App-Entwickler

Zugehörige Ressourcen

- Erste Schritte mit AWS Database Migration Service (AWS-DMS-Dokumentation)
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS (AWS DMS-Dokumentation)
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS (AWS DMS-Dokumentation)
- Generierte Spalten in PostgreSQL (PostgreSQL-Dokumentation)
- Trigger-Funktionen (PostgreSQL-Dokumentation)
- Virtuelle Spalten in Oracle Database (Oracle-Dokumentation)

Einrichten der Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL – kompatibel

Erstellt von Rakesh Raghav (AWS) und Anuradha Chitha (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: Aurora PostgreSQL
R-Typ: Neuarchitektur	Workload: Oracle	Technologien: Migration; Infrastruktur; Datenbanken
AWS-Services: Amazon S3; Amazon Aurora		

Übersicht

Im Rahmen Ihrer Migration von Oracle zu Amazon Aurora PostgreSQL – Kompatible Edition in der Amazon Web Services (AWS) Cloud können mehrere Herausforderungen auftreten. Beispielsweise ist die Migration von Code, der auf dem Oracle-`UTL_FILE`Dienstprogramm basiert, immer eine Herausforderung. In Oracle PL/SQL wird das `UTL_FILE` Paket für Dateioperationen wie Lesen und Schreiben in Verbindung mit dem zugrunde liegenden Betriebssystem verwendet. Das `UTL_FILE` Dienstprogramm funktioniert sowohl für Server- als auch für Client-Computersysteme.

Amazon Aurora PostgreSQL – kompatibel ist ein verwaltetes Datenbankangebot. Aus diesem Grund ist es nicht möglich, auf Dateien auf dem Datenbankserver zuzugreifen. Dieses Muster führt Sie durch die Integration von Amazon Simple Storage Service (Amazon S3) und Amazon Aurora PostgreSQL – kompatibel, um eine Teilmenge der `UTL_FILE` Funktionalität zu erreichen. Mit dieser Integration können wir Dateien erstellen und verwenden, ohne ETL-Tools (Extract, Transform, Load) oder -Services von Drittanbietern zu verwenden.

Optional können Sie die Amazon- CloudWatch Überwachung und Amazon SNS-Benachrichtigungen einrichten.

Wir empfehlen, diese Lösung gründlich zu testen, bevor Sie sie in einer Produktionsumgebung implementieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Database Migration Service (AWS DMS)-Erfahrung
- Bol in PL/pgSQL-Codierung
- Ein mit Amazon Aurora PostgreSQL kompatibler Cluster
- Ein S3-Bucket

Einschränkungen

Dieses Muster bietet nicht die Funktionalität, als Ersatz für das Oracle-`UTL_FILE`Dienstprogramm zu dienen. Die Schritte und der Beispielcode können jedoch weiter verbessert werden, um die Modernisierungsziele Ihrer Datenbank zu erreichen.

Produktversionen

- Amazon Aurora PostgreSQL – Kompatible Edition 11.9

Architektur

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL – kompatibel
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon S3

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Darstellung der Lösung.

1. Dateien werden von der Anwendung in den S3-Bucket hochgeladen.
2. Die `aws_s3` Erweiterung greift mithilfe von PL/pgSQL auf die Daten zu und lädt die Daten in Aurora PostgreSQL hoch – kompatibel.

Tools

- Amazon Aurora PostgreSQL – kompatibel – Amazon Aurora PostgreSQL – Kompatible Edition ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-kompatible relationale Datenbank-Engine. Es kombiniert die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Kosteneffizienz von Open-Source-Datenbanken.
- AWS CLI – Die AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services. Mit nur einem Tool zum Herunterladen und Konfigurieren können Sie mehrere AWS-Services über die Befehlszeile steuern und über Skripts automatisieren.
- Amazon CloudWatch – Amazon CloudWatch überwacht Amazon S3-Ressourcen und -Nutzung.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. In diesem Muster bietet Amazon S3 eine Speicherebene zum Empfangen und Speichern von Dateien für die Nutzung und Übertragung zum und vom Aurora PostgreSQL -kompatiblen Cluster.
- aws_s3 – Die `aws_s3` Erweiterung integriert Amazon S3 und Aurora PostgreSQL – kompatibel.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients. In diesem Muster wird Amazon SNS verwendet, um Benachrichtigungen zu senden.
- pgAdmin – pgAdmin ist ein Open-Source-Verwaltungstool für Postgres. pgAdmin 4 bietet eine grafische Oberfläche zum Erstellen, Verwalten und Verwenden von Datenbankobjekten.

Code

Um die erforderliche Funktionalität zu erreichen, erstellt das Muster mehrere Funktionen mit einer Benennung ähnlich wie `UTL_FILE`. Der Abschnitt Zusätzliche Informationen enthält die Codebasis für diese Funktionen.

Ersetzen Sie im Code durch `testaurorabucket` den Namen Ihres Test-S3-Buckets. Ersetzen Sie durch `us-east-1` die AWS-Region, in der sich Ihr S3-Test-Bucket befindet.

Polen

Integrieren von Amazon S3 und Aurora PostgreSQL – kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie IAM-Richtlinien ein.	Erstellen Sie AWS Identity and Access Management	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(IAM)-Richtlinien, die Zugriff auf den S3-Bucket und die darin enthaltenen Objekte gewähren. Den Code finden Sie im Abschnitt Zusätzliche Informationen.	
Fügen Sie Amazon S3-Zugriffsrollen zu Aurora PostgreSQL hinzu.	Erstellen Sie zwei IAM-Rollen: eine Rolle für den Lese- und eine Rolle für den Schreibzugriff auf Amazon S3. Fügen Sie die beiden Rollen an den Aurora PostgreSQL -kompatiblen Cluster an: • Eine Rolle für die S3Export-Funktion • Eine Rolle für die S3Import-Funktion Weitere Informationen finden Sie in der Aurora-PostgreSQL-kompatiblen Dokumentation zum Importieren und Exportieren von Daten nach Amazon S3.	AWS-Administrator, DBA

Einrichten der Erweiterungen in Aurora PostgreSQL – kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Erweiterung aws_commons.	Die `aws_commons` Erweiterung ist eine Abhängigkeit der `aws_s3` Erweiterung.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Erweiterung aws_s3.	Die `aws_s3` Erweiterung interagiert mit Amazon S3.	DBA, Entwickler

Validieren der mit Amazon S3 und Aurora PostgreSQL kompatiblen Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Import von Dateien aus Amazon S3 in Aurora PostgreSQL .	Um den Import von Dateien in Aurora PostgreSQL – kompatibel zu testen, erstellen Sie eine CSV-Beispieldatei und laden Sie sie in den S3-Bucket hoch. Erstellen Sie eine Tabellendefinition basierend auf der CSV-Datei und laden Sie die Datei mithilfe der `aws_s3.table_import_from_s3` Funktion in die Tabelle.	DBA, Entwickler
Testen Sie den Export von Dateien von Aurora PostgreSQL nach Amazon S3.	Um den Export von Dateien aus Aurora PostgreSQL – kompatibel zu testen, erstellen Sie eine Testtabelle, füllen Sie sie mit Daten auf und exportieren Sie dann die Daten mithilfe der `aws_s3.query_export_to_s3` Funktion .	DBA, Entwickler

Um das UTL_FILE-Dienstprogramm nachzuahmen, erstellen Sie Wrapper-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Schema utl_file_utility.	Das Schema hält die Wrapper-Funktionen zusammen. Führen Sie den folgenden Befehl aus, um das Schema zu erstellen. `CREATE SCHEMA utl_file_utility;`	DBA, Entwickler
Erstellen Sie den file_type-Typ.	Verwenden Sie den folgenden Code, um den `file_type` Typ zu erstellen. `CREATE TYPE utl_file_utility.file_type AS ( p_path character varying(30), p_file_name character varying );`	DBA/Entwickler
Erstellen Sie die Init-Funktion.	Die `init` Funktion initialisiert eine gemeinsame Variable wie `bucket` oder `region`. Den Code finden Sie im Abschnitt Zusätzliche Informationen.	DBA/Entwickler
Erstellen Sie die Wrapper-Funktionen.	Erstellen Sie die Wrapper-Funktionen `fopen`, `put_line`, und `fclose`. Code finden Sie im Abschnitt Zusätzliche Informationen.	DBA, Entwickler

Testen der Wrapper-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Wrapper-F unktionen im Schreibmodus.	Um die Wrapper-Funktionen im Schreibmodus zu testen, verwenden Sie den Code, der im Abschnitt Zusätzliche Informationen bereitgestellt wird.	DBA, Entwickler
Testen Sie die Wrapper-F unktionen im Append-Modus.	Um die Wrapper-Funktionen im Append-Modus zu testen, verwenden Sie den Code, der im Abschnitt Zusätzliche Informationen bereitgestellt wird.	DBA, Entwickler

Zugehörige Ressourcen

- Amazon S3-Integration
- Amazon S3
- Aurora
- Amazon CloudWatch
- Amazon SNS

Zusätzliche Informationen

Einrichten von IAM-Richtlinien

Erstellen Sie die folgenden Richtlinien.

Richtlinienname	JSON
S3IntRead	`{ "Version": "2012-10-17",`

```
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
         "arn:aws:s3:::testaurorabuc
ket/*",
         "arn:aws:s3:::testaurorabuc
ket"
            ]
        }
    ]
}
```

S3IntWrite

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",

                "s3:ListBucket"
            ],
            "Resource": [
    "arn:aws:s3:::testaurorabucket/
*",               "arn:aws:s3:::test
aurorabucket"
            ]
        }
    ]
}
```

Erstellen der Init-Funktion

Um allgemeine Variablen wie `bucket` oder zu initialisieren`region`, erstellen Sie die `init` Funktion mit dem folgenden Code.

```
CREATE OR REPLACE FUNCTION utl_file_utility.init(
    )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
BEGIN
      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 'region' )
      , 'us-east-1'::text
      , false );

      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 's3bucket' )
      , 'testaurorabucket'::text
      , false );
END;
$BODY$;
```

Erstellen der Wrapper-Funktionen

Erstellen Sie die `fopen`-`put_line`, - und -`fclose`Wrapper-Funktionen.

-Fopen

```
CREATE OR REPLACE FUNCTION utl_file_utility.fopen(
    p_file_name character varying,
    p_path character varying,
    p_mode character DEFAULT 'W'::bpchar,
    OUT p_file_type utl_file_utility.file_type)
    RETURNS utl_file_utility.file_type
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
declare
    v_sql character varying;
```

```
    v_cnt_stat integer;
    v_cnt integer;
    v_tabname character varying;
    v_filewithpath character varying;
    v_region character varying;
    v_bucket character varying;

BEGIN
    /*initialize common variable */
    PERFORM utl_file_utility.init();
    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    /* set tabname*/
    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;
    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region;

    /* APPEND MODE HANDLING; RETURN EXISTING FILE DETAILS IF PRESENT ELSE CREATE AN
 EMPTY FILE */
    IF p_mode = 'A' THEN
        v_sql := concat_ws('','create temp table if not exists ', v_tabname,' (col1
 text)');
        execute v_sql;

        begin
        PERFORM aws_s3.table_import_from_s3
            ( v_tabname,
            '',
            'DELIMITER AS ''#''',
            aws_commons.create_s3_uri
            (     v_bucket,
                v_filewithpath ,
                v_region)
            );
        exception
            when others then
             raise notice 'File load issue ,%',sqlerrm;
             raise;
        end;
        execute concat_ws('','select count(*) from ',v_tabname) into v_cnt;
```

```
        IF v_cnt > 0
        then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
        else
            PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
 v_region)
                             );

            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
        end if;
        v_sql := concat_ws('','drop table ', v_tabname);
        execute v_sql;
    ELSEIF p_mode = 'W' THEN
            PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
 v_region)
                             );
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
    END IF;

EXCEPTION
        when others then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
            raise notice 'fopenerror,%',sqlerrm;
            raise;
END;
$BODY$;
```

put_line

```
CREATE OR REPLACE FUNCTION utl_file_utility.put_line(
    p_file_name character varying,
    p_path character varying,
    p_line text,
    p_flag character DEFAULT 'W'::bpchar)
    RETURNS boolean
    LANGUAGE 'plpgsql'
```

```
    COST 100
    VOLATILE
AS $BODY$
/*****************************************************************************
* Write line, p_line in windows format to file, p_fp - with carriage return
* added before new line.
*****************************************************************************/
declare
    v_sql varchar;
    v_ins_sql varchar;
    v_cnt INTEGER;
    v_filewithpath character varying;
    v_tabname  character varying;
    v_bucket character varying;
    v_region character varying;

BEGIN
 PERFORM utl_file_utility.init();

/* check if temp table already exist */

 v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );

 v_sql := concat_ws('','select count(1) FROM pg_catalog.pg_class c LEFT JOIN
 pg_catalog.pg_namespace n ON n.oid = c.relnamespace where n.nspname like ''pg_temp_
%'''
                         ,' AND pg_catalog.pg_table_is_visible(c.oid) AND
 Upper(relname) = Upper( '''
                         ,  v_tabname ,''' ) ');

 execute v_sql into v_cnt;

  IF v_cnt = 0 THEN
        v_sql := concat_ws('','create temp table ',v_tabname,' (col text)');
       execute v_sql;
       /* CHECK IF APPEND MODE */
       IF upper(p_flag) = 'A' THEN
           PERFORM utl_file_utility.init();
           v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 'region' ) );
           v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 's3bucket' ) );
```

```
            /* set tabname*/
            v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

            begin
               PERFORM aws_s3.table_import_from_s3
                     ( v_tabname,
                          '',
                       'DELIMITER AS ''#''',
                        aws_commons.create_s3_uri
                           ( v_bucket,
                               v_filewithpath,
                               v_region    )
                     );
            exception
                when others then
                    raise notice  'Error Message : %',sqlerrm;
                    raise;
            end;
        END IF;
    END IF;
    /* INSERT INTO TEMP TABLE */
    v_ins_sql := concat_ws('','insert into ',v_tabname,' values(''',p_line,''')');
    execute v_ins_sql;
    RETURN TRUE;
    exception
            when others then
                raise notice  'Error Message : %',sqlerrm;
                raise;
END;
$BODY$;
```

fclose

```
CREATE OR REPLACE FUNCTION utl_file_utility.fclose(
    p_file_name character varying,
    p_path character varying)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
```

```
AS $BODY$
DECLARE
    v_filewithpath character varying;
    v_bucket character varying;
    v_region character varying;
    v_tabname character varying;
    v_sql character varying;
BEGIN
      PERFORM utl_file_utility.init();

    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region ;

    /* exporting to s3 */
    perform aws_s3.query_export_to_s3
        (concat_ws('','select * from ',v_tabname,'  order by ctid asc'),
            aws_commons.create_s3_uri(v_bucket, v_filewithpath, v_region)
        );
    v_sql := concat_ws('','drop table ', v_tabname);
    execute v_sql;
    RETURN TRUE;
EXCEPTION
       when others then
     raise notice 'error fclose %',sqlerrm;
     RAISE;
END;
$BODY$;
```

Testen Ihrer Einrichtungs- und Wrapper-Funktionen

Verwenden Sie die folgenden anonymen Codeblöcke, um Ihre Einrichtung zu testen.

Testen des Schreibmodus

Der folgende Code schreibt eine Datei mit dem Namen `s3inttest` im S3-Bucket.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'W';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Testen des Append-Modus

Der folgende Code hängt Zeilen an die `s3inttest` Datei an, die im vorherigen Test erstellt wurde.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'A';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;


select * from
```

```
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose : append 1', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket : for
 test purpose : append 2', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Amazon SNS-Benachrichtigungen

Optional können Sie die Amazon- CloudWatch Überwachung und Amazon SNS-Benachrichtigungen für den S3-Bucket einrichten. Weitere Informationen finden Sie unter Überwachen von Amazon S3 und Einrichten von Amazon SNS-Benachrichtigungen.

Validieren von Datenbankobjekten nach der Migration von Oracle zu Amazon Aurora PostgreSQL

Erstellt von Venkatramana Chintha (AWS) und Eduardoentim (AWS)

R-Typ: Neuarchitektur	Quelle: Relational	Ziel: Amazon Aurora PostgreSQL , Amazon RDS für PostgreSQL
Erstellt von: AWS	Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Migration
Workload: Oracle	AWS-Services: Amazon Aurora	

Übersicht

Dieses Muster beschreibt einen step-by-step Ansatz zur Validierung von Objekten nach der Migration einer Oracle-Datenbank zu Amazon Aurora PostgreSQL – kompatible Edition.

Dieses Muster beschreibt Nutzungsszenarien und Schritte für die Validierung von Datenbankobjekten. Ausführlichere Informationen finden Sie unter Validieren von Datenbankobjekten nach der Migration mit AWS SCT und AWS DMS im AWS Database Blog .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine On-Premises-Oracle-Datenbank, die zu einer Aurora-PostgreSQL-kompatiblen Datenbank migriert wurde.
- Anmeldeinformationen, für die die AmazonRDSDataFullAccess-Richtlinie angewendet wurde, für die Aurora-PostgreSQL-kompatible Datenbank.
- Dieses Muster verwendet den Abfrage-Editor für Aurora-Serverless-DB-Cluster, der in der Amazon Relational Database Service (Amazon RDS)-Konsole verfügbar ist. Sie können dieses Muster jedoch mit jedem anderen Abfrage-Editor verwenden.

Einschränkungen

- Oracle SYNONYM-Objekte sind in PostgreSQL nicht verfügbar, können aber teilweise über Ansichten oder SET search_path-Abfragen validiert werden.
- Der Amazon RDS-Abfrage-Editor ist nur in bestimmten AWS-Regionen und für bestimmte MySQL- und PostgreSQL-Versionen verfügbar.

Architektur

Tools

Tools

- Amazon Aurora PostgreSQL – Kompatible Edition – Aurora PostgreSQL – Kompatibilität ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-kompatible relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken kombiniert.
- Amazon RDS – Amazon Relational Database Service (Amazon RDS) erleichtert das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud. Dieser Service bietet kostengünstige und anpassbare Kapazität für eine Branchenstandards entsprechende relationale Datenbank sowie die Verwaltung gängiger Datenbankaufgaben.
- Abfrage-Editor für Aurora Severless – Der Abfrage-Editor hilft Ihnen, SQL-Abfragen in der Amazon-RDS-Konsole auszuführen. Sie können jede gültige SQL-Anweisung auf dem DB-Cluster von Aurora Serverless ausführen, einschließlich Datenmanipulation und Datendefinitionsanweisungen.

Um die Objekte zu validieren, verwenden Sie die vollständigen Skripts in der Datei „Objektvalidierungsskripte“ im Abschnitt „Anhänge“. Verwenden Sie die folgende Tabelle als Referenz.

Oracle-Objekt	Zu verwendendes Skript
Pakete	Abfrage 1
Tabellen	Abfrage 3

Ansichten	Abfrage 5
Sequenzen	Abfrage 7
Auslöser	Abfrage 9
Primärschlüssel	Abfrage 11
Indizes	Abfrage 13
Einschränkungen prüfen	Abfrage 15
Fremdschlüssel	Abfrage 17

PostgreSQL-Objekt	Zu verwendendes Skript
Pakete	Abfrage 2
Tabellen	Abfrage 4
Ansichten	Abfrage 6
Sequenzen	Abfrage 8
Auslöser	Abfrage 10
Primärschlüssel	Abfrage 12
Indizes	Abfrage 14
Einschränkungen prüfen	Abfrage 16
Fremdschlüssel	Abfrage 18

Polen

Validieren von Objekten in der Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierungsabfrage „Pakete“ in der Oracle-Quelldatenbank aus.	Laden Sie die Datei „Objektvalidierungsskripte“ herunter und öffnen Sie sie im Abschnitt „Anhänge“. Stellen Sie über Ihr Client-Programm eine Verbindung mit der Oracle-Quelldatenbank her. Führen Sie das Validierungsskript „Abfrage 1“ aus der Datei „Objektvalidierungsskripte“ aus. Wichtig: Geben Sie Ihren Oracle-Benutzernamen anstelle von „your_schema“ in die Abfragen ein. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Tabellen“ aus.	Führen Sie das Skript „Abfrage 3“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Ansichten“ aus.	Führen Sie das Skript „Abfrage 5“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierung der Anzahl der „Sequenzen“ aus.	Führen Sie das Skript „Abfrage 7“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Auslöser“ aus.	Führen Sie das Skript „Abfrage 9“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Primärschlüssel“ aus.	Führen Sie das Skript „Abfrage 11“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Indizes“ aus.	Führen Sie das Validieru ngsskript „Abfrage 13“ aus der Datei „Objektva lidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichn en.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Einschränkungen überprüfen“ aus.	Führen Sie das Skript „Abfrage 15“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validieru ngsabfrage „Fremdschlüssel“ aus.	Führen Sie das Validieru ngsskript „Abfrage 17“ aus der Datei „Objektva lidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichn en.	Entwickler, DBA

Validieren von Objekten in der Aurora PostgreSQL-kompatiblen Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe des Abfrage-Editors eine Verbindung mit der Aurora-PostgreSQL-kompatiblen Zieldatenbank her.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole. Wählen Sie oben rechts die AWS-Region aus, in der Sie die Aurora PostgreSQ L -kompatible Datenbank erstellt haben. Wählen Sie im Navigationsbereich „Datenban ken“ und dann die Aurora-PostgreSQL-kompatible Zieldatenbank aus. Wählen Sie unter „Aktionen“ die Option „Abfrage“ aus. Wichtig: Wenn Sie noch keine Verbindun g zur Datenbank hergestel lt haben, wird die Seite „Mit Datenbank verbinden “ geöffnet. Anschließend müssen Sie Ihre Datenbank informationen wie Benutzern ame und Passwort eingeben.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validieru ngsabfrage „Pakete“ aus.	Führen Sie das Skript „Abfrage 2“ aus der Datei „Objektvalidierungsskripte“ im Abschnitt „Anhänge“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Tabellen“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora-Po stgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Abfrage 4“ aus der Datei „Objektva lidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichn en.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Ansichten“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora-Po stgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Abfrage 6“ aus der Datei „Objektva lidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichn en.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierung der Anzahl der „Sequenzen“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora-PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Abfrage 8“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Auslöser“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora-PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Abfrage 10“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Primärschlüssel“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora-PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Abfrage 12“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierungsabfrage „Indizes“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora-PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Abfrage 14“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Einschränkungen überprüfen“ aus.	Führen Sie das Skript „Abfrage 16“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Fremdschlüssel“ aus.	Führen Sie das Validierungsskript „Abfrage 18“ aus der Datei „Objektvalidierungsskripte“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Vergleichen von Quell- und Zieldatenbank-Validierungsdatensätzen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergleichen und validieren Sie beide Abfrageergebnisse.	Vergleichen Sie die Abfrageergebnisse der Oracle- und Aurora-PostgreSQL-kompatiblen Datenbanken, um alle Objekte zu validieren. Wenn	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sie alle übereinstimmen, wurden alle Objekte erfolgrei ch validiert.	

Zugehörige Ressourcen

- Validieren von Datenbankobjekten nach einer Migration mit AWS SCT und AWS DMS
- Funktionen von Amazon Aurora: PostgreSQL – kompatible Edition

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erneut hosten

Themen

Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS

Erstellt von Ali Alzand

Umgebung: Produktion	Quelle: Microsoft-Workload, der entweder On-Premises oder andere Cloud-Serviceanbieter ausführt	Ziel: Amazon EC2 Windows
R-Typ: Hostwechsel	Workload: Microsoft	Technologien: Migration
AWS-Services: Amazon EC2		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie das PowerShell Modul Migration Validator Toolkit verwenden, um Ihre Microsoft-Workloads zu AWS zu erkennen und zu migrieren. Das Modul führt mehrere Prüfungen und Validierungen für häufige Aufgaben im Zusammenhang mit beliebigen Microsoft-Workloads durch. Das Modul sucht beispielsweise nach Instances, an die möglicherweise mehrere Festplatten angeschlossen sind, oder nach Instances, die viele IP-Adressen verwenden. Eine vollständige Liste der Prüfungen, die das Modul durchführen kann, finden Sie im Abschnitt Prüfungen auf der GitHub Seite des Moduls.

Das PowerShell Modul Migration Validator Toolkit kann Ihrer Organisation helfen, den Zeit- und Arbeitsaufwand zu reduzieren, der damit verbunden ist, zu ermitteln, welche Anwendungen und Services auf Ihren Microsoft-Workloads ausgeführt werden. Das Modul unterstützt Sie außerdem dabei, die Konfigurationen Ihrer Workloads zu identifizieren, sodass Sie herausfinden können, ob Ihre Konfigurationen auf AWS unterstützt werden. Das Modul bietet auch Empfehlungen für die nächsten Schritte und Abhilfemaßnahmen, sodass Sie Fehlkonfigurationen vor, während oder nach der Migration vermeiden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Lokales Administratorkonto

- PowerShell 4.0

Einschränkungen

- Funktioniert nur unter Microsoft Windows Server 2012 R2 oder höher

Tools

Tools

- PowerShell 4.0

Code-Repository

Das PowerShell Modul Migration Validator Toolkit für dieses Muster ist im GitHubRepository migration-validator-toolkit-for-microsoft-workloads verfügbar.

Polen

Führen Sie das PowerShell Modul Migration Validator Toolkit auf einem einzigen Ziel aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Modul herunter, extrahieren, importieren und rufen Sie es auf.	Wählen Sie eine der folgenden Methoden zum Herunterladen und Bereitstellen des Moduls aus: • Ausführen des PowerShell Skripts • Laden Sie die ZIP-Datei herunter und extrahieren Sie sie • Klonen des GitHub Repositorys	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Ausführen des PowerShell Skripts
	
	PowerShellFühren Sie in den folgenden Beispielcode aus:
	
	`#MigrationValidatorToolkit`
	`$uri = 'https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads/archive/refs/heads/main.zip'`
	`$destination = (Get-Location).Path`
	`if ((Test-Path -Path "$destination\MigrationValidatorToolkit.zip" -PathType Leaf) -or (Test-Path -Path "$destination\MigrationValidatorToolkit")) {`
	`write-host "File $destination\MigrationValidatorToolkit.zip or folder $destination\MigrationValidatorToolkit found, exiting"`
	`}else {`
	`Write-host "Enable TLS 1.2 for this PowerShell session only."`
	`[Net.ServicePointManager]::SecurityProtocol = [Net.Secu`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rityProtocolType]::Tls12 $webClient = New-Object System.Net.WebClient Write-host "Downloading MigrationValidatorToolkit.zip" $webClient.DownloadFile($uri, "$destination\MigrationValidatorToolkit.zip") Write-host "MigrationValidatorToolkit.zip download successfully" Add-Type -Assembly "system.io.compression.filesystem" [System.IO.Compression.ZipFile]::ExtractToDirectory("$destination\MigrationValidatorToolkit.zip","$destination\MigrationValidatorToolkit") Write-host "Extracting MigrationValidatorToolkit.zip complete successfully" Import-Module "$destination\MigrationValidatorToolkit\migration-validator-toolkit-for-microsoft-workloads-main\MigrationValidatorToolkit.psm1"; Invoke-MigrationValidatorToolkit	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>}</pre> Der Code lädt das Modul aus einer ZIP-Datei herunter. Anschließend extrahiert, importiert und ruft der Code das Modul auf. Laden Sie die ZIP-Datei herunter und extrahieren Sie sie 1. Laden Sie die ZIP-Datei herunter (Download). 2. Entpacken Sie die ZIP-Datei. 3. Führen Sie die Schritte in der Beschreibung Modul manuell aufrufen dieses Handbuchs aus. Klonen des GitHub Repositorys 1. Um das Repository GitHubmigration-validator-toolkit-for-microsoft-workloads zu klonen, führen Sie den folgenden Git-Befehl in einem Terminalfenster aus: <pre>git clone https://github.com/aws-samples/migration-validator-toolkit-for-</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`microsoft-workloads.git` 2. Führen Sie die Schritte in der Beschreibung Modul manuell aufrufen dieses Handbuchs aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie das Modul manuell auf.	1. Gehen Sie zu dem Verzeichnis, in dem das heruntergeladene Modul gespeichert ist.
	2. Um die Ausgabe Ihrer Wahl zu generieren, führen Sie einen der folgenden Befehle als Administrator in aus PowerShell:
	
	Format-Tabelle-Format:
	
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit`
	
	Formatlistenformat:
	
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -List`
	
	OutformatGridView:
	
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -GridView`
	
	ConvertTo-Csv-Format:
		Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -csv`	

Führen Sie das PowerShell Modul Migration Validator Toolkit auf mehreren Zielen aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die ZIP-Datei herunter oder klonen Sie das GitHub Repository.	Wählen Sie eine der folgenden Optionen: • Laden Sie die ZIP-Datei herunter. (Download). • Um das Repository GitHubmigration-validator-toolkit-for-microsoft-workloads zu klonen, führen Sie den folgenden Git-Befehl in einem Terminalfenster aus: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git`	Systemadministrator
Aktualisieren Sie die server.csv-Liste.	Wenn Sie die ZIP-Datei heruntergeladen haben, gehen Sie wie folgt vor: 1. Entpacken Sie die ZIP-Datei.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wechseln Sie zum Verzeichnis `Migration ValidatorToolkit\I nputs\ .` 3. Aktualisieren Sie `serverlist.csv` mit dem Hostnamen Ihrer Zielcomputer.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das Modul auf.	Sie können jeden Computer innerhalb der Domäne verwenden, der einen Domänenbenutzer verwendet , der Administratorzugriff auf Zielcomputer hat. 1. Laden Sie den Quellcode als ZIP-Datei herunter und extrahieren Sie die Datei. 2. PowerShellFühren Sie als Administrator in den folgenden Befehl aus: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-DomainComputers` Die CSV-Ausgabedatei wird in`MigrationValidatorToolkit\Outputs\folder` mit dem Präfixnamen gespeichert`DomainComputers_MigrationAutomations_YYYY-MM-DDTHH-MM-SS` .	Systemadministrator

Fehlerbehebung

Problem	Lösung
`MigrationValidatorToolkit` schreibt Informationen zu Ausführungen, Befehlen und	Sie können Protokolldateien manuell am folgenden Speicherort anzeigen:

Problem	Lösung
Fehlern in Protokolldateien auf dem laufenden Host.	1. Wechseln Sie zum Verzeichnis `Migration ValidatorToolkit\logs\ .` 2. Suchen Sie die Protokolldatei. Das Format des Protokolldateinamens lautet: `ComputerName_MigrationValid atorToolkit_YYYY-MM-SSTHH-MM-SS.log`

Zugehörige Ressourcen

- Optionen, Tools und bewährte Methoden für die Migration von Microsoft-Workloads zu AWS (AWS Prescriptive Guidance)
- Microsoft-Migrationsmuster (AWS Prescriptive Guidance)
- Kostenlose Cloud-Migrationsservices in AWS (AWS-Dokumentation)
- Vordefinierte Aktionen nach dem Start (Dokumentation zum Anwendungs-Marketing)

Zusätzliche Informationen

Häufig gestellte Fragen

Wo kann ich das PowerShell Modul Migration Validator Toolkit ausführen?

Sie können das Modul unter Microsoft Windows Server 2012 R2 oder höher ausführen.

Wann führe ich dieses Modul aus?

Wir empfehlen Ihnen, das Modul während der Assess-Phase der Migration auszuführen.

Ändert das Modul meine vorhandenen Server?

Nein. Alle Aktionen in diesem Modul sind schreibgeschützt.

Wie lange dauert es, bis das Modul ausgeführt wird?

Die Ausführung des Moduls dauert in der Regel 1–5 Minuten, hängt jedoch von der Ressourcenzuweisung Ihres Servers ab.

Welche Berechtigungen muss das Modul ausführen?

Sie müssen das Modul von einem lokalen Administratorkonto aus ausführen.

Kann ich das Modul auf physischen Servern ausführen?

Ja, solange das Betriebssystem Microsoft Windows Server 2012 R2 oder höher ist.

Wie führe ich das Modul in großem Umfang für mehrere Server aus?

Um das Modul auf mehreren Computern auszuführen, die einer Domain beigetreten sind, führen Sie die Schritte im PowerShell Modul Migration Validator Toolkit auf mehreren Zielen ausführen aus diesem Leitfaden aus. Verwenden Sie für Computer, die nicht mit einer Domain verbunden sind, einen Remote-Aufruf oder führen Sie das Modul lokal aus, indem Sie die Schritte im PowerShell Modul Migration Validator Toolkit ausführen auf einem einzigen Ziel-Epi dieses Handbuchs ausführen.

Automatisieren von Aktivitäten vor der Workload-Erfassung für AWS Managed Services unter Windows

Erstellt von Jacob Zhang (AWS), Calvin Yeh (AWS) und Dwayne Bordelon (AWS)

Code-Repository: GitHub	Umgebung: Produktion	Quelle: Windows Servers
Ziel: AWS Managed Services	R-Typ: Hostwechsel	Technologien: Migration
AWS-Services: AWS CloudFormation; AWS Managed Services ; AWS Systems Manager ; Amazon S3		

Übersicht

In der Amazon Web Services (AWS) Cloud verwendet AWS Managed Services (AMS) AMS Workload Ingest (WIGS), um vorhandene Workloads in eine von AMS verwaltete VPC zu verschieben. Dieses Muster beschreibt eine Lösung zur Automatisierung gängiger Aktivitäten vor der Workload-Erfassung, wie z. B. das Upgrade von .NET und Windows PowerShell und das Ausführen der von AMS verwalteten Windows-WIGS-Vorab-Erfassungsvalidierung. Das Muster bietet auch eine einheitliche Benutzeroberfläche für die Ausführungsergebnisse. Es verpackt ein AWS Systems Manager-Befehlsdokument, das die Aktivitäten vor der Sitzung ausführt, in eine AWS-CloudFormation Vorlage. Die Vorlage kann wiederholt bereitgestellt werden, ohne dass Zugriff auf Systems Manager selbst erforderlich ist oder mit Automatisierungen von AMS in Konflikt steht.

Geschäftshintergrund

Migrationen zu AMS erfordern die Bereitstellung neuer Amazon Elastic Compute Cloud (Amazon EC2)-Instances mit von AMS verwalteten Amazon Machine Images (AMIs), die AMS-Komponenten enthalten. Alle Workloads oder Anwendungen, die in vorhandenen Rechenzentren ausgeführt werden, müssen auf neuen EC2-Instances erneut bereitgestellt werden, die von diesen AMS-AMIs gestartet werden. Um die potenziell umfangreiche manuelle Arbeit während des Prozesses zu vermeiden, hat das AMS-Team den Workflow zur AMS-Workload-Erfassung (WIGS) erstellt, um Ihre benutzerdefinierten Images in AMS einzubinden.

Windows-Instances müssen einige Voraussetzungen erfüllen, bevor der WIGS-Prozess stattfindet. Windows- PowerShell Skripts werden normalerweise verwendet, um die erforderlichen Vorbereitungen durchzuführen (WIGS-Vorbereitung) und zu überprüfen, ob die Instances für WIGs bereit sind (WIGS-Vorab Für die Vorbereitungs- und Validierungsprozesse muss ein Techniker 15–30 Minuten auf jedem Server verbringen, sich nacheinander manuell anmelden und die Skripts ausführen.

Geschäftstreiber

Traditionell können Sie mit Systems Manager Betriebsaufgaben automatisieren, z. B. das Ausführen von Windows- PowerShell Skripts. Aufgrund erhöhter Risiken und häufiger Konflikte zwischen Automatisierungen von AMS und Automatisierungen der Benutzer gewährt AMS seinen Benutzern jedoch normalerweise keinen Zugriff auf Systems Manager.

Bei Massenmigrationen mit AWS Application Migration Service (AWS MGN) werden Windows-PowerShell Skripts in der`C:\Program Files (x86)\AWS Replication Agent\post_launch folder` normalerweise automatisch ausgeführt, wenn eine Test- oder Cutover-Instance gestartet wird. Wenn diese Skripts jedoch sofort während eines Instance-Starts ausgeführt werden, führen sie häufig Konflikte mit Automatisierungen von AMS. Infolgedessen schlägt der Start möglicherweise fehl, ohne die Ausführungsergebnisse bereitzustellen, die Sie zur Behebung des Fehlers benötigen.

Dieses Muster behebt diese Probleme und bietet eine funktionierende automatisierte Lösung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit AMS-Onboarding wurde abgeschlossen.
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket im AWS-Konto. Wenn es keinen S3-Bucket gibt, über den Sie die Kontrolle im Konto haben, verwenden Sie eine RFC (Request for Change), um einen zu erstellen.
- Die PreWIGs _CFN.json-Vorlage, die aus dem [ams-auto-prewigs-windows]Repository heruntergeladen wurde.
- Ein Server, auf den Sie dieses Muster anwenden, muss die folgenden Anforderungen erfüllen:
  - Führen Sie Windows Server 2012 oder höher aus.
  - Wird gestartet oder kann im Sandbox-VPC-Migrationssubnetz gestartet werden.

- Sie müssen einen AWS Systems Manager Agent (SSM Agent) installiert haben.
- Fügen Sie ein AWS Identity and Access Management (IAM)-Instance-Profil an. Das Instance-Profil muss über Berechtigungen zum Herunterladen von Dateien aus S3-Buckets im selben AWS-Konto verfügen. Ein Instance-Profil, das die oben genannten Anforderungen erfüllt, ist normalerweise bereits bei früheren Einrichtungsvorgängen einer Migration eingerichtet.
- Von AWS Systems Manager Fleet Manager aus sichtbar sein.

Einschränkungen

- Die Pre-WIGS-Aktivitäten variieren je nach Umgebung und Geschäftsanforderungen. Möglicherweise müssen Sie geringfügige Änderungen an diesem Muster vornehmen, um Ihren spezifischen Anforderungen gerecht zu werden.

Produktversionen

- Das Muster wurde mit Windows Server 2012, 2012 R2, 2016 und 2019 getestet. Es funktioniert theoretisch mit späteren Windows-Versionen. Sie funktioniert nicht mit früheren Windows-Versionen.

Architektur

Das Architekturdiagramm zeigt Folgendes:

1. Eine Sandbox-VPC mit einem Migrationssubnetz, das Server enthält, die nicht vorbereitet wurden.
2. Der S3-Bucket, der Skripts speichert, die von der CloudFormation Vorlage verwendet werden.
3. Die CloudFormation Vorlage stellt das Systems Manager-Befehlsdokument bereit. Der Prozess iteriert, bis die Schritte abgeschlossen sind.
4. Die Instances sind vorbereitet und RFCs für WIGS werden erstellt.
5. In der von AMS verwalteten VPC enthält das von AMS verwaltete Subnetz die Server nach der Workload-Erfassung.

Funktionsweise

- Dieses Muster ist in eine AWS- CloudFormation Vorlage verpackt, die wiederholbare Bereitstellungen von Infrastructure as Code (IaC) ermöglicht. Sie müssen diese Vorlage nur einmal für jedes AWS-Konto bereitstellen, das diese Automatisierung erfordert.
- Die Automatisierung wird auf alle EC2-Instances mit Tag-Schlüssel-AutoPreWIGs in dem AWS-Konto angewendet, in dem dieses Muster bereitgestellt wird. Wenn eine Amazon EC2-Windows-Instance mit dem Tag-Schlüssel AutoPreWIGs zum ersten Mal gestartet wird, führt die Automatisierung die folgenden Aufgaben aus.
  1. Aktualisiert Windows PowerShell auf Version 5.1 und .NET auf Version 4.5.2. Abhängig von den vorhandenen Windows- PowerShell und .NET-Versionen kann die Instance mehrmals neu gestartet werden. Nach jedem Neustart werden die Upgrades fortgesetzt, bis sie abgeschlossen sind. In diesem Schritt werden eingebetteter Code in der CloudFormation Vorlage verwendet, die von einem Windows- PowerShell Skript geändert wurde, sowie spezifische Systems Manager-Anleitungen zu Serverneustarts.
  2. Lädt von Amazon S3 herunter und führt ein Windows- PowerShell Skript aus, das Sie angepasst haben, um die Amazon EC2-Windows-Instance auf WIGS vorzubereiten. Weitere Informationen finden Sie im Abschnitt „Epics“.
  3. Installiert das Windows WIGS- PowerShell Validierungsmodul vor der Sitzung von AWS.
  4. Führt die Windows WIGS-Validierung vor der Sitzung aus und macht die Ergebnisse in Systems Manager State Manager sichtbar.

Tools

- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt. Sie können einen verwenden, der alle gewünschten AWS-Ressourcen und ihre Abhängigkeiten beschreibt, sodass Sie diese Ressourcen als Stack starten und konfigurieren können. Dieses Muster verwendet eine CloudFormation Vorlage, um die Bereitstellung der Ressourcen in diesem Muster zu automatisieren.
- AWS Managed Services – AWS Managed Services (AMS) ist ein Unternehmensservice, der die kontinuierliche Verwaltung Ihrer AWS-Infrastruktur ermöglicht. Änderungen an der Infrastruktur in einer AMS-Umgebung müssen über einen RFC vorgenommen werden.
- AWS Systems Manager – AWS Systems Manager (früher bekannt als SSM) ist ein AWS-Service, mit dem Sie Ihre Infrastruktur in AWS anzeigen und steuern können. Mit der Systems Manager-Konsole können Sie Betriebsdaten aus mehreren AWS-Services anzeigen und Betriebsaufgaben in Ihren AWS-Ressourcen automatisieren. Dieses Muster verwendet Systems Manager, um die Ausführungsergebnisse der Pre-WIGS-Aktivitäten auszuführen und anzuzeigen.

- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenweit führende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Dieses Muster verwendet Amazon S3, um die CloudFormation Vorlage und ein Windows- PowerShell Skript zu speichern, das heruntergeladen wird.

Polen

Erstellen eines benutzerdefinierten Windows- PowerShell Skripts zur Automatisierung zusätzlicher Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die erforderlichen Änderungen an den Servern entsprechend den Geschäfts anforderungen durch.	Wenn Sie Änderungen benötigen, die vor deren Aufnahme automatisch auf Ihre Server angewendet werden, erstellen Sie ein Windows- PowerShell Skript mit dem Namen `ingestion -prep.ps1` . Wichtig: Das Skript darf keine Anweisungen zum Neustarte n des Servers enthalten und darf keine Administratorrechte erfordern.	PowerShell Skripterstellung
Entfernen Sie Software, die von AMS nicht unterstützt wird.	AMS erfordert bestimmte Software, wie Antiviren anwendungen und VMware Tools, die entfernt werden, bevor WIGS ausgeführt wird. Fügen Sie die Deinstallation in das `ingestion-prep.ps1` Skript ein. Weitere Informati onen zu Software, die nicht	PowerShell Skripterstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unterstützt wird, finden Sie in der AWS-Dokumentation.	

Hochladen der CloudFormation Vorlage und des optionalen Windows- PowerShell Skripts in Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Ordner in S3.	Erstellen Sie in einem S3-Bucket in demselben AWS-Konto, in dem Sie dieses Muster bereitstellen, einen Ordner.	Allgemeines AWS
Laden Sie die Skripts hoch.	Laden Sie die `PreWIGs_CFN.json` CloudFormation Vorlage und das `ingestion-prep.ps1` Windows-PowerShell Skript, das Sie im vorherigen Epi erstellt haben, in den Amazon S3-Ordner hoch.	Allgemeines AWS

Bereitstellen des CloudFormation Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Änderungstyp aus.	Navigieren Sie zur AMS-Konsole, um einen RFC zu erstellen. Verwenden Sie den Änderungstyp Create Stack from CloudFormation (CFN) Template.	Allgemeines AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Ausführungsparameter für den Pfad zur CloudFormation Vorlage fest.	Erweitern Sie im Abschnitt Ausführungskonfiguration die Option Zusätzliche Konfiguration . Fügen Sie im Feld CloudFormation S3-Endpunkt der Vorlage die URL in die CloudFormation Vorlage ein.	Allgemeines AMS
Geben Sie den Pfad zum Amazon S3-Ordner an.	Verwenden Sie unter Parameter ScriptSource als Namen . Geben Sie für Wert den Pfad zum S3-Ordner ein, der die Windows-PowerShell Skripte enthält. Stellen Sie sicher, dass Sie die `https://xxx` URL anstelle des `s3://xxx` URI verwenden, und fügen Sie `/` am Ende ein.	Allgemeines AMS
Stellen Sie den Stack bereit.	Um den Stack bereitzustellen, wählen Sie Erstellen aus.	Allgemeines AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Skalieren Sie das RFC auf AMS Ops.	Das RFC muss manuell vom AMS Ops-Team implement iert werden, da es Systems Manager verwendet, um Ressourcen mit bereitzus tellen, und eine Sicherhei tsüberprüfung erfordert. Sobald Sie das RFC erstellt haben, wird es vom System automatisch abgelehnt. Wählen Sie das RFC aus und fügen Sie dem RFC eine Korrespondenz hinzu, die Bitte führen Sie manuell aus. Notieren Sie sich die RFC-ID und eskalieren Sie sie mit einer Serviceanfrage.	Allgemeines AMS

Anwenden der Automatisierung auf die Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das AutoPreWIGs-Tag zu Instances hinzu.	Notieren Sie sich die IDs aller Instances, auf die Sie diese Automatisierung anwenden möchten, und warten Sie mindestens 30 Minuten, bis die Instance die von AMS implementierten Automatis ierungen abgeschlossen hat. Senden Sie ein automatis iertes RFC, um das Tag mit AutoPreWIGs als Schlüssel und einer beliebigen Zeichenfo	Allgemeines AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lge, z. B. 1, als Wert hinzuzufügen. Die Automatisierung wird einige Minuten nach dem Hinzufügen des Tags angewendet.	
Überprüfen Sie die Automatisierungsergebnisse.	Öffnen Sie die Systems Manager-Konsole und wählen Sie State Manager aus. Wählen Sie die Zuordnungs-ID mit dem Namen AMS-PreWIG-Prep-and-Validation-Association aus. Auf der Registerkarte Ausführungsverlauf können Sie die Ergebnisse der Automatisierung sehen.	Allgemeines AMS
Beheben Sie vorhandene Fehler.	Wenn die Automatisierung fehlschlägt, wählen Sie ihre Ausführungs-ID aus. Sie können die Ausführungsergebnisse für jede EC2-Instance sehen. Um die Details für jeden Schritt der Automatisierung anzuzeigen, wählen Sie Ausgabe aus. Wenn ein bestimmter Schritt fehlschlägt, verwenden Sie die Informationen in den Abschnitten Ausgabe und Fehler, um das Problem zu diagnostizieren.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie das AutoPreWIGs-Tag.	Wichtig: Nachdem Sie die Fehler behoben haben, senden Sie einen automatisierten RFC, um das AutoPreWIGs-Tag zu entfernen. WIGS schlägt fehl, wenn Sie das Tag nicht entfernen.	Allgemeines AMS

Nehmen Sie die vorbereiteten Instances auf

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie RFCs für WIGS.	Nachdem die Instances für die Workload-Erfassung bereit sind, senden Sie die RFCs für WIGS.	Allgemeines AMS

Zugehörige Ressourcen

- AMS Workload Ingest (WIGS)
- Migrieren von Workloads: Validierung vor der Sitzung von Windows
- AWS Application Migration Service – Schnellstartanleitung
- Erste Schritte mit AWS CloudFormation
- Einrichten von AWS Systems Manager

Erstellen eines Genehmigungsprozesses für Firewall-Anforderungen während einer Hostwechsel-Migration zu AWS

Erstellt von Srikanth Rangavajhala (AWS)

R-Typ: Hostwechsel	Umgebung: Produktion	Technologien: Migration
Quelle: On-Premises	Ziel: AWS Cloud	

Übersicht

Wenn Sie AWS Application Migration Service oder Cloud Migration Factory in AWS für eine Hostwechsel-Migration in die Amazon Web Services (AWS) Cloud verwenden möchten, müssen Sie die TCP-Ports 443 und 1500 geöffnet lassen. In der Regel erfordert das Öffnen dieser Firewall-Ports die Genehmigung Ihres InfoSecTeams für Informationssicherheit ().

In diesem Muster wird der Prozess beschrieben, mit dem während einer Hostwechsel-Migration in die AWS Cloud eine Genehmigung eines Firewall-Antrags von einem - InfoSec Team erhalten wird. Sie können diesen Prozess verwenden, um Ablehnungen Ihrer Firewall-Anfrage durch das InfoSec Team zu vermeiden, was teuer und zeitaufwändig werden kann. Der Firewall-Anforderungsprozess umfasst zwei Überprüfungs- und Genehmigungsschritte zwischen AWS-Migrationsempfehlungen und -leitern, die mit Ihren InfoSec und Anwendungsteams zusammenarbeiten, um die Firewall-Ports zu öffnen.

Bei diesem Muster wird davon ausgegangen, dass Sie eine Hostwechsel-Migration mit AWS-Empfehlungen oder -Migrationswissenschaftlern aus Ihrer Organisation planen. Sie können dieses Muster verwenden, wenn Ihre Organisation nicht über ein Genehmigungsverfahren für die Firewall oder ein Genehmigungsformular für die Firewall-Anforderung verfügt. Weitere Informationen dazu finden Sie im Abschnitt Einschränkungen dieses Musters. Weitere Informationen zu den Netzwerkanforderungen für Application Migration Service finden Sie unter Netzwerkanforderungen in der Dokumentation zum Application Migration Service.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine geplante Hostwechsel-Migration mit AWS-Empfehlungen oder -Migrationswissenschaftlern aus Ihrer Organisation

- Der erforderliche Port und die IP-Informationen für die Migration des Stacks
- Vorhandene und zukünftige Architekturdiagramme
- Firewall-Informationen über die On-Premises- und Zielinfrastruktur, Ports und den zone-to-zone Datenverkehrsfluss
- Eine Checkliste zur Überprüfung von Firewall-Anforderungen (angefügt)
- Ein Firewall-Anforderungsdokument, das gemäß den Anforderungen Ihrer Organisation konfiguriert ist
- Eine Kontaktliste für die Firewall-Prüfer und Genehmiger, einschließlich der folgenden Rollen:
  - Firewall-Anforderungseinreichung – AWS-Migrationsexperten oder -herkunft. Der Sender der Firewall-Anfrage kann auch ein Migrationsspezialist aus Ihrer Organisation sein.
  - Firewall-Anforderungsprüfer – In der Regel ist dies der Single Point of Contact (SPOC) von AWS.
  - Genehmiger der Firewall-Anforderung – Ein InfoSec Teammitglied.

Einschränkungen

- Dieses Muster beschreibt einen generischen Genehmigungsprozess für Firewall-Anfragen. Die Anforderungen können je nach Organisation variieren.
- Stellen Sie sicher, dass Sie Änderungen an Ihrem Firewall-Anforderungsdokument verfolgen.

Die folgende Tabelle zeigt die Anwendungsfälle für dieses Muster.

Verfügt Ihre Organisation über einen bestehenden Firewall-Genehmigungsprozess?	Verfügt Ihre Organisation über ein vorhandenes Firewall-Anforderungsformular?	Vorgeschlagene Aktion
Ja	Ja	Arbeiten Sie mit AWS-Kundendienstmitarbeitern oder Ihren Migrationsmitarbeitern zusammen, um den Prozess Ihrer Organisation zu implementieren.
Nein	Ja	Verwenden Sie den Firewall-Genehmigungsprozess dieses Musters. Verwenden Sie

		entweder eine AWS-Herkunft oder einen Migrationsexperten aus Ihrer Organisation, um das Genehmigungsformular für die Firewall-Anfrage zu übermitteln.
Nein	Nein	Verwenden Sie den Firewall-Genehmigungsprozess dieses Musters. Verwenden Sie entweder eine AWS-Herkunft oder einen Migrationsexperten aus Ihrer Organisation, um das Genehmigungsformular für die Firewall-Anfrage zu übermitteln.

Architektur

Das folgende Diagramm zeigt die Schritte für den Genehmigungsprozess für Firewall-Anfragen.

Tools

Sie können microSD-Tools wie Palo Alto Networks oder verwendenSolarWinds, um Firewalls und IP-Adressen zu analysieren und zu validieren.

Polen

Analysieren der Firewall-Anforderung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die Ports und IP-Adressen.	Der Sender der Firewall-Anforderung führt eine erste Analyse durch, um die erforderlichen Firewall-Ports	AWS Cloud-Techniker, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und IP-Adressen zu verstehen . Nachdem dies abgeschlo ssen ist, fordert er Ihr InfoSec Team auf, die erforderlichen Ports zu öffnen und die IP-Adressen zuzuordnen.	

Validieren der Firewall-Anforderung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Firewall-Informationen.	Der AWS Cloud-Techniker plant ein Treffen mit Ihrem InfoSec Team. Während dieses Treffens untersucht und validiert der Techniker die Firewall-Anforderungsinform ationen. In der Regel ist der Sender der Firewall-Anforderung dieselbe Person wie der Anforderer der Firewall. Diese Validieru ngsphase kann basierend auf dem Feedback des Genehmigers iterativ werden, wenn etwas beobachtet oder empfohlen wird.	AWS Cloud-Techniker, Migrationsspezialist
Aktualisieren Sie das Firewall-Anforderungsdokument.	Nachdem das InfoSec Team sein Feedback geteilt hat, wird das Firewall-Anforderungsdokument bearbeitet, gespeichert und erneut hochgeladen. Dieses	AWS Cloud-Techniker, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokument wird nach jeder Iteration aktualisiert. Wir empfehlen Ihnen, dieses Dokument in einem versionsg esteuerten Speicherordner zu speichern. Das bedeutet, dass alle Änderungen nachverfo lgt und korrekt angewendet werden.	

Senden der Firewall-Anforderung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die Firewall-Anfrage.	Nachdem der Genehmiger der Firewall-Anforderung die Genehmigungsanforderung für die Firewall genehmigt hat, sendet der AWS Cloud-Tec hniker die Firewall-Anforderu ng. Die Anforderung gibt die Ports an, die geöffnet sein müssen, und IP-Adress en, die zum Zuordnen und Aktualisieren des AWS-Kontos erforderlich sind. Sie können Vorschläge machen oder Feedback geben, nachdem die Firewall-Anfrage eingereic ht wurde. Wir empfehlen Ihnen, diesen Feedback-Prozess zu automatisieren	AWS Cloud-Techniker, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und alle Änderungen über einen definierten Workflow-Mechanismus zu senden.	

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Aufnehmen und Migrieren von EC2-Windows-Instances in ein AWS Managed Services-Konto

Erstellt von Anil Kunapareddy (AWS) und Venkatramana Chintha (AWS)

Umgebung: Produktion	Quelle: VPC in AWS Cloud	Ziel: Von AWS Managed Services verwaltete VPC
R-Typ: Hostwechsel	Workload: Microsoft	Technologien: Migration; Betrieb; Sicherheit, Identität, Compliance; Cloudnativ
AWS-Services: AWS Managed Services		

Übersicht

Dieses Muster erklärt den step-by-step Prozess der Migration und Aufnahme von Windows-Instances von Amazon Elastic Compute Cloud (Amazon EC2) in ein Amazon Web Services (AWS) Managed Services (AMS)-Konto. AMS kann Ihnen helfen, die Instance effizienter und sicher zu verwalten. AMS bietet betriebliche Flexibilität, verbessert Sicherheit und Compliance und hilft Ihnen, die Kapazität zu optimieren und die Kosten zu senken.

Dieses Muster beginnt mit einer EC2-Windows-Instance, die Sie in ein Staging-Subnetz in Ihrem AMS-Konto migriert haben. Für diese Aufgabe stehen eine Vielzahl von Migrationsservices und Tools zur Verfügung, z. B. AWS Application Migration Service.

Um eine Änderung an Ihrer von AMS verwalteten Umgebung vorzunehmen, erstellen Sie eine Änderungsanfrage (RFC) für eine bestimmte Operation oder Aktion und senden sie. Mit einem AMS Workload Ingest (WIGS) RFC nehmen Sie die Instance in das AMS-Konto auf und erstellen ein benutzerdefiniertes Amazon Machine Image (AMI). Anschließend erstellen Sie die von AMS verwaltete EC2-Instance, indem Sie einen weiteren RFC senden, um einen EC2-Stack zu erstellen. Weitere Informationen finden Sie unter AMS Workload Ingest in der AMS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives, von AMS verwaltetes AWS-Konto
- Eine vorhandene Landing Zone
- Berechtigungen zum Vornehmen von Änderungen in der von AMS verwalteten VPC
- Eine Amazon EC2-Windows-Instance in einem Staging-Subnetz in Ihrem AMS-Konto
- Abschluss der allgemeinen Voraussetzungen für die Migration von Workloads mit AMS WIGS
- Abschluss der Windows-Voraussetzungen für die Migration von Workloads mit AMS WIGS

Einschränkungen

- Dieses Muster gilt für EC2-Instances, auf denen Windows Server ausgeführt wird. Dieses Muster gilt nicht für Instances, auf denen andere Betriebssysteme wie Linux ausgeführt werden.

Architektur

Quelltechnologie-Stack

Amazon EC2-Windows-Instance in einem Staging-Subnetz in Ihrem AMS-Konto

Zieltechnologie-Stack

Von AWS Managed Services (AMS) verwaltete Amazon EC2-Windows-Instance

Zielarchitektur

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können Amazon EC2 verwenden, um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können auf- oder abskalieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Managed Services (AMS) hilft Ihnen, effizienter und sicherer zu arbeiten, indem es die kontinuierliche Verwaltung Ihrer AWS-Infrastruktur ermöglicht, einschließlich Überwachung, Vorfallmanagement, Sicherheitsleitfäden, Patch-Unterstützung und Backup für AWS-Workloads.

Andere -Services

- PowerShell ist ein Microsoft-Automatisierungs- und Konfigurationsmanagementprogramm, das unter Windows, Linux und macOS ausgeführt wird.

Polen

Konfigurieren von Einstellungen auf der Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die DNS-Client-Einstellungen.	1. Öffnen Sie in der EC2-Quell-Instance die Eingabeaufforderung als Administrator, geben Sie ein `gpedit.msc` und drücken Sie dann die Eingabetaste. 2. Navigieren Sie im Editor für lokale Gruppenrichtlinien zu Computerkonfiguration , Administrative Vorlagen , Netzwerk , DNS-Client . 3. Wählen Sie für Primäres DNS-Suffix die Option Nicht konfiguriert aus. 4. Wählen Sie für Devolution des primären DNS-Suffixes die Option Nicht konfiguriert aus.	Migrationsingenieur
Ändern Sie die Windows Update-Einstellungen.	1. Navigieren Sie im Editor für lokale Gruppenrichtlinien zu Computerkonfiguration , Administrative Vorlagen , Windows-Komponenten , Windows-Aktualisierung .	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie für Den Speicherort des Microsoft-Update-Services angeben die Option Nicht konfiguriert aus. 3. Wählen Sie für Automatische Updates konfigurieren die Option Nicht konfiguriert aus. 4. Wählen Sie für Erkennungshäufigkeit automatischer Updates die Option Nicht konfiguriert aus. 5. Schließen Sie den Editor für lokale Gruppenrichtlinien.	
Aktivieren Sie die Firewall.	1. Öffnen Sie in der EC2-Quell-Instance die Eingabeaufforderung als Administrator, geben Sie ein `services.msc` und drücken Sie dann die Eingabetaste. 2. Aktivieren Sie in Windows-Services die Firewall . 3. Schließen Sie Windows-Services.	Migrationsingenieur

Vorbereiten der Instance auf AMS WIGS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Instance und bereiten Sie sie vor.	1. Erstellen Sie mithilfe eines Bastion-Hosts und lokaler	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anmeldeinformationen eine Remote Desktop Protocol (RDP)-Verbindung zur EC2-Instance im Staging-Subnetz. 2. Entfernen Sie alle Legacy-Software-, Antiviren software- und Backup-Lösungen, die in AMS nicht erforderlich sind.	

Reparieren Sie die Datei sppnp.dll.	1. Wechseln Sie zu `C:\Windows\System32\sppnp.dll` .
	2. Umbenennen `sppnp.dll` in `sppnp_old.dll` .
	3. Geben Sie unter Verwendung von -PowerShell und -Administratoranmeldeinformationen die folgenden Befehle ein:
	`dism /online /cleanup-image /restorehealth`
	`sfc /scannnow`
	4. Starten Sie die EC2-Windows-Instance neu.
		Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Pre-WIG-Validierungsskript aus.	1. Laden Sie die ZIP-Datei für die Validierung vor der Erweiterung von Windows WIGS (`windows-prewings-valication.zip`) aus Migrieren von Workloads herunter: Validierung vor der Erweiterung von Windows in der AMS-Dokumentation. 2. Führen Sie das Windows-Pre-WIG-Validierungsskript aus und überprüfen Sie die Ergebnisse. 3. Wenn die Validierung fehlschlägt, beheben Sie das Problem und führen Sie das Validierungsskript erneut aus, bis die Validierung erfolgreich ist.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das ausfallsi chere AMI.	Nachdem die Pre-WIG-V alidierung erfolgreich war, erstellen Sie wie folgt ein Pre-Insestion-AMI: 1. Wählen Sie Bereitstellung, Erweiterte Stack-Kom ponenten, AMI ,Erstellen aus. 2. Fügen Sie während der Erstellung ein Tag hinzu`Key=Name, Value=APPLICATION-ID_IngestReady` . 3. Warten Sie, bis das AMI erstellt wurde, bevor Sie fortfahren. Weitere Informationen finden Sie unter AMI | Erstellen in der AMS-Dokumentation.	Migrationsingenieur

Aufnehmen und Validieren der Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie das RFC, um den Workload-Erfassungs-Stack zu erstellen.	Senden Sie eine Änderungs anfrage (RFC), um die AMS-WIGS zu starten. Anweisung en finden Sie unter Workload Ingest Stack: Creating in der AMS-Dokumentation. Dadurch wird die Workload-	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erfassung gestartet und die gesamte für AMS erforderliche Software installiert, einschließlich Backup-Tools, Amazon EC2-Verwaltungssoftware und Antivirensoftware.	
Validieren Sie die erfolgreiche Migration.	Nachdem die Workload-Erfassung abgeschlossen ist, können Sie die AMS-verwaltete Instance und das AMS-verschachtelte AMI sehen. 1. Melden Sie sich bei der von AMS verwalteten Instance mit Domänenanmeldeinformationen an. 2. Validieren Sie die Domain, die beitritt, wie folgt: a. Klicken Sie im Windows Explorer mit der rechten Maustaste auf diesen PC und wählen Sie dann Eigenschaften aus. b. Vergewissern Sie sich im Abschnitt Gerätespezifikation, dass die Domain im vollständigen Gerätenamen angezeigt wird. 3. Validieren Sie die Quell- und Ziel-Festplattenlaufwerke.	Migrationsingenieur

Starten der Instance im AMS-Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie das RFC, um einen EC2-Stack zu erstellen.	1. Bereiten Sie mithilfe des AMS-verschachtelten AMI der Windows-Instance ein RFC für einen EC2-Stack vor, gemäß den Anweisungen unter Erstellen einer EC2-Stack-Instance in der AMS-Dokumentation. Geben Sie im EC2-Stack RFC alle Parameter an, einschließlich Servername, Tags, Ziel-VPC, Zielsubnetz, Instance-Typ, Zielsicherheitsgruppen, Aufnahme-AMI und Rolle. 2. Senden Sie das RFC für den EC2-Stack und warten Sie dann, bis die Instance erfolgreich erstellt wurde.	Migrationsingenieur

Zugehörige Ressourcen

AWS Prescriptive Guidance

- Automatisieren von Aktivitäten vor der Workload-Erfassung für AWS Managed Services unter Windows
- Automatisches Erstellen eines RFC in AMS mit Python

AMS-Dokumentation

- AMS-Workload-Erfassung
- Wie sich Ihre Ressource durch Migration ändert

- Migrieren von Workloads: Standardprozess

Marketingressourcen

- AWS Managed Services
- Häufig FAQs zu AWS Managed Services
- AWS Managed Services-Ressourcen
- AWS Managed Services-Funktionen

Migrieren Sie Db2 für LUW zu Amazon EC2, indem Sie den Protokoll-Versand verwenden, um die Ausfallzeit zu reduzieren

Erstellt von Feng Cai (AWS), Ambarish Satarkar (AWS) undrabh Sharma (AWS)

Umgebung: Produktion	Quelle: On-Premises-Db2 für Linux	Ziel: Db2 auf Amazon EC2
R-Typ: Hostwechsel	Workload: IBM	Technologien: Migration; Datenbanken
AWS-Services: AWS Direct Connect; Amazon EBS; Amazon EC2; Amazon S3; AWS Site-to-Site VPN		

Übersicht

Wenn Kunden ihre Workloads von IBM Db2 für LUW (Linux, UNIX und Windows) zu Amazon Web Services (AWS) migrieren, ist die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2) mit dem BYOL-Modell (Bring Your Own License) die schnellste Möglichkeit. Die Migration großer Datenmengen von On-Premises-Db2 zu AWS kann jedoch eine Herausforderung darstellen, insbesondere wenn das Ausfallfenster kurz ist. Viele Kunden versuchen, das Ausfallfenster auf weniger als 30 Minuten festzulegen, was der Datenbank selbst wenig Zeit bleibt.

Dieses Muster behandelt, wie eine Db2-Migration mit einem kurzen Ausfallfenster mithilfe des Transaktionsprotokoll-Versands durchgeführt wird. Dieser Ansatz gilt für Db2 auf einer Little-Endian-Linux-Plattform.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Db2-Instance, die auf EC2-Instances ausgeführt wird und den Layouts des On-Premises-Dateisystems entspricht

- Ein Amazon Simple Storage Service (Amazon S3)-Bucket, auf den die EC2-Instance zugreifen kann
- Eine AWS Identity and Access Management (IAM)-Richtlinie und -Rolle für programmgesteuerte Aufrufe an Amazon S3
- Synchronisierte Zeitzone und Systemuhren auf Amazon EC2 und dem On-Premises-Server
- Das On-Premises-Netzwerk, das über AWS Site-to-Site VPN oder AWS Direct Connect mit AWS verbunden ist

Einschränkungen

- Die On-Premises-Db2-Instance und Amazon EC2 müssen sich auf derselben Plattformfamilie befinden.
- Der On-Premises-Workload von Db2 muss protokolliert werden. Um jede nicht protokollierte Transaktion zu blockieren, legen Sie `blocknonlogged=yes` in der Datenbankkonfiguration fest.

Produktversionen

- Db2 für LUW Version 11.5.9 und höher

Architektur

Quelltechnologie-Stack

- Db2 unter Linux x86_64

Zieltechnologie-Stack

- Amazon EBS
- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- AWS Site-to-Site VPN oder Direct Connect

Zielarchitektur

Das folgende Diagramm zeigt eine Db2-Instance, die On-Premises mit einer Virtual Private Network (VPN)-Verbindung zu Db2 auf Amazon EC2 ausgeführt wird. Die gepunkteten Linien stellen den VPN-Tunnel zwischen Ihrem Rechenzentrum und der AWS Cloud dar.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Block Store (Amazon EBS) stellt Volumes für die Speicherung auf Blockebene für die Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2)-Instances bereit.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Mit AWS Site-to-Site VPN können Sie Datenverkehr zwischen Instances, die Sie in AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleiten.

Andere Tools

- db2cli ist der interaktive Db2-CLI-Befehl.

Bewährte Methoden

- Verwenden Sie in der Zieldatenbank Gateway-Endpunkte für Amazon S3, um auf das Datenbank-Backup-Image und die Protokolldateien in Amazon S3 zuzugreifen.

- Verwenden Sie in der Quelldatenbank AWS PrivateLink für Amazon S3, um das Datenbank-Backup-Image und die Protokolldateien an Amazon S3 zu senden.

Polen

Festlegen von Umgebungsvariablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Umgebungs variablen fest.	Dieses Muster verwendet die folgenden Namen: • Instance-Name: `db2inst1` • Datenbankname: `SAMPLE` Sie können sie an Ihre Umgebung anpassen.	DBA

Konfigurieren des On-Premises-Db2-Servers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Einrichten des AWS CLI.	Führen Sie die folgenden Befehle aus, um die neueste Version der AWS CLI herunterzuladen und zu installieren:
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie ein lokales Ziel für Db2-Archivprotokolle ein.	Um die Zieldatenbank auf Amazon EC2 mit der On-Premises-Quelldatenbank synchron zu halten, müssen die neuesten Transakti onsprotokolle von der Quelle abgerufen werden.
	
	In dieser Einrichtung `/db2logs` wird von `LOGARCHMETH2` auf der Quelle als Staging-Bereich festgelegt. Die archivier ten Protokolle in diesem Verzeichnis werden in Amazon S3 synchronisiert und Db2 auf Amazon EC2 greift darauf zu. Das Muster verwendet , `LOGARCHME TH2` da `LOGARCHMETH1` möglicherweise für die Verwendung eines Drittanbi eter-Tools konfiguriert wurde, auf das der AWS CLI-Befehl nicht zugreifen kann. Führen Sie den folgenden Befehl aus, um die Protokolle abzurufen:
	
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHME TH2 disk:/db2logs`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie ein Online-Datenbank-Backup aus.	Führen Sie ein Online-Datenbank-Backup aus und speichern Sie es im lokalen Sicherungsdateisystem: `db2 backup db sample online to /backup`	DBA

Einrichten des S3-Buckets und der IAM-Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für den On-Premises-Server, an den die Db2-Sicherungsabbilder und Protokolldateien in AWS gesendet werden sollen. Auf den Bucket wird auch Amazon EC2 zugreifen: `aws s3api create-bucket --bucket logshipmig-db2 --region us-east-1`	AWS-Systemadministrator
Erstellen Sie eine IAM-Richtlinie.	Die `db2bucket.json` Datei enthält die IAM-Richtlinie für den Zugriff auf den Amazon S3-Bucket: `{ "Version": "2012-10-17", "Statement": [ {`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Effect": "Allow", "Action": ["kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts"], "Resource": ["arn:aws:s3:::logshipmig-db2/*", "arn:aws:s3:::logshipmig-db2"] }] }	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Verwenden Sie den folgenden AWS CLI-Befehl, um die Richtlinie zu erstellen:
	`aws iam create-policy \ --policy-name db2s3policy \ --policy-document file://db2bucket.json`
	Die JSON-Ausgabe zeigt den Amazon-Ressourcennamen (ARN) für die Richtlinie, wobei Ihre Konto-ID `aws_account_id` darstellt:
	`"Arn": "arn:aws:iam::aws_account_id:policy/db2s3policy"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie die IAM-Richtlinie an die IAM-Rolle an, die von der EC2-Instance verwendet wird.	In den meisten AWS-Umgebungen hat eine ausgeführte EC2-Instance eine IAM-Rolle, die von Ihrem Systemadministrator festgelegt wurde. Wenn die IAM-Rolle nicht festgelegt ist, erstellen Sie die Rolle und wählen Sie IAM-Rolle ändern in der EC2-Konsole aus, um die Rolle der EC2-Instance zuzuordnen, die die Db2-Datenbank hostet. Hängen Sie die IAM-Richtlinie mit dem Richtlinien-ARN an die IAM-Rolle an: `aws iam attach-role-policy \ --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3policy" \ --role-name db2s3role` Nachdem die Richtlinie angefügt wurde, kann jede EC2-Instance, die der IAM-Rolle zugeordnet ist, auf den S3-Bucket zugreifen.	AWS-Administrator, AWS-Systemadministrator

Senden des Quelldatenbank-Sicherungs-Images und der Protokolldateien an Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die AWS CLI auf dem On-Premises-Db2-Server.	Konfigurieren Sie die AWS CLI mit dem `Access Key ID` und , die im vorherigen Schritt `Secret Access Key` generiert wurden:
	`$ aws configure`
	`AWS Access Key ID [None]: **********`
	`AWS Secret Access Key [None]: ********** **********`
	`Default region name [None]: us-east-1`
	`Default output format [None]: json`
		AWS-Administrator, AWS-Systemadministrator

Senden Sie das Backup-Image an Amazon S3.	Zuvor wurde ein Online-Datenbank-Backup im `/backup` lokalen Verzeichnis gespeichert. Um dieses Backup-Image an den S3-Bucket zu senden, führen Sie den folgenden Befehl aus: `aws s3 sync /backup s3://logshipmig-db2/SAMPLE_backup`	AWS-Administrator, Migrationsingenieur
Senden Sie die Db2-Archivprotokolle an Amazon S3.	Synchronisieren Sie die lokalen Db2-Archivprotokolle mit dem S3-Bucket, auf den die Db2-Ziel-Instance auf Amazon EC2 zugreifen kann:	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws s3 sync /db2logs s3://logshipmig-db2/SAMPLE_LOG` Führen Sie diesen Befehl regelmäßig mit Cron oder anderen Planungstools aus. Die Häufigkeit hängt davon ab, wie oft die Quelldatenbank Transaktionsprotokolldateien archiviert.	

Verbinden Sie Db2 auf Amazon EC2 mit Amazon S3 und starten Sie die Datenbanksynchronisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen PKCS12-Keystore.	Db2 verwendet einen Public-Key Cryptography Standards (PKCS)-Verschlüsselungsschlüsselspeicher, um den AWS-Zugriffsschlüssel sicher zu halten. Erstellen Sie einen Keystore und konfigurieren Sie die Db2-Quell-Instance für deren Verwendung:
	
	`gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`
	
	`db2 "update dbm cfg using keystore_location /home/db2`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Erstellen Sie den Db2-Speicherzugriffsalias.	Verwenden Sie die folgende Skriptsyntax, um den Speicherzugriffsalias zu erstellen:
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	
	Ihr Skript könnte beispielsweise wie folgt aussehen:
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'logshipmig-db2'"`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie den Staging-Bereich fest.	Standardmäßig verwendet Db2 `DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH` als Staging-Bereich zum Hochladen und Herunterladen von Dateien zu und von Amazon S3. Der Standardpfad befindet sich `sqllib/tmp/RemoteStorage.xxxx` unter dem Instance-Stammverzeichnis, wobei auf die Db2-Partitionsnummer `xxxx` verweist. Beachten Sie, dass der Staging-Bereich über genügend Kapazität verfügen muss, um die Backup-Images und Protokolldateien zu speichern. Sie können die Registrierung verwenden, um den Staging-Bereich in ein anderes Verzeichnis zu verweisen. Wir empfehlen außerdem, `DB2_ENABLE_COS_SDK=ON` , und den Link zur `awssdk` Bibliothek zu verwenden`DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , um den Amazon S3-Stagingbereich für Datenbanksicherung und -wiederherstellung zu umgehen:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`Db2set DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`
	`db2stop`
	`db2start`	

Stellen Sie die Datenbank aus dem Backup-Image wieder her.	Stellen Sie die Zieldatenbank auf Amazon EC2 aus dem Backup-Image im S3-Bucket wieder her: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup replace existing`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie ein Roll-Forward für die Datenbank aus.	Nachdem die Wiederher stellung abgeschlossen ist, wird die Zieldatenbank in den Rollforward-Status „Ausstehe nd“ versetzt. Konfigurieren Sie `LOGARCHMETH1` und `LOGARCHMETH2` so, dass Db2 weiß, wo die Transakti onsprotokolldateien abgerufen werden sollen:
	`db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/' db2 update db cfg for SAMPLE using LOGARCHME TH2 OFF`
	Starten Sie das Datenbank-Rollforward:
	`db2 ROLLFORWARD DATABASE sample to END OF LOGS`
	Dieser Befehl verarbeitet alle Protokolldateien, die in den S3-Bucket übertrage n wurden. Führen Sie sie regelmäßig basierend auf der Häufigkeit des `s3 sync` Befehls auf den On-Premis es-Db2-Servern aus. Wenn beispielsweise stündlich `s3 sync` ausgeführt wird und es
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10 Minuten dauert, bis alle Protokolldateien synchronisiert sind, legen Sie fest, dass der Befehl 10 Minuten nach jeder Stunde ausgeführt wird.	

Bringen Sie Db2 auf Amazon EC2 während des Cutover-Fensters online

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bringen Sie die Zieldatenbank online.	Führen Sie während des Cutover-Fensters einen der folgenden Schritte aus:
	• Platzieren Sie die On-Premises-Datenbank in und führen Sie den `s3 sync` Befehl aus`ADMIN MODE`, um die Archivierung des letzten Transaktionsprotokolls zu erzwingen.
	• Fahren Sie die Datenbank herunter.
	
	Nachdem das letzte Transakti onsprotokoll mit Amazon S3 synchronisiert wurde, führen Sie den `ROLLFORWARD` Befehl zum letzten Mal aus:
	`db2 rollforward DB sample to END OF LOGS`
	`db2 rollforward DB sample complete`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Rollforward Status .... Rollforward status = not pending .... DB20000I The ROLLFORWARD command completed successfully.`
	
	`db2 activate db sample DB20000I The ACTIVATE DATABASE command completed successfully.`
	
	Bringen Sie die Zieldatenbank online und verweisen Sie die Anwendungsverbindungen zu Db2 auf Amazon EC2.	

Fehlerbehebung

Problem	Lösung
Wenn mehrere Datenbanken denselben Instance-Namen und Datenbanknamen auf verschiedenen Hosts (DEV, QA, PROD) haben, können Backups und Protokolle in dasselbe Unterverzeichnis gehen.	Verwenden Sie verschiedene S3-Buckets für DEV, QA und PROD und fügen Sie den Hostnamen als Unterverzeichnispräfix hinzu, um Verwechslungen zu vermeiden.
Wenn sich mehrere Backup-Images am selben Speicherort befinden, erhalten Sie bei der Wiederherstellung die folgende Fehlermeldung:	Fügen Sie im `restore` Befehl den Zeitstempel des Backups hinzu:

Problem	Lösung
`SQL2522N More than one backup file matches the time stamp value provided for the backed up database image.`	`db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup taken at 20230628164042 replace existing`

Zugehörige Ressourcen

- Db2-Backup- und Wiederherstellungsvorgänge zwischen verschiedenen Betriebssystemen und Hardwareplattformen
- Einrichten von Db2 STORAGE ACCESS ALIAS und DB2REMOTE
- Db2-Befehl ROLLFORWARD
- Sekundäre Db2-Protokollarchivierungsmethode

Migrieren Sie Db2 für LUW zu Amazon EC2 mit Notfallwiederherstellung für hohe Verfügbarkeit

Erstellt von Feng Cai (AWS), Aruna Gangireddy (AWS) und Venkatesan Govindan (AWS)

Umgebung: Produktion	Quelle: IBM Db2 für LUW On-Premises	Ziel: Db2 auf Amazon EC2
R-Typ: Hostwechsel	Workload: IBM	Technologien: Migration ; Datenbanken; Betriebss ysteme
AWS-Services: AWS Direct Connect; Amazon EC2; Amazon S3; AWS Site-to-Site VPN		

Übersicht

Wenn Kunden ihren IBM Db2 LUW (Linux, UNIX und Windows)-Workload zu Amazon Web Services (AWS) migrieren, ist die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2) mit dem BYOL-Modell (Bring Your Own License) die beste Möglichkeit. Die Migration großer Datenmengen von On-Premises-Db2 zu AWS kann jedoch eine Herausforderung darstellen, insbesondere wenn das Ausfallfenster kurz ist. Viele Kunden versuchen, das Ausfallfenster auf weniger als 30 Minuten festzulegen, was der Datenbank selbst wenig Zeit gibt.

Dieses Muster behandelt, wie Sie eine Db2-Migration mit einem kurzen Ausfallfenster mithilfe von Db2 High Availability Disaster Recovery (HADR) durchführen. Dieser Ansatz gilt für Db2-Datenbanken, die sich auf der Little-Endian-Linux-Plattform befinden und keine Data Partitioning Feature (DPF) verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Eine Db2-Instance, die auf einer Amazon EC2-Instance ausgeführt wird und den Layouts des On-Premises-Dateisystems entspricht
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket, auf den die EC2-Instance zugreifen kann
- Eine AWS Identity and Access Management (IAM)-Richtlinie und -Rolle für programmgesteuerte Aufrufe an Amazon S3
- Synchronisierte Zeitzone und Systemuhren auf Amazon EC2 und dem On-Premises-Server
- Das On-Premises-Netzwerk, das über AWS Site-to-Site VPN oder AWS Direct Connect mit AWS verbunden ist
- Kommunikation zwischen dem On-Premises-Server und Amazon EC2 über HADR-Ports

Einschränkungen

- Die On-Premises-Db2-Instance und Amazon EC2 müssen sich auf derselben Plattformfamilie befinden.
- HADR wird in einer partitionierten Datenbankumgebung nicht unterstützt.
- HADR unterstützt nicht die Verwendung von unformatierten E/A (direkter Festplattenzugriff) für Datenbankprotokolldateien.
- HADR unterstützt keine Endlosprotokollierung.
- `LOGINDEXBUILD` muss auf gesetzt sein`YES`, was die Protokollnutzung für die Neuerstellung des Index erhöht.
- Der On-Premises-Workload von Db2 muss protokolliert werden. Legen Sie `blocknonlogged=yes` in der Datenbankkonfiguration fest, um alle nicht protokollierten Transaktionen zu blockieren.

Produktversionen

- Db2 für LUW Version 11.5.9 und höher

Architektur

Quelltechnologie-Stack

- Db2 unter Linux x86_64

Zieltechnologie-Stack

- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- AWS Site-to-Site-VPN

Zielarchitektur

Im folgenden Diagramm wird Db2 On-Premises auf `db2-server1` als primär ausgeführt. Es hat zwei HADR-Standby-Ziele. Ein Standby-Ziel ist On-Premises und optional. Das andere Standby-Ziel, `db2-ec2`, befindet sich auf Amazon EC2. Nachdem die Datenbank auf AWS umgestellt wurde, `db2-ec2` wird zur primären Datenbank.

1. Protokolle werden von der primären On-Premises-Datenbank zur On-Premises-Standby-Datenbank gestreamt.
2. Mit Db2 HADR werden Protokolle von der primären On-Premises-Datenbank über Site-to-Site VPN zu Db2 auf Amazon EC2 gestreamt.
3. Db2-Backup- und Archivprotokolle werden von der primären On-Premises-Datenbank an den S3-Bucket in AWS gesendet.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Mit AWS Site-to-Site VPN können Sie Datenverkehr zwischen Instances, die Sie in AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleiten.

Andere Tools

- db2cli ist der interaktive Db2-CLI-Befehl.

Bewährte Methoden

- Verwenden Sie in der Zieldatenbank Gateway-Endpunkte für Amazon S3, um auf das Datenbank-Backup-Image und die Protokolldateien in Amazon S3 zuzugreifen.
- Verwenden Sie in der Quelldatenbank AWS PrivateLink für Amazon S3, um das Datenbank-Backup-Image und die Protokolldateien an Amazon S3 zu senden.

Polen

Festlegen von Umgebungsvariablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Umgebungs variablen fest.	Dieses Muster verwendet die folgenden Namen und Ports: 1. On-Premises-Hostname für Db2: `db2-server1` 2. HADR-Standby-Hostname: `db2-server2` (wenn HADR derzeit On-Premises ausgeführt wird) 3. Amazon EC2-Hostname: `db2-ec2` 4. Instance-Name: `db2inst1`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Datenbankname: `SAMPLE` 6. HADR-Ports: • `db2-server1: 50010` • `db2-server2: 50011` • `db2-ec2: 50012` Sie können sie an Ihre Umgebung anpassen.	

Konfigurieren des On-Premises-Db2-Servers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie AWS CLI ein.	Führen Sie die folgenden Befehle aus, um die neueste Version von AWS CLI herunterzuladen und zu installieren:
	
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Linux-Administrator

Richten Sie ein lokales Ziel für Db2-Archivprotokolle ein.	Bedingungen wie umfangreiche Update-Batch-Aufträge und Netzwerkverlangsamungen können dazu führen, dass der HADR-Standby-Server eine Verzögerung hat. Um aufzuholen, benötigt der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standby-Server die Transakti onsprotokolle vom primären Server. Die Reihenfolge der Stellen, an denen Protokolle angefordert werden sollen, ist wie folgt: • Das aktive Protokoll verzeichnis auf dem primären Server • Der `LOGARCHMETH2` Speicherort `LOGARCHME TH1` oder auf dem Standby-Server • Der - `LOGARCHMETH1` oder -`LOGARCHMETH2` Speichero rt auf dem primären Server In diesem Setup `/db2logs` wird von `LOGARCHMETH2` auf der Quelle als Staging-Bereich festgelegt. Die archivierten Protokolle in diesem Verzeichnis werden in Amazon S3 synchronisiert und Db2 auf Amazon EC2 greift darauf zu. Das Muster verwendet , `LOGARCHME TH2` da `LOGARCHMETH1` möglicherweise für die Verwendung eines Drittanbi eter-Tools konfiguriert wurde, auf das der AWS CLI-Befehl nicht zugreifen kann:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`db2 connect to sample` `db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	
Führen Sie ein Online-Datenbank-Backup aus.	Führen Sie eine Online-Datenbanksicherung aus und speichern Sie sie im lokalen Sicherungsdateisystem: `db2 backup db sample online to /backup`	DBA

Einrichten des S3-Buckets und der IAM-Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für den On-Premises-Server, an den die Db2-Sicherungsabbilder und Protokolldateien in AWS gesendet werden sollen. Auf den Bucket wird von Amazon EC2 zugegriffen: `aws s3api create-bucket --bucket hadrmig-db2 --region us-east-1`	AWS-Administrator
Erstellen Sie eine IAM-Richtlinie.	Die `db2bucket.json` Datei enthält die IAM-Richtlinie für den Zugriff auf den S3-Bucket: `{`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts"], "Resource": ["arn:aws:s3:::hadrmig-db2/*", "arn:aws:s3:::hadrmig-db2"] }]</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>}</pre>
	Verwenden Sie den folgenden AWS CLI-Befehl, um die Richtlinie zu erstellen:
	<pre>aws iam create-policy \
	      --policy-name
	 db2s3hapolicy \
	      --policy-document
	 file://db2bucket.j
	son</pre>
	Die JSON-Ausgabe zeigt den Amazon-Ressourcennamen (ARN) für die Richtlinie, wobei Ihre Konto-ID `aws_accou nt_id` darstellt:
	<pre>"Arn": "arn:aws:
	iam::aws_account_i
	d:policy/db2s3hapo
	licy"</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die IAM-Richtlinie an die IAM-Rolle an.	Normalerweise würde der EC2-Instance mit Db2 eine IAM-Rolle vom Systemadm inistrator zugewiesen. Wenn keine IAM-Rolle zugewiesen ist, können Sie in der Amazon EC2-Konsole IAM-Rolle ändern auswählen. Hängen Sie die IAM-Richt linie an die IAM-Rolle an, die der EC2-Instance zugeordne t ist. Nachdem die Richtlini e angefügt wurde, kann die EC2-Instance auf den S3-Bucket zugreifen: `aws iam attach-role-policy --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3hapolicy" --role-name db2s3harole`	

Senden des Quelldatenbank-Backup-Images und der Protokolldateien an Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS CLI auf dem On-Premises-Db2-Se rver.	Konfigurieren Sie AWS CLI mit dem `Access Key ID` und `Secret Access Key`, die Sie zuvor generiert haben: `$ aws configure`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AWS Access Key ID [None]: ************ AWS Secret Access Key [None]: ********* ********** Default region name [None]: us-east-1 Default output format [None]: json`	
Senden Sie das Backup-Image an Amazon S3.	Zuvor wurde ein Online-Datenbank-Backup im `/backup` lokalen Verzeichnis gespeichert. Um dieses Backup-Image an den S3-Bucket zu senden, führen Sie den folgenden Befehl aus: `aws s3 sync /backup s3://hadrmig-db2/SAMPLE_backup`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die Db2-Archivprotokolle an Amazon S3.	Synchronisieren Sie die lokalen Db2-Archivprotokolle mit dem Amazon S3-Bucket, auf den die Db2-Ziel-Instance auf Amazon EC2 zugreifen kann: `aws s3 sync /db2logs s3://hadrmig-db2/SAMPLE_LOGS` Führen Sie diesen Befehl regelmäßig aus, indem Sie Cron oder andere Planungstools verwenden. Die Häufigkeit hängt davon ab, wie oft die Quelldatenbank Transaktionsprotokolldateien archiviert.	

Verbinden Sie Db2 auf Amazon EC2 mit Amazon S3 und starten Sie die erste Datenbanksynchronisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen PKCS12-Keystore.	Db2 verwendet einen Public-Key Cryptography Standards (PKCS)-Verschlüsselungsschlüsselspeicher, um den AWS-Zugriffsschlüssel zu schützen. Erstellen Sie einen Keystore und konfigurieren Sie den Quell-Db2 für seine Verwendung:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`
	
	`db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Db2-Speicherzugriffsalias.	Db2 verwendet einen Speicherzugriffsalias, um direkt mit den `RESTORE DATABASE` Befehlen `INGEST`, `LOADBACKUP DATABASE`, oder auf Amazon S3 zuzugreifen.
	
	Da Sie der EC2-Instance eine IAM-Rolle zugewiesen haben `USER` und nicht erforderlich `PASSWORD` sind:
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	
	Ihr Skript könnte beispielsweise wie folgt aussehen:
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'hadrmig-db2'"`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Legen Sie den Staging-Bereich fest.	Wir empfehlen, `DB2_ENABLE_COS_SDK=ON` , und den Link zur `awssdk` Bibliothek zu verwenden`DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , um den Amazon S3-Stagingbereich für Datenbanksicherung und -wiederherstellung zu umgehen:
	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2stop`
	`db2start`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Datenbank aus dem Backup-Image wieder her.	Stellen Sie die Zieldatenbank auf Amazon EC2 aus dem Backup-Image im S3-Bucket wieder her:
	`db2 create db sample on /data1`
	`db2 restore db sample from DB2REMOTE://DB2AWSS3/hadrmig-db2/SAMPLE_backup replace existing`
		DBA

Einrichten von HADR ohne lokales HADR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den On-Premises-Db2-Server als primären Server.	Aktualisieren Sie die Datenbankkonfigurationseinstellungen für HADR auf `db2-server1` (die On-Premises-Quelle) als primäres Element. Stellen Sie `HADR_SYNCMODE` auf den `SUPERASYNC` Modus ein, der die kürzeste Reaktionszeit für Transaktionen hat: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-server1 HADR_LOCAL_SVC 50010 HADR_REMOTE_HOST db2-ec2 HADR_REMOTE_SVC 50012 HADR_REMO`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`TE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000 I The UPDATE DATABASE CONFIGURATION command completed successfu lly` Es werden einige Netzwerkv erzögerungen zwischen dem On-Premises-Rechen zentrum und AWS erwartet. (Sie können einen anderen `HADR_SYNCMODE` Wert basierend auf der Netzwerkz uverlässigkeit festlegen. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen).	
Ändern Sie das Ziel des Datenbankprotokollarchivs.	Ändern Sie das Ziel des Datenbankprotokollarchivs so, dass es der Amazon EC2-Umgebung entspricht: `db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/' LOGARCHMETH2 OFF DB20000I The UPDATE DATABASE CONFIGURA TION command completed successfully`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie HADR für Db2 auf dem Amazon EC2-Server.	Aktualisieren Sie die Datenbankkonfiguration für HADR auf `db2-ec2` als Standby: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die HADR-Einrichtung.	Überprüfen Sie die HADR-Parameter auf den Quell- und Ziel-Db2-Servern. Führen Sie den folgenden Befehl aus`db2-server1` , um die Einrichtung auf zu überprüfen: `db2 get db cfg for sample|grep HADR HADR database role = PRIMARY HADR local host name (HADR_LOCAL_HOST) = db2-server1 HADR local service name (HADR_LOCAL_SVC) = 50010 HADR remote host name (HADR_REMOTE_HOST) = db2-ec2 HADR remote service name (HADR_REMOTE_SVC) = 50012 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = HADR log write synchronization mode`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Führen Sie den folgenden Befehl aus`db2-ec2`, um die Einrichtung auf zu überprüfen: db2 get db cfg for sample|grep HADR HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-ec2 HADR local service name (HADR_LOCAL_SVC) = 50012 HADR remote host name (HADR_REMOTE_HOST) = db2-server1	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Die HADR_REMOTE_SVC Parameter HADR_LOCAL_HOST , HADR_LOCAL_SVC HADR_REMO	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	TE_HOST , und geben die eine primäre und eine Standby-HADR-Einrichtung an.	

Starten Sie die Db2-HADR-Instance.	Starten Sie db2-ec2 zuerst die Db2-HADR-Instance auf dem Standby-Server:
	`db2 start hadr on db sample as standby`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	Starten Sie Db2 HADR auf dem primären (Quell-)Server db2-server1 :
	`db2 start hadr on db sample as primary`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	Die HADR-Verbindung zwischen Db2 On-Premises und auf Amazon EC2 wurde jetzt erfolgreich hergestellt. Der primäre Db2-Server db2-server1 startet das Streamen von Transaktionsprotokolldatensätzen db2-ec2 in Echtzeit an .
		DBA

Einrichten von HADR, wenn HADR On-Premises vorhanden ist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Db2 auf Amazon EC2 als zusätzliche Standby-Instance hinzu.	Wenn HADR auf der On-Premises-Db2-Instance ausgeführt wird, können Sie Db2 auf Amazon EC2 als zusätzliche Standby-Instance hinzufügen, `HADR_TARGET_LIST` indem Sie die folgenden Befehle auf ausführen`db2-ec2`: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010|db2-server2:50011" DB20000I The UPDATE DATABASE CONFIGURATION command`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`completed successfully.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die zusätzlichen Standby-Informationen zu den On-Premises-Servern hinzu.	Aktualisieren Sie `HADR_TARGET_LIST` auf den beiden On-Premises-Servern (primär und Standby). `db2-server1` Führen Sie auf den folgenden Code aus: `db2 update db cfg for sample using HADR_TARGET_LIST "db2-server2:50011|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`  `db2-server2` Führen Sie auf den folgenden Code aus:  `db2 update db cfg for sample using HADR_TARG`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ET_LIST "db2-serv er1:50010|db2-ec2: 50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfu lly. SQL1363W One or more of the parameter s submitted for immediate modificat ion were not changed dynamically. For these configura tion parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die HADR-Einrichtung.	Überprüfen Sie die HADR-Parameter auf den Quell- und Ziel-Db2-Servern.
	
	`db2-server1` Führen Sie auf den folgenden Code aus:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50011`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server2:50011|db2-ec2:50012`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>HADR log write
	synchronization mode
	(HADR_SYNCMODE) =
	NEARSYNC
	HADR spool log data
	limit (4KB)
	(HADR_SPOOL_LIMIT) =
	AUTOMATIC(52000)
	HADR log replay delay
	(seconds) (HADR_REP
	LAY_DELAY) = 0
	HADR peer window
	duration (seconds)
	(HADR_PEER_WINDOW) = 0
	HADR SSL certifica
	te label
	(HADR_SSL_LABEL) =
	HADR SSL Hostname
	Validation
	(HADR_SSL_HOST_VAL) =
	OFF</pre>	

	`db2-server2` Führen Sie auf den folgenden Code aus:
	<pre>db2 get db cfg for
	sample|grep HADR
	HADR database role
	
	= STANDBY
	HADR local host name
	(HADR_LOC
	AL_HOST) = db2-server2
	HADR local service
	name
	(HADR_LOCAL_SVC) =
	50011
	HADR remote host name
	(HADR_REM
	OTE_HOST) = db2-serve
	r1</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>HADR remote service
	name
	(HADR_REMOTE_SVC) =
	50010
	HADR instance name
	of remote server
	(HADR_REMOTE_INST) =
	db2inst1
	HADR timeout value
	
	(HADR_TIMEOUT) = 120
	HADR target list
	(HADR_TAR
	GET_LIST) = db2-serve
	r1:50010|db2-ec2:5
	0012
	HADR log write
	synchronization mode
	(HADR_SYNCMODE) =
	NEARSYNC
	HADR spool log data
	limit (4KB)
	(HADR_SPOOL_LIMIT) =
	AUTOMATIC(52000)
	HADR log replay delay
	(seconds) (HADR_REP
	LAY_DELAY) = 0
	HADR peer window
	duration (seconds)
	(HADR_PEER_WINDOW) = 0
	HADR SSL certifica
	te label
	(HADR_SSL_LABEL) =
	HADR SSL Hostname
	Validation
	(HADR_SSL_HOST_VAL) =
	OFF</pre>
	`db2-ec2`Führen Sie auf den folgenden Code aus:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`
	`HADR remote service name (HADR_REMOTE_SVC) = 50010`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-server2:50011`
	`HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC`
	`HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0
	HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0
	HADR SSL certificate label (HADR_SSL_LABEL) =
	HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF</pre>
	Die HADR_TARGET_LIST Parameter HADR_LOCAL_HOST , HADR_LOCAL_SVC , HADR_REMOTE_HOST HADR_REMOTE_SVC , und geben das eine primäre und zwei Standby-HADR-Setup an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stoppen und starten Sie Db2 HADR.	`HADR_TARGET_LIST` ist jetzt auf allen drei Servern eingerichtet. Jeder Db2-Server kennt die anderen beiden. Halten Sie HADR (-Ausfall) an und starten Sie es neu, um die Vorteile der neuen Konfiguration zu nutzen.
	
	Führen Sie `db2-server1` auf die folgenden Befehle aus:
	
	`db2 stop hadr on db sample`
	`db2 deactivate db sample`
	`db2 activate db sample`
	
	Führen Sie `db2-server2` auf die folgenden Befehle aus:
	
	`db2 deactivate db sample`
	`db2 start hadr on db sample as standby`
	`SQL1766W The command completed successfully`
	
	Führen Sie `db2-ec2`auf die folgenden Befehle aus:
	
	`db2 start hadr on db sample as standby`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL1766W The command completed successfully`
	
	Führen Sie `db2-server1` auf die folgenden Befehle aus:
	
	`db2 start hadr on db sample as primary`
	`SQL1766W The command completed successfully`
	
	Die HADR-Verbindung zwischen Db2 On-Premises und auf Amazon EC2 wurde jetzt erfolgreich hergestellt. Der Db2-Primärserver `db2-server1` startet das Streamen von Transaktionsprotokolldatensätzen sowohl in `db2-server2` als auch `db2-ec2` in Echtzeit.	

Machen Sie Db2 auf Amazon EC2 während des Cutover-Fensters als primär

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass es keine HADR-Verzögerung auf dem Standby-Server gibt.	Überprüfen Sie den HADR-Status vom primären Server `db2-server1` . Wird nicht ausgelöst, wenn sich im `REMOTE_CATCHUP` Status `HADR_STATE` befindet, was normal ist, wenn auf gesetzt `HADR_SYNCMODE`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	istSUPERASYNC . und PRIMARY_LOG_TIME STANDBY_REPLAY_LOG _TIME zeigen, dass sie synchronisiert sind:
	
	`db2pd -hadr -db sample`
	
	`HADR_ROLE = PRIMARY`
	
	`REPLAY_TYPE = PHYSICAL`
	
	`HADR_SYNCMODE = SUPERASYNC`
	
	`STANDBY_ID = 2`
	
	`LOG_STREAM_ID = 0`
	
	`HADR_STATE = REMOTE_CATCHUP`
	`.....`
	
	`PRIMARY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`
	
	`STANDBY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`
	`STANDBY_REPLAY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die HADR-Übernahme aus.	Um die Migration abzuschließen, erstellen Sie `db2-ec2` die Primärdatenbank, indem Sie den HADR-Übernahmebefehl ausführen. Verwenden Sie den Befehl db2pd, um den `HADR_ROLE` Wert zu überprüfen:
	`db2 TAKEOVER HADR ON DATABASE sample`
	`DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.`
	`db2pd -hadr -db sample`
	`Database Member 0 -- Database SAMPLE -- Active -- Up 0 days 00:03:25 -- Date 2022-10-26-02.46.45.048988`
	`HADR_ROLE = PRIMARY`
	`REPLAY_TYPE = PHYSICAL`
	Um die Migration zu AWS abzuschließen, verweisen Sie die Anwendungsverbindungen zu Db2 auf Amazon EC2.	

Fehlerbehebung

Problem	Lösung
Wenn Sie NAT aus Firewall- und Sicherheitsgründen verwenden, kann der Host zwei IP-Adressen haben (eine interne und eine externe), was zu einem Fehler bei der Überprüfung der HADR-IP-Adresse führen kann. Der `START HADR ON DATABASE` Befehl gibt die folgende Meldung zurück: `HADR_LOCAL_HOST:HADR_LOCAL_SVC (-xx-xx-xx-xx.:50011 (xx.xx.xx.xx:50011)) on remote database is different from HADR_REMOTE_HOST:HADR_REMOTE_SVC (xx-xx-xx-xx.:50011 (x.x.x.x:50011)) on local database.`	Um HADR in einer NAT-Umgebung zu unterstützen, können Sie die sowohl `HADR_LOCAL_HOST` mit der internen als auch mit der externen Adresse konfigurieren. Wenn der Db2-Server beispielsweise den internen Namen `host1` und den externen Namen hat`host1E`, `HADR_LOCAL_HOST` kann sein`HADR_LOCAL_HOST: "host1 | host1E"`.

Zugehörige Ressourcen

- Db2-Backup- und Wiederherstellungsvorgänge zwischen verschiedenen Betriebssystemen und Hardwareplattformen
- Einrichten von Db2 STORAGE ACCESS ALIAS und DB2REMOTE
- Notfallwiederherstellung mit hoher Verfügbarkeit in Db2
- hadr_syncmode – HADR-Synchronisierungsmodus für Protokollschreibvorgänge im Peer-Status-Konfigurationsparameter

Migrieren Sie VMware-VMs mit HCX Automation mithilfe von PowerCLI

Erstellt von Giri Nadiminty (AWS), Hassan Adekoya (AWS) und Naveen Deshwal

Umgebung: Produktion	Quelle: VMware vCenter oder SDDC vor Ort oder in der Cloud	Ziel: VMware Cloud on AWS
R-Typ: Rehost	Arbeitslast: Alle anderen Workloads	Technologien: Migration; Hybrid-Cloud
AWS-Services: VMware Cloud auf AWS		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie lokale virtuelle Maschinen (VMs) von VMware zu VMware Cloud on AWS mithilfe von VMware Hybrid Cloud Extension (HCX) Automation auf Basis von VMware PowerCLI-Skripts migriert werden. PowerCLI ist ein Befehlszeilentool, das auf Windows basiert. PowerShell Es unterstützt Sie bei der Verwaltung von VMware-Software und automatisiert Infrastruktur- und Migrationsaufgaben.

Sie können dieses Muster für die Migration zwischen einer beliebigen Kombination von vCentern, softwaredefinierten Rechenzentren (SDDCs) und Cloud-Umgebungen anpassen. Die in diesem Muster enthaltenen PowerCLI-Skripts verwenden Automatisierung anstelle von Mausklicks für alle VM-Konfigurations- und Planungsaufgaben, sodass sie Zeit bei Migrationsaktivitäten sparen und das Risiko menschlicher Fehler verringern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein VMware Cloud on AWS AWS-Konto mit SDDC
- Ein vorhandenes lokales oder cloudbasiertes vCenter oder SDDC
- Ein Benutzerkonto mit den erforderlichen Berechtigungen für Quell- und Ziel-vCenter oder SDDCs
- HCX Site Pairing mit HCX Network Extension (HCX-NE), konfiguriert zwischen Quell- und Ziel-vCenters oder SDDCs
- VMware PowerCLI ist auf dem Server Ihrer Wahl installiert

Einschränkungen

- Wenn das Quell-vCenter Cross-vCenter NSX verwendet, funktioniert das PowerCLI-Modul nicht. Verwenden Sie eine Skriptmethode (wie Python) mit der HCX-API anstelle von PowerCLI.
- Wenn die migrierten VMs neue Namen oder IP-Adressen benötigen, verwenden Sie eine Skriptmethode (wie Python) mit der HCX-API.
- Dieses Muster füllt die CSV-Datei nicht auf, was erforderlich ist. Sie können die Datei mithilfe von VMware vRealize Network Insight (vRNI) oder einer anderen Methode auffüllen.

Produktversionen

- VMware vSphere Version 5 oder höher
- VMware HCX Version 4.4 oder höher
- VMware PowerCLI Version 12.7 oder höher

Architektur

Quelltechnologie-Stack

- VMware vor Ort oder in der Cloud

Zieltechnologie-Stack

- VMware Cloud in AWS

Zielarchitektur

Tools

AWS-Services

- VMware Cloud on AWS ist ein Service, der gemeinsam von AWS und VMware entwickelt wurde, um Sie bei der Migration und Erweiterung Ihrer lokalen VMware vSphere-basierten Umgebungen in die AWS-Cloud zu unterstützen.

Andere Tools

- VMware Hybrid Cloud Extension (HCX) ist ein Hilfsprogramm für die Migration von Workloads aus Ihrer lokalen VMware-Umgebung zu VMware Cloud on AWS, ohne die zugrunde liegende Plattform zu ändern. Hinweis: Dieses Produkt war früher als Hybrid Cloud Extension und NSX Hybrid Connect bekannt. Dieses Muster verwendet HCX für die VM-Migration.
- VMware PowerCLI ist ein Befehlszeilentool zur Automatisierung des VMware vSphere- und vCloud-Managements. Sie führen PowerCLI-Befehle in Windows mithilfe von Cmdlets aus. PowerShell PowerShell Dieses Muster verwendet PowerCLI, um Migrationsbefehle auszuführen.

Code

Einfaches, eigenständiges Skript

Es wird empfohlen, dieses Skript für einen einzelnen Computer für erste Tests zu verwenden, um sicherzustellen, dass die Konfigurationsoptionen akzeptiert werden und sich erwartungsgemäß verhalten. Anweisungen finden Sie im Abschnitt Epics.

```
<# Manual Variables #>
$HcxServer = "[enterValue]"
$SrcNetworkName = "[enterValue]"
$DstNetworkName = "[enterValue]"
$DstComputeName = "[enterValue]"
$DstDSName = "[enterValue]"
$DstFolderName = "[enterValue]"
$vmName = "[enterValue]"

<# Environment Setup #>
Connect-HCXServer -Server $HcxServer
$HcxDstSite = Get-HCXSite -Destination
$HcxSrcSite = Get-HCXSite -Source
$SrcNetwork = Get-HCXNetwork -Name $SrcNetworkName -Type VirtualWire -Site $HcxSrcSite
```

```
$DstNetwork = Get-HCXNetwork -Name $DstNetworkName -Type NsxtSegment -Site $HcxDstSite
$DstCompute = Get-HCXContainer -Name $DstComputeName -Site $HcxDstSite
$DstDS = Get-HCXDatastore -Name $DstDSName -Site $HcxDstSite
$DstFolder = Get-HCXContainer -name $DstFolderName -Site $HcxDstSite
$vm = Get-HCXVM -Name $vmName

<# Migration #>
$NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -DestinationNetwork
 $DstNetwork
$NewMigration = New-HCXMigration -VM $vm -MigrationType vMotion -SourceSite $HcxSrcSite
 -DestinationSite $HcxDstSite -Folder $DstFolder -TargetComputeContainer $DstCompute
 -TargetDatastore $DstDS -NetworkMapping $NetworkMapping -DiskProvisionType Thin
 -UpgradeVMTools $True -RemoveISOs $True -ForcePowerOffVm $True -RetainMac $True -
UpgradeHardware $True -RemoveSnapshots $True
```

.csv-basiertes Skript mit vollem Funktionsumfang

Nach Abschluss der Tests können Sie das folgende Skript in Ihren Produktionsumgebungen verwenden. Anweisungen finden Sie im Abschnitt Epics.

```
<# Schedule #>
write-host("Getting Time for Scheduling")
$startTime = [DateTime]::Now.AddDays(12)
$endTime = [DateTime]::Now.AddDays(15)

<# Migration #>
Connect-HCXServer -Server [enterValue]
write-host("Getting Source Site")
$HcxSrcSite = Get-HCXSite
write-host("Getting Target Site")
$HcxDstSite = Get-HCXSite -Destination
$HCXVMS = Import-CSV .\Import_VM_list.csv
ForEach ($HCXVM in $HCXVMS) {
    $DstFolder = Get-HCXContainer $HCXVM.DESTINATION_VM_FOLDER -Site $HcxDstSite
    $DstCompute = Get-HCXContainer $HCXVM.DESTINATION_COMPUTE  -Site $HcxDstSite
    $DstDatastore = Get-HCXDatastore $HCXVM.DESTINATION_DATASTORE -Site $HcxDstSite
    $SrcNetwork = Get-HCXNetwork $HCXVM.SOURCE_NETWORK -Type VirtualWire -Site
 $HcxSrcSite
    $DstNetwork = Get-HCXNetwork $HCXVM.DESTINATION_NETWORK -Type NsxtSegment -Site
 $HcxDstSite
    $NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -
DestinationNetwork $DstNetwork
```

```
    $NewMigration = New-HCXMigration -VM (Get-HCXVM $HCXVM.VM_NAME) -MigrationType
 Bulk -SourceSite $HcxSrcSite -DestinationSite $HcxDstSite -Folder $DstFolder -
TargetComputeContainer $DstCompute -TargetDatastore $DstDatastore -NetworkMapping
 $NetworkMapping -DiskProvisionType Thin -UpgradeVMTools $True -RemoveISOs $True -
ForcePowerOffVm $True -RetainMac $True -UpgradeHardware $True -RemoveSnapshots $True -
ScheduleStartTime $startTime -ScheduleEndTime $endTime
    Start-HCXMigration -Migration $NewMigration -Confirm:$false
}
```

Epen

Sammeln Sie Informationen für manuelle Variablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie die Quell- und Ziel-vCenter- und SDDC-Servernamen.	PowerCLI-Skripts benötigen die in diesem Epos beschriebenen Variablen. Sie können diese Informationen im Voraus sammeln, um die Verwendung des Skripts zu vereinfachen. Wählen Sie im Abschnitt HCX der vSphere-Konsole Infrastructure, Site Pairing aus. Notieren Sie sich die angezeigten Quell- und Zielservernamen.	Cloud-Architekt
Suchen Sie die HCX-Quell- und Zielnamen.	Wählen Sie im HCX-Bereich der vSphere-Konsole System, Administration aus. Notieren Sie sich die angezeigten Quell- und Ziel-HCX-Namen.	Cloud-Architekt
Finden Sie die Namen des Quell- und Zielnetzwerks.	Wählen Sie im HCX-Bereich der vSphere-Konsole System, Network Extension aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Notieren Sie sich die Namen des Quell- und Zielnetzwerks. Hinweis: Alternativ können Sie die Quell- und Zielnetzwerknamen mithilfe der PowerCLI-Befehle Get-HCXNetwork und Get-HCXNetwork-Destination abrufen, nachdem Sie eine Verbindung zum HCX-Server hergestellt haben.	
Sammeln Sie zusätzliche Informationen in der vSphere-Konsole.	Sammeln Sie auf der vSphere-Konsole die folgenden Informationen: • Namen der VMs, die Sie migrieren möchten • Ziel-Computerumgebung (Cluster/Host) • Zieldatenspeicher • Name des Ordners der Ziel-VM	Cloud-Architekt

Treffen Sie Migrationsentscheidungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Migrationsoptionen.	Ermitteln Sie Folgendes: • `MigrationType` — Die HCX-unterstützten Migrationstypen sind vMotion, Bulk, Cold und RAV. Ihre Wahl	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hängt von Ihren Ausfallan forderungen, der Netzwerkb andbreite, dem Migration szeitraum und der Art der Arbeitslast ab. Weitere Informationen finden Sie im AWS-Blogbeitrag Migrieren von Workloads zu VMware Cloud on AWS with Hybrid Cloud Extension (HCX). • `DiskProvisionType (Thin, Thick)` • `UpgradeVMTools ($True, $False)` • `RemoveISOs ($True, $False)` • `ForcePowerOffVm ($True, $False)` • `RetainMac ($True, $False)` • `UpgradeHardware ($True, $False)` • `RemoveSnapshots ($True, $False)` Weitere Informationen zu den einzelnen Optionen finden Sie in der VMware-Entwicklerd okumentation.	

Führen Sie das einfache Skript für erste Tests aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie das Skript.	Die einfache Version des Skripts ist eigenständig in einer einzigen Datei enthalten. Sie können es verwenden, um die Migration einer einzelnen Maschine zu testen. Kopieren Sie das erste Skript aus dem Codeabschnitt dieses Musters und speichern Sie es auf dem Computer, auf dem das VMware PowerCLI-Modul installiert ist. (Folgen Sie den Anweisungen in der VMware-Dokumentation, um PowerCLI zu installieren.)	Cloud-Architekt
Legen Sie Skriptvariablen fest.	Legen Sie alle Variablen im `Manual Variables` Abschnitt des Skripts fest.	Cloud-Architekt
Legen Sie Migrationsvariablen fest.	Legen Sie alle `New-HCXMigration` Einstellungen im `Migration` Abschnitt des Skripts fest.	Cloud-Architekt
Geben Sie Websites an.	(Optional) Wenn die Quelle oder das Ziel mehrere Sites hat, geben Sie die Sites manuell im `Environment Setup` Abschnitt des Skripts an.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn die Quelle und das Ziel einzelne Websites haben, sucht das Skript automatisch nach den Informationen.	
Führen Sie das Skript aus.	Führen Sie auf dem Server, auf dem PowerCLI installie rt ist, in einem PowerShell Fenster mit erhöhten Rechten das Skript aus und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgeford ert werden.	Cloud-Architekt
Validieren Sie das Skript.	Vergewissern Sie sich, dass die VM-Migration initiiert wurde.	Cloud-Architekt

Führen Sie das Skript mit vollem Funktionsumfang aus, um mehrere VMs zu migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CSV-Datei und füllen Sie sie aus.	Erstellen Sie eine CSV-Datei namens `Import_VM_list.csv` auf Ihrem Computer und füllen Sie sie mit dem folgenden Beispieli nhalt: `VM_NAME,DESTINATIO N_VM_FOLDER,DESTIN ATION_COMPUTE,DEST INATION_DATASTORE, SOURCE_NETWORK,DES TINATION_NETWORK`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`[enterValue],[enter Value],[enterValue ],[enterValue],[en terValue],[enterVa lue]` Ersetzen Sie jede Datei `[enterValue]` in der CSV-Datei durch die Informationen, die Sie zuvor gesammelt haben. Hinweis: Sie können die .csv-Datei mithilfe von VMware vRealize Network Insight (vRNI) oder einer anderen Methode auffüllen.	
Kopieren Sie das Skript.	Die Version des Skripts mit vollem Funktionsumfang verwendet Informationen aus einer externen CSV-Datei, um mehrere VMs automatisch zu migrieren. Kopieren Sie das zweite Skript aus dem Codeabschnitt dieses Musters und speichern Sie es auf dem Computer, auf dem das VMware PowerCLI-Modul installiert ist, im selben Ordner wie die CSV-Datei.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie das Skript.	Bearbeiten Sie das Skript, um die folgenden Änderungen vorzunehmen: • Zeile 7: Stellen Sie die HCX-Servervariable (`Connect-HCXServer`) ein. • Zeile 12: (Optional) Wenn Sie den CSV-Dateinamen anders festlegen, aktualisieren Sie ihn. • Zeilen 3-4: (Optional) Stellen Sie den Zeitplan ein. • Zeile 20: (Optional) Geben Sie die `New-HCXMigration` Einstellungen im `Migration` Abschnitt an. • Zeilen 9 und 11: (Optional) Wenn die Quelle oder das Ziel mehrere Standorte umfasst, geben Sie die gewünschten Standorte manuell an.	Cloud-Architekt
Führen Sie das Skript aus.	Führen Sie auf dem Server, auf dem PowerCLI installiert ist, in einem PowerShell Fenster mit erhöhten Rechten das Skript aus und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie das Skript.	Vergewissern Sie sich, dass die VM-Migration initiiert wurde.	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Das Skript schlägt mit der folgenden Fehlermeldung fehl: „Alle Quellnetzwerke sind nicht dem Ziel zugeordnet!“	Wenn das Quell-vCenter Cross-vCenter NSX verwendet, funktioniert das PowerCLI-Modul nicht. Verwenden Sie eine Skriptmethode (wie Python) mit der HCX-API anstelle von PowerCLI. Dies ist eine bekannte Einschränkung des PowerCLI-Skripts.
Das Skript schlägt mit der folgenden Fehlermeldung fehl: „Connect-HCXServer-Fehler: Nicht autorisiert“	Die von Ihnen eingegebenen Anmeldeinformationen bieten nicht die erforderlichen Berechtigungen.

Zugehörige Ressourcen

- Migration von Workloads zu VMware Cloud on AWS mit Hybrid Cloud Extension (HCX) (AWS-Blogbeitrag)
- Auswahl eines Migrationsansatzes für die Verlagerung Ihrer VMware-Anwendungen und -Workloads in die AWS-Cloud (AWS Prescriptive Guidance)
- Migrieren Sie VMware SDDC mithilfe von VMware HCX zu VMware Cloud on AWS (AWS Prescriptive Guidance)
- Erste Schritte mit dem HCX-Modul (VMware-Blogbeitrag)

Migrieren eines F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS Cloud

Erstellt von Will Bauer (AWS)

Quelle: F5-BIG-IP-TSpeed 13.1 und höher	Ziel: F5 BIG-IP VE auf AWS	R-Typ: Hostwechsel
Umgebung: Produktion	Technologien: Migration ; Sicherheit, Identität, Compliance; Netzwerk	Workload: Alle anderen Workloads
AWS-Services: Amazon EC2; Amazon VPC; AWS Transit Gateway; Amazon CloudFront; Amazon CloudWatch; AWS Global Accelerator; AWS CloudFormation		

Übersicht

Organisationen möchten zur Amazon Web Services (AWS) Cloud migrieren, um ihre Agilität und Widerstandsfähigkeit zu erhöhen. Nachdem Sie Ihre F5 BIG-IP-Sicherheits- und Datenverkehrsverwaltungslösungen auf die AWS Cloud migriert haben, können Sie sich auf Agilität und die Einführung hochwertiger Betriebsmodelle in Ihrer gesamten Unternehmensarchitektur konzentrieren.

Dieses Muster beschreibt, wie Sie einen F5 BIG-IP-Workload zu einem F5 BIG-IP Virtual Edition (VE)-Workload in der AWS Cloud migrieren. Der Workload wird migriert, indem die vorhandene Umgebung gehostet und Aspekte des Plattformwechsels bereitgestellt werden, z. B. Service Discovery und API-Integrationen. AWS- CloudFormation Vorlagen beschleunigen die Migration Ihres Workloads zur AWS Cloud.

Dieses Muster richtet sich an technische Entwicklungs- und Architekturteams, die F5-Sicherheits- und Datenverkehrsverwaltungslösungen migrieren, und unterstützt den Leitfaden Migration von F5 BIG-IP zu F5 BIG-IP VE auf der AWS Cloud auf der Website AWS Prescriptive Guidance.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandener On-Premises-F5-BIG-IP-Workload.
- Bestehende F5-Lizenzen für BIG-IP-VE-Versionen.
- Ein aktives AWS-Konto.
- Eine vorhandene Virtual Private Cloud (VPC), die mit einem Ausgang über ein NAT-Gateway oder eine Elastic IP-Adresse konfiguriert und mit Zugriff auf die folgenden Endpunkte konfiguriert ist: Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), AWS Security Token Service (AWS STS) und Amazon CloudWatch. Sie können auch den Schnellstart der modularen und skalierbaren VPC-Architektur als Baustein für Ihre Bereitstellungen ändern.
- Eine oder zwei vorhandene Availability Zones, je nach Ihren Anforderungen.
- Drei vorhandene private Subnetze in jeder Availability Zone.
- AWS- CloudFormation Vorlagen, verfügbar im F5 GitHub -Repository .

Während der Migration können Sie je nach Ihren Anforderungen auch Folgendes verwenden:

- Eine F5-Cloud-Failover-Erweiterung zur Verwaltung von Elastic IP-Adresszuweisung, sekundärer IP-Zuweisung und Routing-Tabellenänderungen.
- Wenn Sie mehrere Availability Zones verwenden, müssen Sie die F5 Cloud Failover Extensions verwenden, um die Elastic IP-Zuweisung zu virtuellen Servern zu verwalten.
- Sie sollten die Verwendung von F5 Application Services 3 (AS3), F5 Application Services Templates (FAST) oder einem anderen Infrastructure as Code (IaC)-Modell in Betracht ziehen, um die Konfigurationen zu verwalten. Die Vorbereitung der Konfigurationen in einem IaC-Modell und die Verwendung von Code-Repositorys wird bei der Migration und Ihren laufenden Verwaltungsbemühungen helfen.

Bol

- Dieses Muster erfordert Vertrautheit damit, wie eine oder mehrere VPCs mit vorhandenen Rechenzentren verbunden werden können. Weitere Informationen dazu finden Sie unter Konnektivitätsoptionen von Netzwerk zu Amazon VPC in der Amazon-VPC-Dokumentation.

- Vertrautheit mit F5-Produkten und -Modulen ist auch erforderlich, darunter Traffic Management Operating System (T Bol), Local Traffic Manager (LTM) ,Global Traffic Manager (GTM) ,Access Policy Manager (APM) ,Application Security Manager (ASM) ,Advanced Firewall Manager (AFM) und BIG-IQ .

Produktversionen

- Wir empfehlen, F5 BIG-IP Version 13.1 oder höher zu verwenden, obwohl das Muster F5 BIG-IP Version 12.1 oder höher unterstützt.

Architektur

Quelltechnologie-Stack

- F5-BIG-IP-Workload

Zieltechnologie-Stack

- Amazon CloudFront
- Amazon CloudWatch
- Amazon EC2
- Amazon S3
- Amazon VPC
- AWS Global Accelerator
- AWS STS
- AWS Transit Gateway
- F5 BIG-IP-VE

Zielarchitektur

Tools

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz verringert und die Leistung verbessert.
- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Token Service (AWS STS) hilft Ihnen, temporäre Anmeldeinformationen mit eingeschränkten Berechtigungen für Benutzer anzufordern.
- AWS Transit Gateway ist ein zentraler Hub, der Virtual Private Clouds (VPCs) und On-Premises-Netzwerke miteinander verbindet.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Polen

Erkennung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bewerten Sie die Leistung von F5 BIG-IP.	Erfassen und aufzeichnen Sie die Leistungsmetriken der Anwendungen auf dem virtuellen Server sowie	F5-Architekt, Ingenieur und Netzwerkarchitekt, Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Metriken der Systeme, die migriert werden. Dies trägt dazu bei, die AWS-Zielinfrastruktur korrekt zu dimensionieren, um die Kosten zu optimieren.	
Bewerten Sie das F5-BIG-IP-Betriebssystem und die Konfiguration.	Prüfen Sie, welche Objekte migriert werden und ob eine Netzwerkstruktur aufrechte rhalten werden muss, z. B. VLANs.	F5-Architekt, Ingenieur
Bewerten Sie die F5-Lizenz optionen.	Prüfen Sie, welches Lizenz- und Nutzungsmodell Sie benötigen. Diese Bewertung sollte auf Ihrer Bewertung des F5-BIG-IP-Betriebs systems und der Konfiguration basieren.	F5-Architekt, Ingenieur
Bewerten Sie die öffentlichen Anwendungen.	Bestimmen Sie, welche Anwendungen öffentliche IP-Adressen benötigen. Richten Sie diese Anwendung en an den erforderlichen Instances und Clustern aus, um die Anforderungen an Performance und Service Level Agreement (SLA) zu erfüllen.	F5 Architect, Cloud Architect, Network Architect, Ingenieur, App Teams

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bewerten Sie interne Anwendungen.	Prüfen Sie, welche Anwendungen von internen Benutzern verwendet werden. Stellen Sie sicher, dass Sie wissen, wo sich diese internen Benutzer in der Organisat ion befinden und wie diese Umgebungen mit der AWS Cloud verbunden sind. Sie sollten auch sicherstellen, dass diese Anwendungen das Domain Name System (DNS) als Teil der Standarddomäne verwenden können.	F5 Architect, Cloud Architect, Network Architect, Ingenieur, App Teams
Finalisieren Sie das AMI.	Nicht alle F5-BIG-IP-Versione n werden als Amazon Machine Images (AMIs) erstellt. Sie können das F5 BIG-IP Image Generator Tool verwenden , wenn Sie über bestimmte erforderliche Quick-Fix Engineering (QFE)-Versionen verfügen. Weitere Informati onen zu diesem Tool finden Sie im Abschnitt „Verwandte Ressourcen“.	F5 Architect, Cloud Architect, Ingenieur
Finalisieren Sie die Instance-Typen und die Architektur.	Entscheiden Sie sich für die Instance-Typen, die VPC-Architektur und die miteinand er verbundene Architektur.	F5 Architect, Cloud Architect, Network Architect, Ingenieur

Ausführen von sicherheits- und Compliance-bezogenen Aktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie die vorhandenen F5-Sicher heitsrichtlinien.	Erfassen und dokumentieren Sie vorhandene F5-Sicher heitsrichtlinien. Stellen Sie sicher, dass Sie eine Kopie davon in einem sicheren Code-Repository erstellen.	F5-Architekt, Ingenieur
Verschlüsseln Sie das AMI.	(Optional) Ihre Organisation benötigt möglicherweise die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen zum Erstellen eines benutzerdefinierten BYOL-Images (Bring Your Own License) finden Sie im Abschnitt „Verwandte Ressourcen“.	F5-Architekt, Ingenieur Cloud Architect, Ingenieur
Harden Sie die Geräte.	Dies trägt zum Schutz vor potenziellen Schwachstellen bei.	F5-Architekt, Ingenieur

Konfigurieren Ihrer neuen AWS-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Edge- und Sicherheitskonten.	Melden Sie sich bei der AWS-Managementkonsole an und erstellen Sie die AWS-Konte n, die die Edge- und Sicherhei tsservices bereitstellen und betreiben. Diese Konten können sich von den Konten	Cloud-Architekt, Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unterscheiden, die VPCs für gemeinsam genutzte Services und Anwendungen betreiben . Dieser Schritt kann als Teil einer Landing Zone abgeschlo ssen werden.	
Stellen Sie Edge- und Sicherheits-VPCs bereit.	Richten Sie die VPCs ein und konfigurieren Sie sie, die für die Bereitstellung von Edge- und Sicherheitsservices erforderlich sind.	Cloud-Architekt, Ingenieur
Stellen Sie eine Verbindung zum Quell-Rechenzentrum her.	Stellen Sie eine Verbindung mit dem Quell-Rechenzentru m her, das Ihre F5-BIG-IP-Workload hostet.	Cloud Architect, Network Architect, Ingenieur
Stellen Sie die VPC-Verbi ndungen bereit.	Verbinden Sie die Edge- und Sicherheitsservice-VPCs mit den Anwendungs-VPCs.	Netzwerkarchitekt, Ingenieur
Stellen Sie die Instances bereit.	Stellen Sie die Instances mithilfe der AWS- CloudForm ation Vorlagen aus dem Abschnitt „Verwandte Ressourcen“ bereit.	F5-Architekt, Ingenieur
Testen und konfigurieren Sie das Instance-Failover.	Stellen Sie sicher, dass die AWS Advanced HA iAPP-Vorl age oder F5 Cloud Failover Extension konfiguriert ist und ordnungsgemäß funktioniert.	F5-Architekt, Ingenieur

Netzwerk konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die VPC-Topologie vor.	Öffnen Sie die Amazon-VPC-Konsole und stellen Sie sicher, dass Ihre VPC über alle erforderlichen Subnetze und Schutzmaßnahmen für die F5-BIG-IP-VE-Bereitstellung verfügt.	Network Architect, F5 Architect, Cloud Architect, Ingenieur
Bereiten Sie Ihre VPC-Endpunkte vor.	Bereiten Sie die VPC-Endpunkte für Amazon EC2, Amazon S3 und AWS STS vor, wenn ein F5 BIG-IP-Workload keinen Zugriff auf ein NAT-Gateway oder eine Elastic IP-Adresse auf einer TMM-Schnittstelle hat.	Cloud-Architekt, Ingenieur

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Konfiguration.	Migrieren Sie die F5 BIG-IP-Konfiguration zu F5 BIG-IP VE in der AWS Cloud.	F5-Architekt, Ingenieur
Ordnen Sie die sekundären IPs zu.	Virtuelle Server-IP-Adressen haben eine Beziehung zu den sekundären IP-Adressen, die den Instances zugewiesen sind. Weisen Sie sekundäre IP-Adressen zu und stellen Sie sicher, dass „Neuzuwei	F5-Architekt, Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sung/Neuzuweisung zulassen“ ausgewählt ist.	

Testkonfigurationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Konfigura tionen des virtuellen Servers.	Testen Sie die virtuellen Server.	F5-Architekt, App Teams

Abschließen von Vorgängen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Backup-St rategie.	Systeme müssen heruntergefahren werden, um einen vollständigen Snapshot zu erstellen. Weitere Informationen finden Sie unter „Aktualisieren einer virtuellen F5-BIG-IP-Maschine“ im Abschnitt „Verwandte Ressourcen“.	F5 Architect, Cloud Architect, Ingenieur
Erstellen Sie das Cluster-Failover-Runbook.	Stellen Sie sicher, dass der Failover-Runbook-Prozess abgeschlossen ist.	F5-Architekt, Ingenieur
Richten Sie die Protokollierung ein und validieren Sie sie.	Konfigurieren Sie F5 Telemetry Streaming, um Protokolle an die erforderlichen Ziele zu senden.	F5-Architekt, Ingenieur

Abschließen des Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zur neuen Bereitstellung.		F5 Architect, Cloud Architect, Network Architect, Ingenieur, AppTeams

Zugehörige Ressourcen

Migrationsleitfaden

- Migration von F5 BIG-IP zu F5 BIG-IP VE in der AWS Cloud

F5-Ressourcen

- AWS- CloudFormation Vorlagen im F5 GitHub -Repository
- F5 im AWS Marketplace
- Übersicht über F5 BIG-IP VE
- Beispiel für Schnellstart – BIG-IP Virtual Edition mit WAF (LTM + ASM)
- F5-Anwendungsservices in AWS: eine Übersicht (Video)
- Benutzerhandbuch für F5 Application Services 3 Extension
- F5-Cloud-Dokumentation
- F5-iControl-REST-Wiki
- F5 Übersicht über einzelne Konfigurationsdateien (11.x–15.x)
- F5-Topologieumgebung
- F5-Whitepaper
- F5-BIG-IP-Image-Generator-Tool
- Aktualisieren einer virtuellen F5-BIG-IP-VE-Maschine
- Übersicht über die Option „plattformmigration“ des UCS-Archivs

Migrieren Sie eine lokale Go-Webanwendung mithilfe der binären Methode zu AWS Elastic Beanstalk

Erstellt von Suhas Basavaraj (AWS) und Shumaz Mukhtar Kazi (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Anwendungen	Ziel: Elastic Beanstalk
R-Typ: Rehost	Technologien: Migration; Web- und mobile Apps	AWS-Dienste: AWS Elastic Beanstalk

Übersicht

Dieses Muster beschreibt, wie eine lokale Go-Webanwendung zu AWS Elastic Beanstalk migriert wird. Nach der Migration der Anwendung erstellt Elastic Beanstalk die Binärdatei für das Quellpaket und stellt sie auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance bereit.

Als Rehost-Migrationsstrategie ist der Ansatz dieses Musters schnell und erfordert keine Codeänderungen, was weniger Test- und Migrationszeit bedeutet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine lokale Go-Webanwendung.
- Ein GitHub Repository, das den Quellcode Ihrer Go-Anwendung enthält. Wenn Sie es nicht verwenden GitHub, gibt es andere Möglichkeiten, ein Anwendungsquellpaket für Elastic Beanstalk zu erstellen.

Produktversionen

- Die neueste Go-Version, die von Elastic Beanstalk unterstützt wird. Weitere Informationen finden Sie in der Elastic Beanstalk Beanstalk-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Go-Webanwendung

Zieltechnologie-Stack

- AWS Elastic Beanstalk
- Amazon CloudWatch

Zielarchitektur

Tools

- AWS Elastic Beanstalk stellt Anwendungen in der AWS-Cloud schnell bereit und verwaltet sie, ohne dass Benutzer sich mit der Infrastruktur vertraut machen müssen, auf der diese Anwendungen ausgeführt werden. Elastic Beanstalk vereinfacht die komplexe Verwaltung, ohne Einschränkungen in Bezug auf Auswahl oder Kontrolle nach sich zu ziehen.
- GitHubist ein verteiltes Open-Source-Versionskontrollsystem.

Epen

Erstellen Sie die ZIP-Datei mit dem Quellpaket für die Go-Webanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Quellpaket für die Go-Anwendung.	Öffnen Sie das GitHub Repository, das den Quellcode Ihrer Go-Anwendung enthält, und bereiten Sie das Quellpaket vor. Das Quellpaket enthält eine `application.go` Quelldatei im Stammverzeichnis, die	Systemadministrator, Anwendungsentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Hauptpaket für Ihre Go-Anwendung hostet. Wenn Sie es nicht verwenden GitHub, finden Sie im Abschnitt Voraussetzungen weiter oben in diesem Muster weitere Möglichkeiten, Ihr Anwendung squellpaket zu erstellen.	
Erstellen einer Konfigura tionsdatei	Erstellen Sie einen `.ebextensions` Ordner in Ihrem Quellpaket und dann eine `options.config` Datei in diesem Ordner. Weitere Informationen finden Sie in der Elastic Beanstalk Beanstalk-Dokumentation.	Systemadministrator, Anwendungsentwickler
Erstellen Sie die ZIP-Datei des Quellpakets.	Führen Sie den folgenden Befehl aus. `git archive -o ../godemo app.zip HEAD` Dadurch wird die .zip-Date i des Quellpakets erstellt. Laden Sie die ZIP-Datei herunter und speichern Sie sie als lokale Datei. Wichtig: Die ZIP-Datei darf 512 MB nicht überschreiten und darf keinen übergeord neten Ordner oder ein Verzeichnis der obersten Ebene enthalten.	Systemadministrator, Anwendungsentwickler

Migrieren Sie die Go-Webanwendung zu Elastic Beanstalk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Elastic Beanstalk Beanstalk-Anwendung aus.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Elastic Beanstalk Beanstalk-Konsole. 2. Wählen Sie aus der Liste der Regionen Ihre AWS-Region aus. 3. Wählen Sie im Navigationsbereich Applications und dann eine bestehende Elastic Beanstalk Beanstalk-Anwendung aus oder erstellen Sie eine. Anweisungen zum Erstellen einer Elastic Beanstalk Beanstalk-Anwendung finden Sie in der Elastic Beanstalk Beanstalk-Dokumentation.	Systemadministrator, Anwendungsentwickler
Initiieren Sie die Elastic Beanstalk Beanstalk-Webserver-Umgebung.	1. Wählen Sie auf der Seite mit der Anwendungsübersicht die Option Neue Umgebung erstellen und anschließend Webserver-Umgebung aus. 2. Füllen Sie die Felder Umgebungsname und Domänenname aus.	Systemadministrator, Anwendungsentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Plattform version und anschließend Go als Plattform aus.	
Laden Sie die .zip-Datei des Quellpakets auf Elastic Beanstalk hoch.	1. Wählen Sie unter Anwendungscode die Option Code hochladen und dann Lokale Datei aus. 2. Wählen Sie die ZIP-Datei aus, die Ihr Quellpaket enthält. 3. Geben Sie der Datei unter Versionsbezeichnung einen eindeutigen Namen und wählen Sie dann Umgebung erstellen aus.	Systemadministrator, Anwendungsentwickler
Testen Sie die bereitgestellte Go-Webanwendung.	Sie werden zur Übersicht sseite der Elastic Beanstalk Beanstalk-Anwendung weitergeleitet. Wählen Sie oben in der Übersicht neben Environment ID die URL aus, die mit „Um zu Ihrer Anwendung `elasticbe anstalk.com` zu navigiere n“ endet. Ihre Anwendung muss diesen Namen in ihrer Konfigurationsdate i als Umgebungsvariable verwenden und ihn auf der Webseite anzeigen.	Systemadministrator, Anwendungsentwickler

Fehlerbehebung

Problem	Lösung
Auf die Anwendung kann nicht über einen Application Load Balancer zugegriffen werden.	Überprüfen Sie die Zielgruppe, die Ihre Elastic Beanstalk Beanstalk-Anwendung enthält. Wenn sie fehlerhaft ist, melden Sie sich bei Ihrer Elastic Beanstalk Beanstalk-Instance an und überprüfen Sie die `nginx.conf` Dateikonf iguration, um sicherzustellen, dass sie zur richtigen Integritätsstatus-URL weitergeleitet wird. Möglicherweise müssen Sie die URL für die Zustandsprüfung der Zielgruppe ändern.

Zugehörige Ressourcen

- Von Elastic Beanstalk unterstützte Go-Plattformversionen
- Verwenden von Konfigurationsdateien mit Elastic Beanstalk
- Eine Beispielanwendung in Elastic Beanstalk erstellen

Migrieren Sie mithilfe von AWS Transfer for SFTP einen lokalen SFTP-Server zu AWS

Erstellt von Akash Kumar (AWS)

Umgebung: Produktion	Quelle: Speicher	Ziel: Amazon S3
R-Typ: Rehost	Technologien: Migration; Speicher und Backup; Web- und mobile Apps	AWS-Services: Amazon S3; AWS Transfer-Familie; Amazon CloudWatch Logs

Übersicht

Dieses Muster beschreibt, wie eine lokale Dateiübertragungslösung, die das Secure Shell (SSH) File Transfer Protocol (SFTP) verwendet, mithilfe des AWS Transfer for SFTP-Service in die Amazon Web Services (AWS) -Cloud migriert wird. Benutzer stellen in der Regel entweder über seinen Domainnamen oder eine feste IP eine Verbindung zu einem SFTP-Server her. Dieses Muster deckt beide Fälle ab.

AWS Transfer for SFTP ist ein Mitglied der AWS Transfer Family. Es ist ein sicherer Übertragungsservice, mit dem Sie Dateien über SFTP in und aus AWS-Speicherservices übertragen können. Sie können AWS Transfer for SFTP mit Amazon Simple Storage Service (Amazon S3) oder Amazon Elastic File System (Amazon EFS) verwenden. Dieses Muster verwendet Amazon S3 für die Speicherung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener SFTP-Domainname oder eine feste SFTP-IP.

Einschränkungen

- Das größte Objekt, das Sie in einer Anfrage übertragen können, ist derzeit 5 GiB groß. Für Dateien, die größer als 100 MiB sind, sollten Sie den mehrteiligen Amazon S3 S3-Upload in Betracht ziehen.

Architektur

Quelltechnologie-Stack

- Lokale Flatfiles oder Datenbank-Dumpdateien.

Zieltechnologie-Stack

- AWS Transfer for SFTP
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)
- Rollen und Richtlinien von AWS Identity and Access Management (IAM)
- Elastic-IP-Adressen
- Sicherheitsgruppen
- CloudWatch Amazon-Protokolle (optional)

Zielarchitektur

Automatisierung und Skalierung

Verwenden Sie die angehängten CloudFormation AWS-Vorlagen, um die Zielarchitektur für dieses Muster zu automatisieren:

- `amazon-vpc-subnets.yml`stellt eine Virtual Private Cloud (VPC) mit zwei öffentlichen und zwei privaten Subnetzen bereit.
- `amazon-sftp-server.yml`stellt den SFTP-Server bereit.
- `amazon-sftp-customer.yml`fügt Benutzer hinzu.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet Amazon S3 als Speichersystem für Dateiübertragungen.
- Mit AWS Transfer for SFTP können Sie Dateien über das SFTP-Protokoll in und aus AWS-Speicherservices übertragen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Erstellen einer VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC mit Subnetzen.	Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Erstellen Sie eine Virtual Private Cloud (VPC) mit zwei öffentlichen Subnetzen. (Das zweite Subnetz bietet hohe Verfügbarkeit.) –oder– Sie können die angehängte CloudFormation Vorlage in der CloudFormation Konsole bereitstellen`amazon-vpc-subnets.yml` , um die	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufgaben in diesem Epos zu automatisieren.	
Fügen Sie ein Internet-Gateway hinzu.	Stellen Sie ein Internet-Gateway bereit und verbinden Sie es mit der VPC.	Entwickler, Systemadm inistrator
Migrieren Sie eine bestehende IP.	Hängen Sie eine bestehende IP an die Elastic IP-Adresse an. Sie können eine Elastic IP-Adresse aus Ihrem Adresspool erstellen und verwenden.	Entwickler, Systemadm inistrator

Stellen Sie einen SFTP-Server bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SFTP-Server.	Öffnen Sie die AWS Transfer Family Family-Konsole unter https://console.aws.amazon.com/transfer/. Folgen Sie den Anweisungen unter Erstellen eines mit dem Internet verbundenen Endpunkts für Ihren Server in der Dokumentation zur AWS Transfer Family, um einen SFTP-Server mit einem mit dem Internet verbundenen Endpunkt zu erstellen. Wählen Sie als Endpunkttyp die Option VPC Hosted aus. Wählen Sie für Access die Option Internet Facing aus. Wählen Sie für VPC die VPC aus, die Sie	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im vorherigen Epos erstellt haben. –oder– Sie können die angehängte CloudFormation Vorlage in der CloudFormation Konsole bereitstellen `amazon-sftp-server.yml` , um die Aufgaben in diesem Epic zu automatisieren.	
Migrieren Sie den Domainnamen.	Hängen Sie den vorhandenen Domainnamen an den benutzerdefinierten Hostnamen an. Wenn Sie einen neuen Domainnamen verwenden, verwenden Sie den Amazon Route 53 53-DNS-Alias. Wählen Sie für einen vorhandenen Domainnamen „Anderes DNS“. Weitere Informationen finden Sie unter Arbeiten mit benutzerdefinierten Hostnamen in der Dokumentation zur AWS Transfer-Familie.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine CloudWatch Logging-Rolle hinzu.	(Optional) Wenn Sie die CloudWatch Protokollierung aktivieren möchten, erstellen Sie eine `Transfer` Rolle mit den CloudWatch Logs-API-Vorgängen `logs:CreateLogGroup` `logs:CreateLogStream` , `logs:DescribeLogStreams` , und `logs:PutLogEvents` . Weitere Informationen finden Sie unter Aktivität protokollieren mit CloudWatch in der Dokumentation zur AWS Transfer-Familie.	Entwickler, Systemadministrator
Speichern und abschicken.	Wählen Sie Speichern. Wählen Sie für Aktionen die Option Start und warten Sie, bis der SFTP-Server mit dem Status Online erstellt wurde.	Entwickler, Systemadministrator

Ordnen Sie dem SFTP-Server Elastic IP-Adressen zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie den Server, damit Sie die Einstellungen ändern können.	Wählen Sie in der AWS Transfer Family Family-Konsole Server und dann den von Ihnen erstellten SFTP-Server aus. Wählen Sie für Actions (Aktionen) die Option Stop (Stopp). Wenn der	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Server offline ist, wählen Sie Bearbeiten, um seine Einstellungen zu ändern.	
Wählen Sie Availability Zones und Subnetze.	Wählen Sie im Abschnitt Availability Zones die Availability Zones und Subnetze für Ihre VPC aus.	Entwickler, Systemadministrator
Fügen Sie Elastic IP-Adressen hinzu.	Wählen Sie für IPv4-Adressen eine Elastic IP-Adresse für jedes Subnetz aus und klicken Sie dann auf Speichern.	Entwickler, Systemadministrator

Hinzufügen von Benutzern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle, damit Benutzer auf den S3-Bucket zugreifen können.	Erstellen Sie eine IAM-Rolle für `Transfer` und fügen Sie `s3:ListBucket` `s3:GetBucketLocation` , und `s3:PutObject` mit dem S3-Bucket-Namen als Ressource hinzu. Weitere Informationen finden Sie unter Erstellen einer IAM-Rolle und -Richtlinie in der Dokumentation zur AWS Transfer-Familie. –oder– Sie können die angehängte CloudFormation Vorlage in	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der CloudFormation Konsole bereitstellen `amazon-sftp-customer.yml` , um die Aufgaben in diesem Epos zu automatisieren.	
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für die Anwendung.	Entwickler, Systemadministrator
Erstellen Sie optionale Ordner.	(Optional) Wenn Sie Dateien für Benutzer separat in bestimmten Amazon S3 S3-Ordnern speichern möchten, fügen Sie die entsprechenden Ordner hinzu.	Entwickler, Systemadministrator
Erstellen Sie einen öffentlichen SSH-Schlüssel.	Informationen zum Erstellen eines SSH-Schlüsselpaars finden Sie unter Generieren von SSH-Schlüsseln in der Dokumentation zur AWS Transfer-Familie.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hinzufügen von Benutzern.	Wählen Sie in der AWS Transfer Family Family-Konsole Server, wählen Sie den von Ihnen erstellten SFTP-Server aus und klicken Sie dann auf Benutzer hinzufügen. Wählen Sie für das Home-Verzeichnis den S3-Bucket aus, den Sie erstellt haben. Geben Sie für den öffentlichen SSH-Schlüssel den öffentlichen Schlüsselteil des SSH-Schlüsselpaars an. Fügen Sie Benutzer für den SFTP-Server hinzu und wählen Sie dann Hinzufügen aus.	Entwickler, Systemadministrator

Testen Sie den SFTP-Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Sicherheitsgruppe.	Fügen Sie im Abschnitt Sicherheitsgruppen Ihres SFTP-Servers die IP Ihres Testcomputers hinzu, um SFTP-Zugriff zu erhalten.	Developer
Verwenden Sie ein SFTP-Client-Hilfsprogramm, um den Server zu testen.	Testen Sie Dateiübertragungen mit einem beliebigen SFTP-Client-Hilfsprogramm. Eine Liste der Clients und Anweisungen finden Sie unter Übertragen von Dateien mithilfe eines Clients in der	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokumentation zur AWS Transfer Family.	

Zugehörige Ressourcen

- AWS Transfer Family Family-Benutzerhandbuch
- Amazon S3 S3-Benutzerhandbuch
- Elastische IP-Adressen in der Amazon EC2 EC2-Dokumentation

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren einer On-Premises-VM zu Amazon EC2 mithilfe von AWS Application Migration Service

Erstellt von Thanh Nguyen (AWS)

Umgebung: Produktion	Quelle: On-Premises virtuelle Maschine	Ziel: Amazon EC2
R-Typ: Hostwechsel	Technologien: Migration	AWS-Services: AWS Application Migration Service; Amazon EC2; Amazon EBS

Übersicht

Wenn es um die Anwendungsmigration geht, können Organisationen unterschiedliche Ansätze verfolgen, um die Server der Anwendung von der On-Premises-Umgebung in die Amazon Web Services (AWS) Cloud zu hosten (Lift and Shift). Eine Möglichkeit besteht darin, neue Amazon Elastic Compute Cloud (Amazon EC2)-Instances bereitzustellen und dann die Anwendung von Grund auf neu zu installieren und zu konfigurieren. Ein weiterer Ansatz besteht darin, native Migrationsservices von Drittanbietern oder AWS zu verwenden, um mehrere Server gleichzeitig zu migrieren.

Dieses Muster beschreibt die Schritte zur Migration einer unterstützten virtuellen Maschine (VM) zu einer Amazon EC2-Instance in der AWS Cloud mithilfe von AWS Application Migration Service. Sie können den Ansatz in diesem Muster verwenden, um eine oder mehrere virtuelle Maschinen manuell, einzeln oder automatisch zu migrieren, indem Sie geeignete Automatisierungsskripts basierend auf den beschriebenen Schritten erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto in einer der AWS-Regionen, die Application Migration Service unterstützen
- Netzwerkkonnektivität zwischen dem Quellserver und dem Ziel-EC2-Server über ein privates Netzwerk mithilfe von AWS Direct Connect oder einem Virtual Private Network (VPN) oder über das Internet

Einschränkungen

- Die neueste Liste der unterstützten Regionen finden Sie unter Unterstützte AWS-Regionen.
- Eine Liste der unterstützten Betriebssysteme finden Sie im Abschnitt Unterstützte Betriebssysteme und im Abschnitt Allgemein unter Häufig FAQs zu Amazon EC2.

Architektur

Quelltechnologie-Stack

- Ein physischer, virtueller oder in der Cloud gehosteter Server, auf dem ein von Amazon EC2 unterstütztes Betriebssystem ausgeführt wird

Zieltechnologie-Stack

- Eine Amazon EC2-Instance, auf der dasselbe Betriebssystem wie die Quell-VM ausgeführt wird
- Amazon Elastic Block Store (Amazon EBS)

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die High-Level-Architektur und die Hauptkomponenten der Lösung. Im On-Premises-Rechenzentrum gibt es virtuelle Maschinen mit lokalen Festplatten. Auf AWS gibt es einen Staging-Bereich mit Replikationsservern und einen Bereich für migrierte Ressourcen mit EC2-Instances zum Testen und Cutover. Beide Subnetze enthalten EBS-Volumes.

1. Initialisieren Sie AWS Application Migration Service.
2. Richten Sie die Konfiguration und Berichterstattung des Servers des Staging-Bereichs ein, einschließlich der Ressourcen des Staging-Bereichs.
3. Installieren Sie Agenten auf Quellservern und verwenden Sie die kontinuierliche Datenreplikation auf Blockebene (komprimiert und verschlüsselt).
4. Automatisieren Sie die Orchestrierung und die Systemkonvertierung, um das Cutover-Fenster zu verkürzen.

Netzwerkarchitektur

Das folgende Diagramm zeigt die allgemeine Architektur und die wichtigsten Komponenten der Lösung aus Netzwerksicht, einschließlich der erforderlichen Protokolle und Ports für die Kommunikation zwischen primären Komponenten im On-Premises-Rechenzentrum und in AWS.

Tools

- AWS Application Migration Service hilft Ihnen dabei, Anwendungen ohne Änderungen und mit minimaler Ausfallzeit in die AWS Cloud zu hosten (Lift and Shift durchzuführen).

Bewährte Methoden

- Nehmen Sie den Quellserver erst offline und führen Sie einen Neustart durch, wenn der Cutover auf die EC2-Ziel-Instance abgeschlossen ist.
- Geben Sie den Benutzern ausreichend Gelegenheit, Benutzerakzeptanztests (UAT) auf dem Zielserver durchzuführen, um Probleme zu identifizieren und zu beheben. Idealerweise sollten diese Tests mindestens zwei Wochen vor dem Cutover beginnen.
- Überwachen Sie häufig den Serverreplikationsstatus in der Application Migration Service-Konsole, um Probleme frühzeitig zu identifizieren.
- Verwenden Sie temporäre AWS Identity and Access Management (IAM)-Anmeldeinformationen für die Agent-Installation anstelle dauerhafter IAM-Benutzeranmeldeinformationen.

Polen

Generieren von AWS-Anmeldeinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle des AWS Replication Agent.	Melden Sie sich mit Administratorberechtigungen für das AWS-Konto an. Erstellen Sie in der AWS Identity and Access Management (IAM)-Konsole eine IAM-Rolle:	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Wählen Sie in der IAM-Konsole Rollen aus. 2. Wählen Sie Rolle erstellen aus. 3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen im Abschnitt Vertrauenswürdiger Entitätstyp die Option AWS-Konto aus. 4. Wählen Sie im Abschnitt Ein AWS-Konto die Option Dieses Konto (<account-id>) aus. 5. Wählen Sie Weiter aus. 6. Suchen Sie auf der Seite Berechtigungen hinzufügen nach der `AWSApplicationMigrationAgentInstallationPolicy` Richtlinie und aktivieren Sie das Kontrollkästchen neben dem Richtlinennamen. 7. Wählen Sie Weiter aus. 8. Geben Sie auf der Seite Rollendetails MGN_Agent_Installation_Role als Rollennamen ein. 9. Überprüfen Sie, ob die Felder korrekt sind, und wählen Sie dann Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie temporäre Sicherheitsanmeldeinformationen.	Melden Sie sich auf einem Computer mit installierter AWS Command Line Interface (AWS CLI) mit Administratorberechtigungen an. Oder melden Sie sich alternativ (innerhalb einer unterstützten AWS-Region) in der AWS-Managementkonsole mit Administratorberechtigungen für das AWS-Konto an und öffnen Sie AWS CloudShell. Generieren Sie temporäre Anmeldeinformationen mit dem folgenden Befehl und ersetzen Sie durch `<account-id>` die AWS-Konto-ID. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/MGN_Agent_Installation_Role --role-session-name mgn_installation_session_role` Kopieren Sie aus der Ausgabe des Befehls die Werte für `AccessKeyId` `SecretAccessKey` , und `SessionToken` . Speichern Sie sie an	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einem sicheren Ort für die spätere Verwendung. Wichtig: Diese temporäre n Anmeldeinformationen laufen nach einer Stunde ab. Wenn Sie nach einer Stunde Anmeldeinformationen benötigen, wiederholen Sie die vorherigen Schritte.	

Initialisieren des Application Migration Service und Erstellen der Vorlage für Replikationseinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie den Service.	Melden Sie sich in der -Konsole mit Administr atorberechtigungen für das AWS-Konto an. Wählen Sie Application Migration Service und dann Erste Schritte aus.	AWS-Administrator, Migration singenieur
Erstellen und konfigurieren Sie die Vorlage für Replikati onseinstellungen.	1. Geben Sie die folgenden Konfigurationsdetails an: a. Wählen Sie das Subnetz des Staging-Bereichs aus. b. Wählen Sie den Instance-Typ des Replikationsservers aus (`t3.small`standardm äßig).	AWS-Administrator, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Wählen Sie den EBS-Volume-Typ aus (standardmäßig gp3). d. Wählen Sie die Option EBS-Verschlüsselung aus. e. Stellen Sie sicher, dass das Kontrollkästchen Sicherheitsgruppe des Anwendungsmigratio nsdienstes immer verwenden aktiviert ist. f. Aktivieren Sie das Kontrollkästchen Private IP für die Datenrepl ikation (VPN, VPC Peering) verwenden DirectConnect, wenn Sie private Netzwerkk onnektivität zwischen der On-Premises-Umgebung und AWS verwenden. g. Aktivieren Sie das Kontrollkästchen Netzwerkbandbreite drosseln (pro Server – in Mbit/s), wenn Sie die Netzwerkbandbreite für Application Migration Service einschränken möchten. 2. Wählen Sie Create template (Vorlage erstellen) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Application Migration Service erstellt automatisch alle IAM-Rollen, die für die Datenrepl ikation und den Start migrierter Server erforderlich sind.	

Installieren von AWS Replication Agents auf Quellcomputern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die erforderlichen AWS-Anmeldeinformationen bereit.	Wenn Sie die Installat ionsdatei auf einem Quellserv er ausführen, müssen Sie die temporären Anmeldein formationen eingeben, die Sie zuvor generiert haben, einschließlich `AccessKey Id SecretAccessKey` , und `SessionToken` .	Migrationsingenieur, AWS-Administrator
Installieren Sie für Linux-Ser ver den Agenten.	Kopieren Sie den -Befehl des Installationsprogramms, melden Sie sich bei Ihren Quellservern an und führen Sie das Installationsprogramm aus. Detaillierte Anweisungen finden Sie in der AWS-Dokum entation.	AWS-Administrator, Migration singenieur
Installieren Sie für Windows-S erver den Agenten.	Laden Sie die Installat ionsdatei auf jeden Server herunter und führen Sie dann den Installationsbefehl aus. Detaillierte Anweisungen	AWS-Administrator, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der AWS-Dokumentation.	
Warten Sie, bis die erste Datenreplikation abgeschlossen ist.	Wenn der Agent installiert wurde, wird der Quellserver in der Application Migration Service-Konsole im Abschnitt Quellserver angezeigt. Warten Sie, bis der Server einer ersten Datenreplikation unterzogen wird.	AWS-Administrator, Migrationsingenieur

Konfigurieren von Starteinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Serverdetails an.	Wählen Sie in der Application Migration Service-Konsole den Abschnitt Quellserver und dann einen Servernamen aus der Liste aus, um auf die Serverdetails zuzugreifen.	AWS-Administrator, Migrationsingenieur
Konfigurieren Sie die Starteinstellungen.	Wählen Sie die Registerkarte Starteinstellungen aus. Sie können eine Vielzahl von Einstellungen konfigurieren, einschließlich allgemeiner Starteinstellungen und EC2-Startvorlageneinstellungen. Detaillierte Anweisungen finden Sie in der AWS-Dokumentation.	AWS-Administrator, Migrationsingenieur

Durchführen eines Tests

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Quellserver.	1. Stellen Sie in der Application Migration Service-Konsole im Abschnitt Quellserver sicher, dass der Migrationslebenszyklus der Quellserver zum Testen bereit ist und dass der Datenreplikationsstatus Zustand ist. 2. Aktivieren Sie das Kontrollkästchen links neben jedem Quellserver. 3. Wählen Sie Test und Cutover und dann Test-Instance starten aus. 4. Wenn Sie dazu aufgefordert werden, wählen Sie Starten aus. Die Server werden gestartet.	AWS-Administrator, Migrationsingenieur
Überprüfen Sie, ob der Test erfolgreich abgeschlossen wurde.	Nachdem der Testserver vollständig gestartet wurde, zeigt der Status Warnungen auf der Seite für jeden Server Launched an.	AWS-Administrator, Migrationsingenieur
Testen Sie den Server.	Führen Sie Tests mit dem Testserver durch, um sicherzustellen, dass er wie erwartet funktioniert.	AWS-Administrator, Migrationsingenieur

Planen und Durchführen eines Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie ein Cutover-Fenster.	Planen Sie einen geeigneten Cutover-Zeitrahmen mit relevanten Teams.	AWS-Administrator, Migrationsingenieur
Führen Sie den Cutover durch.	1. Aktivieren Sie auf der Konsole für Anwendungsmigration auf der Seite Quellserver das Kontrollkästchen links neben jedem Quellserver. 2. Wählen Sie Test und Cutover und dann Als „Bereit für Cutover“ markieren aus. 3. Stellen Sie sicher, dass der Migrationslebenszyklus jedes Quellservers für den Cutover bereit ist. 4. Wählen Sie Test und Cutover und dann Cutover-Instances starten aus. 5. Wenn Sie dazu aufgefordert werden, wählen Sie Starten aus. Die Server werden gestartet. Der Migrationslebenszyklus des Quellservers ändert sich in Cutover läuft .	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob der Cutover erfolgreich abgeschlossen wurde.	Nachdem die Cutover-Server vollständig gestartet wurden, zeigt der Status Warnungen auf der Seite Quellserver die Option Für jeden Server gestartet an.	AWS-Administrator, Migrationsingenieur
Testen Sie den Server.	Führen Sie Tests mit dem Cutover-Server durch, um sicherzustellen, dass er wie erwartet funktioniert.	AWS-Administrator, Migrationsingenieur
Schließen Sie den Cutover ab.	Wählen Sie Test und Cutover und dann Cutover abschließen aus, um den Migrationsprozess abzuschließen.	AWS-Administrator, Migrationsingenieur

Zugehörige Ressourcen

- AWS Application Migration Service
- AWS Application Migration Service-Benutzerhandbuch

Migrieren Sie kleine Datensätze mithilfe von AWS SFTP von der lokalen Infrastruktur zu Amazon S3

R-Typ: Rehost	Quelle: Speicher	Ziel: Amazon S3
Erstellt von: AWS	Umgebung: Produktion	Technologien: Speicher und Backup; Migration
AWS-Dienste: Amazon S3		

Übersicht

Dieses Muster beschreibt, wie kleine Datenmengen (5 TB oder weniger) von lokalen Rechenzentren zu Amazon Simple Storage Service (Amazon S3) mithilfe von AWS Transfer for SFTP (AWS SFTP) migriert werden. Bei den Daten kann es sich entweder um Datenbank-Dumps oder um Flatfiles handeln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Direct Connect, die zwischen Ihrem Rechenzentrum und AWS hergestellt wurde

-Einschränkungen

- Die Datendateien müssen weniger als 5 TB groß sein. Für Dateien über 5 TB können Sie einen mehrteiligen Upload auf Amazon S3 durchführen oder eine andere Datenübertragungsmethode wählen.

Architektur

Quelltechnologie-Stack

- Lokale Flatfiles oder Datenbank-Dumps

Zieltechnologie-Stack

- Amazon S3

Quell- und Zielarchitektur

Tools

- AWS SFTP — Ermöglicht die direkte Übertragung von Dateien in und aus Amazon S3 mithilfe des Secure File Transfer Protocol (SFTP).
- AWS Direct Connect — Stellt eine dedizierte Netzwerkverbindung von Ihren lokalen Rechenzentren zu AWS her.
- VPC-Endpunkte — Ermöglicht es Ihnen, eine VPC privat mit unterstützten AWS-Services und VPC-Endpunktservices zu verbinden, die von AWS bereitgestellt werden, PrivateLink ohne dass ein Internet-Gateway, ein NAT-Gerät (Network Address Translation), eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung erforderlich ist. Instances in einer VPC benötigen keine öffentlichen IP-Adressen, um mit Ressourcen im Service zu kommunizieren.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie die aktuellen SFTP-Anfo rderungen.		Inhaber der Anwendung, SA
Identifizieren Sie die Authentif izierungsanforderungen.	Zu den Anforderungen können eine schlüssel basierte Authentifizierung, ein Benutzername oder ein Passwort oder ein Identität sanbieter (IdP) gehören.	Inhaber der Anwendung, SA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Anforderungen an die Anwendung sintegration.		Besitzer der Anwendung
Identifizieren Sie die Benutzer, die den Dienst benötigen.		Besitzer der Anwendung
Ermitteln Sie den DNS-Namen für den SFTP-Serverendpunkt.		Netzwerk
Ermitteln Sie die Backup-Strategie.		SA, DBA (wenn Daten übertragen werden)
Identifizieren Sie die Strategie für die Anwendungsmigration oder -umstellung.		Inhaber der Anwendung, SA, DBA

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine oder mehrere virtuelle private Clouds (VPCs) und Subnetze in Ihrem AWS-Konto.		Inhaber der Anwendung, AMS
Erstellen Sie die Sicherheitsgruppen und die Network Access Control List (ACL).		Sicherheit, Netzwerke, AMS
Erstellen Sie den S3-Bucket.		Inhaber der Anwendung, AMS
Erstellen Sie die Rolle Identity and Access Management (IAM).	Erstellen Sie eine IAM-Richtlinie, die die Berechtigungen enthält, um AWS SFTP den Zugriff auf Ihren S3-Bucket	Sicherheit, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zu ermöglichen. Diese IAM-Richtlinie bestimmt, welche Zugriffsebene Sie SFTP-Benutzern gewähren. Erstellen Sie eine weitere IAM-Richtlinie, um eine Vertrauensbeziehung mit AWS SFTP aufzubauen.	
Ordnen Sie eine registrierte Domain zu (optional).	Wenn Sie eine eigene registrierte Domain haben, können Sie diese mit dem SFTP-Server verknüpfen. Sie können SFTP-Verkehr von einer Domain oder von einer Subdomain an Ihren SFTP-Serverendpunkt weiterleiten.	Netzwerke, AMS
Erstellen Sie einen SFTP-Server.	Geben Sie den Identitätsanbietertyp an, den der Dienst zur Authentifizierung Ihrer Benutzer verwendet.	Inhaber der Anwendung, AMS
Öffnen Sie einen SFTP-Client.	Öffnen Sie einen SFTP-Client und konfigurieren Sie die Verbindung für die Verwendung des SFTP-Endpunkthosts. AWS SFTP unterstützt jeden Standard-SFTP-Client. Zu den häufig verwendeten SFTP-Clients gehören OpenSSH, WinSCP, Cyberduck und. FileZilla Sie können den Hostnamen des SFTP-Servers von der AWS-SFTP-Konsole abrufen.	Besitzer der Anwendung, AMS

Planen und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie die Anwendungsmigration.	Planen Sie alle erforderlichen Änderungen an der Anwendungskonfiguration ein, legen Sie das Migrationsdatum fest und legen Sie den Testplan fest.	Inhaber der Anwendung, AMS
Testen Sie die Infrastruktur.	Testen Sie in einer Umgebung außerhalb der Produktionsumgebung.	Inhaber der Anwendung, AMS

Zugehörige Ressourcen

Referenzen

- AWS Transfer for SFTP — Benutzerhandbuch
- AWS Direct Connect Connect-Ressourcen
- VPC-Endpunkte

Tutorials und Videos

- AWS Transfer for SFTP (Video)
- AWS Transfer for SFTP — Benutzerhandbuch
- AWS SA Whiteboarding — Direktverbindung (Video)

Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk

R-Typ: Rehost	Quelle: Anwendungsentwicklung	Ziel: AWS Elastic Beanstalk
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Container und Mikroservices; Web- und mobile Apps; Migration
Arbeitslast: Open Source; Oracle	AWS-Dienste: AWS Elastic Beanstalk	

Übersicht

Dieses Muster beschreibt, wie eine Java-Anwendung, die auf einem lokalen GlassFish Oracle-Server ausgeführt wird, zu AWS Elastic Beanstalk in der AWS-Cloud migriert wird.

Auf AWS wird die Java-Anwendung auf einem GlassFish Docker-Server mit AWS Elastic Beanstalk bereitgestellt, der in einer Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppe ausgeführt wird.

Zusätzliche Funktionen:

- Amazon Elastic Beanstalk fungiert als Wrapper für mehrere zugrunde liegende Ressourcen. Es richtet Elastic Load Balancing ein (das den eingehenden Verkehr von Amazon Route 53 verarbeitet), verteilt den Datenverkehr auf eine oder mehrere EC2-Instances und dient auch als Bereitstellungstool.
- Um eine lokale Datenbank zu Amazon Relational Database Service (Amazon RDS) zu migrieren, aktualisieren Sie die Datenbankverbindungsdetails. In der Backend-Datenbank können Sie Amazon RDS Multi-AZ-Bereitstellungen konfigurieren und den Datenbank-Engine-Typ auswählen.
- Sie können die Multi-AZ-Bereitstellung für hohe Verfügbarkeit zusammen mit der Auto Scaling-Gruppe und der Skalierungsrichtlinie verwenden, um die Ausfallsicherheit zu verbessern.
- Sie können eine Skalierungsrichtlinie einrichten, die auf CloudWatch Amazon-Metriken basiert.
- In AWS Elastic Beanstalk können Sie die zugrunde liegenden Elastic Load Balancing Balancing-Einstellungen und Amazon EC2 Auto Scaling konfigurieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine lokale Java-Anwendung, die auf läuft GlassFish
- Eine WAR-Datei (Java Web Application Resource)

Produktversionen

- Oracle Glassfish 4.1.2 und 5.0
- Java 7 4.0 GlassFish
- Java 8 GlassFish 4.1 oder höher

Architektur

Quelltechnologie-Stack

- Anwendungen, die in entwickelt wurden GlassFish

Zieltechnologie-Stack

- Elastic Beanstalk

Zielarchitektur

Arbeitsablauf bei der Bereitstellung

Tools

- Amazon Elastic Beanstalk — Ein Service für die Bereitstellung und Skalierung von Webanwendungen und Services, die mit Java, .NET, PHP, Node.js, Python, Ruby, Go und Docker auf Servern wie Apache, NGINX, Passenger und IIS entwickelt wurden.

- Amazon CloudWatch — Bietet Daten und umsetzbare Erkenntnisse zur Überwachung von Anwendungen, reagiert auf systemweite Leistungsänderungen, optimiert die Ressourcennutzung und bietet einen einheitlichen Überblick über den Betriebsstatus.
- Docker — Eine Plattform, die Software in standardisierte Einheiten verpackt, um Anwendungen schnell zu erstellen, zu testen und bereitzustellen.
- Java — Eine Allzweck-Programmiersprache. Java ist klassenbasiert, objektorientiert und so konzipiert, dass es weniger Implementierungsabhängigkeiten aufweist.

Epen

Richten Sie eine VPC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Virtual Private Cloud (VPC) -Instanz mit den erforderlichen Informationen.		SysAdmin
Erstellen Sie mindestens zwei Subnetze innerhalb der VPC.		SysAdmin
Erstellen Sie eine Routing-Tabelle gemäß den Anforderungen.		SysAdmin

Amazon S3 einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-Simple-Storage-Service-(Amazon S3)-Bucket.		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die WAR-Datei in den S3-Bucket und laden Sie den Anwendungscode hoch.		SysAdmin

Erstellen einer IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Identity and Access Management (IAM) -Rolle.	Sie können das Standardprofil „aws-elasticbeanstalk-ec2-role“ verwenden oder es von Elastic Beanstalk automatisch erstellen lassen.	SysAdmin

Elastic Beanstalk einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie das Elastic Beanstalk-Dashboard.		SysAdmin
Erstellen Sie eine neue Anwendung und wählen Sie die Webserver-Umgebung aus.		SysAdmin
Wählen Sie GlassFish Docker als vorkonfigurierte Plattform.		SysAdmin
Laden Sie den Code hoch.	Geben Sie die URL der S3-Bucket-Datei oder die ZIP-Datei aus den lokalen Systemdateien an.	SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Umgebungstyp aus.	Wählen Sie in den Einstellungen für die Konfigurationskapazität entweder Single Instance oder Load Balancer aus.	SysAdmin
Konfigurieren Sie den Load Balancer.	Wenn Sie im vorherigen Schritt Load Balancer ausgewählt haben, konfigurieren Sie die Multi-AZ-Bereitstellung.	SysAdmin
Wählen Sie in den Sicherheitseinstellungen der Konfiguration die zuvor erstellte IAM-Rolle aus.		SysAdmin
Wenn Sie unter Konfiguration und Sicherheitseinstellungen ein vorhandenes key pair haben, verwenden Sie es oder erstellen Sie ein neues Amazon EC2 EC2-Schlüsselpaar.		SysAdmin
Konfigurieren Sie Amazon in den Einstellungen für die Konfigurationsüberwachung CloudWatch.		SysAdmin
Wählen Sie in den Einstellungen für die Konfigurationssicherheit die zuvor erstellte VPC aus.		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie Umgebung erstellen aus.		SysAdmin

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendung mithilfe der URL, die in der erstellten Umgebung bereitgestellt wurde.		
Wenden Sie die DNS-Änderungen (Domain Name Service) in Amazon Route 53 an.		

Zugehörige Ressourcen

- GlassFish Oracle-Dokumentation
- GlassFish Open-Source-Java-EE-Referenzimplementierung
- Dokumentation zu AWS Elastic Beanstalk
- Elastic Beanstalk mit Amazon verwenden CloudWatch
- Preise für AWS Elastic Beanstalk
- EC2 Auto Scaling Scaling-Gruppe
- Skalieren Sie die Größe Ihrer Auto Scaling Scaling-Gruppe
- Amazon RDS Multi-AZ-Bereitstellungen

Migrieren einer lokalen Oracle-Datenbank zu Oracle auf Amazon EC2

Erstellt von Bolji Shaik (AWS) und Pankaj Choudhary (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Oracle auf Amazon EC2
R-Typ: Hostwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon EC2		

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer On-Premises-Oracle-Datenbank zu Oracle auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance. Es werden zwei Optionen für die Migration beschrieben: die Verwendung von AWS Data Migration Service (AWS DMS) oder die Verwendung nativer Oracle-Tools wie RMAN, Data Pump Import/Export, Transportable Tablespaces und Oracle GoldenGate.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem On-Premises-Rechenzentrum

Einschränkungen

- Das Zielbetriebssystem (OS) muss von Amazon EC2 unterstützt werden. Eine vollständige Liste der unterstützten Systeme finden Sie unter Häufig FAQs zu Amazon EC2.

Produktversionen

- Oracle-Versionen 10.2 und höher (für Versionen 10.x), 11g und bis zu 12.2 und 18c für die Editionen Enterprise, Standard, Standard One und Standard Two. Die neueste Liste der von

AWS DMS unterstützten Versionen finden Sie unter „On-Premises- und Amazon EC2-Instance-Datenbanken“ unter Quellen für die Datenmigration in der AWS DMS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Oracle-Datenbank

Zieltechnologie-Stack

- Eine Oracle-Datenbank-Instance auf Amazon EC2

Zielarchitektur

Datenmigrationsarchitektur

Verwenden von AWS DMS:

Verwenden nativer Oracle-Tools:

Tools

- AWS DMS – AWS Database Migration Services (AWS DMS) unterstützt verschiedene Arten von Quell- und Zieldatenbanken. Informationen zu den unterstützten Datenbankversionen und Editionen finden Sie unterVerwenden einer Oracle-Datenbank als Quelle für AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden.
- Native Oracle-Tools – RMAN, Data Pump Import/Export, Transportable Tablespaces, Oracle GoldenGate

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen der Quell- und Zieldaten banken.		DBA
Identifizieren Sie die Version des Zielbetriebssystems.		DBA, SysAdmin
Identifizieren Sie Hardwarea nforderungen für die Zielserve r-Instance basierend auf der Oracle-Kompatibilitätsliste und den Kapazitätsanforderungen.		DBA, SysAdmin
Identifizieren Sie Speichera nforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Identifizieren Sie Netzwerka nforderungen (Latenz und Bandbreite).		DBA, SysAdmin
Wählen Sie basierend auf Kapazität, Speicherfunktionen und Netzwerkfunktionen den richtigen Instance-Typ aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerk-/Hostzugriff für Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie eine Liste der Betriebssystembenutzer,		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
die für die Oracle-Softwareinstallation erforderlich sind.		
Laden Sie das AWS Schema Conversion Tool (AWS SCT) und die Treiber herunter.		DBA
Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindung mit der Quelldatenbank her.		DBA
Generieren Sie SQL-Dateien für die Erstellung von Objekten (Tabellen, Indizes, Sequenzen usw.).		DBA
Legen Sie eine Backup-Strategie fest.		DBA, SysAdmin
Bestimmen Sie die Verfügbarkeitsanforderungen.		DBA
Identifizieren Sie die Strategie für Anwendungsmigration/-wechsel.		DBA, SysAdmin, App-Besitzer

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze in Ihrem AWS-Konto.		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten (ACLs).		SysAdmin
Konfigurieren und starten Sie die EC2-Instance.		SysAdmin

Installieren der Oracle-Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Betriebss ystembenutzer und -gruppen, die für die Oracle-Software erforderlich sind.		DBA, SysAdmin
Laden Sie die erforderliche Version der Oracle-Software herunter.		
Installieren Sie die Oracle-So ftware auf der EC2-Instance.		DBA, SysAdmin
Erstellen Sie Objekte wie Tabellen, Primärschlüssel, Ansichten und Sequenzen mithilfe der von AWS SCT generierten Skripts.		DBA

Daten migrieren – Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native Oracle-Tools oder Tools von Drittanbi	Zu den Oracle-Tools gehören Import/Export von Data	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
etern, um Datenbankobjekte und -daten zu migrieren.	Pump, RMAN, Transportable Tablespaces und GoldenGate.	

Daten migrieren – Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie die Migration smethode.		DBA
Erstellen Sie eine Replikati ons-Instance in der AWS DMS-Konsole.		DBA
Erstellen Sie Quell- und Zielendpunkte.		DBA
Erstellen Sie eine Replikati onsaufgabe.		DBA
Aktivieren Sie Change Data Capture (CDC), um Änderungen für eine kontinuie rliche Replikation zu erfassen.		DBA
Führen Sie die Replikati onsaufgabe aus und überwachen Sie die Protokoll e.		DBA
Erstellen Sie sekundäre Objekte wie Indizes und Fremdschlüssel, wenn der vollständige Ladevorgang abgeschlossen ist.		DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, SysAdmin, App-Besitzer

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie für Anwendungs-Cutover/-Umschaltung.		DBA, SysAdmin, App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS Secrets Manager-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin, App-Besitzer
Erfassen Sie Metriken zur Zeit der Migration, % des manuellen im Vergleich zum Tool, Kosteneinsparungen usw.		DBA, SysAdmin, App-Besitzer
Schließen Sie das Projekt ab und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- Strategien für die Migration von Oracle-Datenbanken zu AWS
- Migrieren von Oracle-Datenbanken in die AWS Cloud
- Amazon EC2-Website
- AWS DMS-Website
- AWS DMS-Blogbeiträge
- Amazon EC2 – Preise
- Lizenzierung von Oracle-Software in der Cloud Computing-Umgebung

Tutorials und Videos

- Erste Schritte mit Amazon EC2
- Erste Schritte mit AWS DMS
- Einführung in Amazon EC2 – Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren einer lokalen Oracle-Datenbank zu Amazon EC2 mithilfe von Oracle Data Pump

Erstellt von Navah Boluri (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises-Oracle-Datenbank	Ziel: Oracle-Datenbank auf Amazon EC2
R-Typ: Hostwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon EC2; AWS Direct Connect		

Übersicht

Bei der Migration von Datenbanken müssen Sie Faktoren wie die Quell- und Zieldatenbank-Engines und -Versionen, Migrationstools und -Services sowie akzeptable Ausfallzeiten berücksichtigen. Wenn Sie eine lokale Oracle-Datenbank zu Amazon Elastic Compute Cloud (Amazon EC2) migrieren, können Sie Oracle-Tools wie Oracle Data Pump und Oracle Recovery Manager (RMAN) verwenden. Weitere Informationen zu -Strategien finden Sie unter Migrieren von Oracle-Datenbanken in die AWS Cloud.

Oracle Data Pump hilft Ihnen, die logische, konsistente Sicherung der Datenbank zu extrahieren und sie auf der EC2-Ziel-Instance wiederherzustellen. Dieses Muster beschreibt, wie eine lokale Oracle-Datenbank mithilfe von Oracle Data Pump und dem `NETWORK_LINK` Parameter mit minimalen Ausfallzeiten zu einer EC2-Instance migriert wird. Der `NETWORK_LINK` Parameter startet einen Import über einen Datenbanklink. Der Oracle Data Pump Import (impdp)-Client auf der EC2-Ziel-Instance stellt eine Verbindung zur Quelldatenbank her, ruft Daten aus dieser ab und schreibt die Daten direkt in die Datenbank auf der Ziel-Instance. Es gibt keine Backup- oder Dump-Dateien, die in dieser Lösung verwendet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- Eine lokale Oracle-Datenbank, die:
  - Ist keine Oracle Real Application Clusters (RAC)-Datenbank
  - Ist keine Oracle Automatic Storage Management (Oracle ASM)-Datenbank
  - Befindet sich im Lese-/Schreibmodus.
- Sie haben einen AWS Direct Connect-Link zwischen Ihrem On-Premises-Rechenzentrum und AWS erstellt. Weitere Informationen finden Sie unter Erstellen einer Verbindung (Direct-Connect-Dokumentation).

Produktversionen

- Oracle Database 10g Version 1 (10.1) und höher

Architektur

Quelltechnologie-Stack

- Ein eigenständiger (Nicht-RAC- und Nicht-ASM) Oracle-Datenbankserver in einem On-Premises-Rechenzentrum

Zieltechnologie-Stack

- Eine Oracle-Datenbank, die auf Amazon EC2 ausgeführt wird

Zielarchitektur

Die Säule der Zuverlässigkeit des AWS Well-Architected Framework empfiehlt, Datensicherungen zu erstellen, um eine hohe Verfügbarkeit und Stabilität zu gewährleisten. Weitere Informationen finden Sie unter Entwerfen einer Architektur für hohe Verfügbarkeit in Bewährte Methoden für die Ausführung von Oracle Database in AWS . Dieses Muster richtet mithilfe von Oracle Active Data Guard Primär- und Standby-Datenbanken auf EC2-Instances ein. Für eine hohe Verfügbarkeit sollten sich die EC2-Instances in unterschiedlichen Availability Zones befinden. Die Availability Zones können sich jedoch in derselben AWS-Region oder in verschiedenen AWS-Regionen befinden.

Active Data Guard bietet schreibgeschützten Zugriff auf eine physische Standby-Datenbank und wendet Redo-Änderungen kontinuierlich von der Primärdatenbank aus an. Basierend auf Ihrem Recovery Point Objective (RPO) und Recovery Time Objective (RTO) können Sie zwischen synchronen und asynchronen Redo-Transportoptionen wählen.

Die folgende Abbildung zeigt die Zielarchitektur, wenn sich die primären und Standby-EC2-Instances in unterschiedlichen AWS-Regionen befinden.

Datenmigrationsarchitektur

Nachdem Sie die Zielarchitektur eingerichtet haben, verwenden Sie Oracle Data Pump, um die On-Premises-Daten und Schemata zur primären EC2-Instance zu migrieren. Während des Cutover können Anwendungen nicht auf die On-Premises-Datenbank oder die Zieldatenbank zugreifen. Sie schalten diese Anwendungen herunter, bis sie mit der neuen Zieldatenbank auf der primären EC2-Instance verbunden werden können.

Die folgende Abbildung zeigt die Architektur während der Datenmigration. In dieser Beispielarchitektur befinden sich die primären und Standby-EC2-Instances in unterschiedlichen AWS-Regionen.

Tools

AWS-Services

- AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

Andere Tools und Services

- Oracle Active Data Guard unterstützt Sie beim Erstellen, Verwalten und Überwachen von Standby-Datenbanken.
- Mit Oracle Data Pump können Sie Daten und Metadaten mit hohen Geschwindigkeiten von einer Datenbank in eine andere verschieben.

Bewährte Methoden

- Bewährte Methoden für die Ausführung von Oracle Database in AWS
- Importieren von Daten mit NETWORK_LINK

Polen

Einrichten der EC2-Instances in AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Quellhardwarekonfiguration für den On-Premises-Host und die Kernel-Parameter.	Validieren Sie die On-Premises-Konfiguration, einschließlich Speichergröße, Eingabe-/Ausgabeoperationen pro Sekunde (IOPS) und CPU. Dies ist wichtig für die Oracle-Lizenzierung, die auf CPU-Kernen basiert.	DBA, SysAdmin
Erstellen Sie die Infrastruktur in AWS.	Erstellen Sie die Virtual Private Clouds (VPCs), privaten Subnetze, Sicherheitsgruppen, Netzwerkzugriffskontrolllisten (ACLs), Routing-Tabellen und das Internet-Gateway. Weitere Informationen finden Sie hier: • VPCs und Subnetze • Tutorial: Erstellen einer VPC zur Verwendung mit einer Datenbank-Instance	DBA, AWS-Systemadministrator
Richten Sie die EC2-Instances mithilfe von Active Data Guard ein.	Konfigurieren Sie AWS EC2-Instances mithilfe einer Active Data Guard-Konfiguration,	DBA, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wie im AWS Well-Architected Framework beschrieben. Die Version von Oracle Database auf der EC2-Instance kann sich von der On-Premis es-Version unterscheiden, da dieses Muster logische Backups verwendet. Beachten Sie Folgendes: • Setzen Sie die Zieldaten bank in den Lese-Schreib-Modus. • Geben Sie in der Zieldaten bank die TNS-Details (Transparent Network Bole) für die Quelldatenbank an. Weitere Informationen finden Sie hier: • Starten einer Datenbank (Oracle-Dokumentation) • Erstellen und Konfigurieren einer Oracle-Datenbank (Oracle-Dokumentation)	

Migrieren der Datenbank zu Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie von der EC2-Instance aus einen dblink zur On-Premises-Datenbank.	Erstellen Sie einen Datenbank link (dblink) zwischen der Oracle-Datenbank auf der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2-Instance und der lokalen Oracle-Datenbank. Weitere Informationen finden Sie unter Verwenden von Network Link Import zum Verschieben von Daten (Oracle-Dokumentation).	
Überprüfen Sie die Verbindung zwischen der EC2-Instance und dem On-Premises-Host.	Verwenden Sie den dblink, um zu bestätigen, dass die Verbindung zwischen der EC2-Instance und der On-Premises-Datenbank funktioniert. Anweisungen finden Sie unter CREATE DATABASE LINK (Oracle-Dokumentation).	DBA
Halten Sie alle Anwendungen an, die mit der On-Premises-Datenbank verbunden sind.	Nachdem die Datenbank ausfallzeit genehmigt wurde, fahren Sie alle Anwendungen und abhängigen Aufträge herunter, die zu Ihrer On-Premises-Datenbank gehören. Sie können dies entweder direkt aus der Anwendung oder aus der Datenbank mithilfe von Cron tun. Weitere Informationen finden Sie unter Verwenden des Crontab-Hilfsprogramms zum Planen von Aufgaben auf Oracle Linux.	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie den Datenmigr ationsauftrag.	Verwenden Sie auf dem Ziel-Host den Befehl , `impdb` um den Data Pump-Import zu planen. Dadurch wird die Zieldatenbank mit dem On-Premises-Host verbunden und die Datenmigration gestartet. Weitere Informationen finden Sie unter Data Pump Import und NETWORK_LINK (Oracle-Dokumentation).	DBA
Validieren Sie die Datenmigr ation.	Die Datenvalidierung ist ein entscheidender Schritt. Für die Datenvalidierung können Sie benutzerdefinierte Tools oder Oracle-Tools verwenden, z. B. eine Kombination aus dblink und SQL-Abfragen.	DBA

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Setzen Sie die Quelldate nbank in den schreibge schützten Modus.	Vergewissern Sie sich, dass die Anwendung heruntergefahren wird und keine Änderungen an der Quelldatenbank vorgenommen werden. Öffnen Sie die Quelldatenbank im schreibgeschützten Modus. Auf diese Weise können Sie offene Transaktionen vermeiden. Weitere Informati	DBA, DevOps Techniker, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen finden Sie unter `ALTER DATABASE` in SQL-Anweisungen (Oracle-Dokumentation).	
Validieren Sie die Anzahl der Objekte und die Daten.	Um die Daten und das Objekt zu validieren, verwenden Sie benutzerdefinierte Tools oder Oracle-Tools, z. B. eine Kombination aus dblink und SQL-Abfragen.	DBA, App-Entwickler
Verbinden Sie die Anwendungen mit der Datenbank auf der primären EC2-Instance.	Ändern Sie das Verbindungsattribut der Anwendung so, dass es auf die neue Datenbank verweist, die Sie auf der primären EC2-Instance erstellt haben.	DBA, App-Entwickler
Validieren Sie die Anwendungsleistung.	Starten Sie die Anwendung. Validieren Sie die Funktionalität und Leistung der Anwendung mithilfe von Automated Workload Repository (Oracle-Dokumentation).	App-Entwickler, DevOps Techniker, DBA

Zugehörige Ressourcen

AWS-Referenzen

- Migrieren von Oracle-Datenbanken in die AWS Cloud
- Amazon EC2 für Oracle
- Migrieren von großen Oracle-Datenbanken zu AWS für plattformübergreifende Umgebungen
- VPCs und Subnetze

- Tutorial: Erstellen einer VPC zur Verwendung mit einer Datenbank-Instance

Oracle-Referenzen

- Oracle Data Guard-Konfigurationen
- Data-Pump-Import

Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2

R-Typ: Rehost	Quelle: Datenbanken: Relational	Ziel: SAP Adaptive Server Enterprise auf Amazon EC2
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: SAP	AWS-Dienste: Amazon EC2	

Übersicht

Dieses Muster beschreibt, wie eine SAP Adaptive Server Enterprise (ASE) -Datenbank von einem lokalen Host zu einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance migriert wird. Das Muster deckt die Verwendung von AWS Database Migration Service (AWS DMS) oder nativen SAP ASE-Tools wie ASE Cockpit, Sybase Central for ASE und DBA Cockpit für die Migration ab.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine SAP ASE-Quelldatenbank in einem lokalen Rechenzentrum

-Einschränkungen

- Die Quelldatenbank muss weniger als 64 TB groß sein

Produktversionen

- SAP ASE Version 15.x und 16.x oder höher

Architektur

Quelltechnologie-Stack

- Lokale SAP ASE-Datenbank

Zieltechnologie-Stack

- SAP ASE-Datenbank auf einer EC2-Instanz

Architektur der Datenbankmigration

Verwenden von AWS DMS:

Verwendung nativer SAP ASE-Tools:

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) unterstützt mehrere verschiedene Quell- und Zieldatenbanken. Weitere Informationen finden Sie unter Quellen für die Datenmigration und Ziele für die Datenmigration. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.
- SAP ASE — Zu den systemeigenen Tools gehören ASE Cockpit, Sybase Central für ASE und DBA Cockpit.

Epen

Analysieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Zielversion des Betriebssystems.		DBA, SysAdmin
Identifizieren Sie die Hardwareanforderungen für		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
die Zielserverinstanz auf der Grundlage der SAP ASE-Kompatibilitätsliste und der Kapazitätsanforderungen.		
Identifizieren Sie die Anforderungen für den Speichertyp und die Kapazität.		DBA, SysAdmin
Identifizieren Sie die Netzwerkanforderungen, einschließlich Latenz und Bandbreite.		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp, die Kapazität, die Speicherfunktionen und die Netzwerkfunktionen aus.		DBA, SysAdmin
Identifizieren Sie die Netzwerk- und Hostzugriffssicherheitsanforderungen für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie eine Liste der Betriebssystembenutzer, die für die SAP ASE-Softwareinstallation erforderlich sind.		DBA, SysAdmin
Bestimmen Sie die Backup-Strategie.		DBA
Ermitteln Sie die Verfügbarkeitsanforderungen.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie für Anwendungsmigration und Switchover.		DBA, Besitzer der SysAdmin App

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen und die Network Access Control List (ACL).		SysAdmin
Konfigurieren und starten Sie die EC2-Instanz.		SysAdmin

Installieren Sie die Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Betriebss ystembenutzer und -gruppen, die für das Funktionieren der SAP ASE-Software erforderl ich sind.		DBA, SysAdmin
Laden Sie die erforderliche Version der SAP ASE-Softw are herunter.		DBA, SysAdmin
Installieren Sie die SAP ASE-Datenbank, die Backup-Se		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
rver-Software und die Replikati onsserversoftware auf der EC2-Instance und konfiguri eren Sie dann den Server.		

Migrieren Sie die Daten — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Datenbank objekte und Daten mithilfe systemeigener SAP ASE-Tools oder Tools von Drittanbi etern.	Informationen zu SAP ASE oder Tools von Drittanbietern finden Sie in der Dokumenta tion. Dazu gehören ASE Cockpit, Sybase Central für ASE und DBA Cockpit.	DBA

Migrieren Sie die Daten — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe von AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Umstellung oder Umstellung der Anwendung.		DBA, Besitzer der App SysAdmin

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, SysAdmin
Validieren und überprüfen Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparungen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		DBA SysAdmin, App-Besitzer

Zugehörige Ressourcen

Referenzen

- Amazon EC2
- AWS DMS
- Amazon EC2 EC2-Preise

Tutorials und Videos

- Erste Schritte mit Amazon EC2
- Erste Schritte mit AWS Database Migration Service
- AWS-Datenmigrationsservice (Video)
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2

R-Typ: Rehost	Quelle: Datenbanken: Relational	Ziel: Microsoft SQL Server auf Amazon EC2
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: Microsoft	AWS-Dienste: Amazon EC2	

Übersicht

Dieses Muster beschreibt, wie eine lokale Microsoft SQL Server-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance zu Microsoft SQL Server migriert wird. Es umfasst zwei Migrationsoptionen: die Verwendung von AWS Data Migration Service (AWS DMS) oder die Verwendung systemeigener Microsoft SQL Server-Tools wie Backup and Restore, Copy Database Wizard oder Copy and Attach Database.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein von Amazon EC2 unterstütztes Betriebssystem (eine vollständige Liste der unterstützten Betriebssystemversionen finden Sie unter Häufig gestellte Fragen zu Amazon EC2)
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum

Produktversionen

- Microsoft SQL Server-Versionen 2005, 2008, 2008R2, 2012, 2014, 2016 und 2017 für die Enterprise, Standard, Workgroup und Developer Editionen, wenn Sie AWS DMS verwenden. Verwenden Sie native Tools oder Tools von Drittanbietern, um Microsoft SQL Server Web oder Express Edition zu migrieren. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Ziel für AWS DMS.

Architektur

Quelltechnologie-Stack

- Lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Microsoft SQL Server-Datenbank auf einer EC2-Instanz

Zielarchitektur

Architektur der Datenmigration

- Verwenden von AWS DMS

- Verwendung nativer SQL Server-Tools

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) unterstützt Sie bei der Migration Ihrer Daten zu und von weit verbreiteten kommerziellen und Open-Source-Datenbanken, darunter Oracle, SQL Server, MySQL und PostgreSQL. Sie können AWS DMS verwenden, um Ihre Daten in die AWS Cloud, zwischen lokalen Instances (über eine AWS Cloud-Einrichtung) oder zwischen Kombinationen aus Cloud und lokalen Einrichtungen zu migrieren.
- Systemeigene Microsoft SQL Server-Tools — Dazu gehören Sicherung und Wiederherstellung, der Assistent zum Kopieren von Datenbanken sowie das Kopieren und Anfügen von Datenbanken.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Version des Zielbetriebssystems.		DBA, SysAdmin
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz auf der Grundlage der Microsoft SQL Server-Kompatibilitätsliste und der Kapazitätsanforderungen.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen für Typ und Kapazität.		DBA, SysAdmin
Identifizieren Sie die Netzwerkanforderungen, einschließlich Latenz und Bandbreite.		DBA, SysAdmin
Wählen Sie den EC2-Instance-Typ auf der Grundlage von Kapazität, Speicherfunktionen und Netzwerkfunktionen aus.		DBA, SysAdmin
Identifizieren Sie die Netzwerk- und Hostzugriffssicherheitsanforderungen		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
für die Quell- und Zieldaten banken.		
Identifizieren Sie eine Liste der Benutzer, die für die Microsoft SQL Server-Softwareins tallation erforderlich sind.		DBA, SysAdmin
Bestimmen Sie die Backup-St rategie.		DBA
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA
Identifizieren Sie die Strategie für die Anwendungsmigration und -umstellung.		DBA, SysAdmin

Konfiguration der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen und eine Network Access Control List (ACL).		SysAdmin
Konfigurieren und starten Sie eine EC2-Instanz.		SysAdmin

Installieren Sie die Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Benutzer und Gruppen, die für die Microsoft SQL Server-Software erforderl ich sind.		DBA, SysAdmin
Laden Sie die Microsoft SQL Server-Software herunter.		DBA, SysAdmin
Installieren Sie die Microsoft SQL Server-Software auf der EC2-Instanz und konfigurieren Sie den Server.		DBA, SysAdmin

Migrieren Sie die Daten — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native Microsoft SQL Server-Tools oder Tools von Drittanbietern, um die Datenbankobjekte und -daten zu migrieren.	Zu den Tools gehören Sicherung und Wiederher stellung, der Assistent zum Kopieren von Datenbank en sowie das Kopieren und Anfügen von Datenbanken.	DBA

Migrieren Sie die Daten — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe von AWS DMS.	Detaillierte Informationen zur Verwendung von AWS DMS finden Sie unter den Links	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Abschnitt Referenzen und Hilfe.	

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.	Verwenden Sie das AWS Schema Conversion Tool (AWS SCT), um den im Quellcode der Anwendung eingebetteten SQL-Code zu analysieren und zu ändern.	DBA, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Umstellung der Anwendung.		DBA, Besitzer der App SysAdmin

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie alle temporären AWS-Ressourcen herunter.	Zu den temporären Ressourcen gehören die AWS DMS-Replikationsinstanz und die EC2-Instance für AWS SCT.	DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparungen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		DBA SysAdmin, Besitzer der App

Zugehörige Ressourcen

Referenzen

- Bereitstellung von Microsoft SQL Server auf Amazon Web Services
- Amazon EC2
- Häufig gestellte Fragen zu Amazon EC2
- AWS Database Migration Service
- Amazon EC2 EC2-Preise
- Microsoft-Produkte auf AWS
- Microsoft-Lizenzierung auf AWS
- Microsoft SQL Server auf AWS

Tutorials und Videos

- Erste Schritte mit Amazon EC2
- Erste Schritte mit dem AWS Database Migration Service
- Fügen Sie Ihrem Verzeichnis eine Amazon EC2 EC2-Instance hinzu (Simple AD und Microsoft AD)

- AWS Database Migration Service (Video)
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2

R-Typ: Rehost	Quelle: Datenbanken: Relational	Ziel: MySQL auf Amazon EC2
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: Open Source		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen MySQL-Datenbank zu einer MySQL-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Das Muster beschreibt die Verwendung von AWS Database Migration Service (AWS DMS) oder nativen MySQL-Tools wie mysqldbcopy und mysqldump für die Migration.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine MySQL-Quelldatenbank in einem lokalen Rechenzentrum

Produktversionen

- MySQL-Versionen 5.5, 5.6 und 5.7
- Eine Liste der von Amazon EC2 unterstützten Zielbetriebssysteme finden Sie unter Häufig gestellte Fragen zu Amazon EC2

Architektur

Quelltechnologie-Stack

- Eine lokale MySQL-Datenbank

Zieltechnologie-Stack

- Eine MySQL-Datenbank-Instance auf Amazon EC2

AWS-Datenmigrationsmethoden

- AWS DMS
- Systemeigene MySQL-Tools (mysqldbcopy, mysqldump)

Zielarchitektur

AWS-Datenmigrationsarchitektur

Verwenden von AWS DMS:

Verwendung nativer MySQL-Tools:

Tools

- AWS DMS — AWS Database Migration Service (AWS DMS) unterstützt mehrere Quell- und Zieldatenbanken. Informationen zu MySQL-Quell- und Zieldatenbanken, die von AWS DMS unterstützt werden, finden Sie unter Migrieren von MySQL-kompatiblen Datenbanken zu AWS. Wenn Ihre Quelldatenbank nicht von AWS DMS unterstützt wird, müssen Sie eine andere Methode zur Migration Ihrer Daten wählen.
- Native MySQL-Tools — mysqldbcopy und mysqldump

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Version des Zielbetriebssystems.		DBA, SysAdmin
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz anhand der MySQL-Kompatibilitätsliste und der Kapazitätsanforder ungen.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Identifizieren Sie Netzwerka nforderungen wie Latenz und Bandbreite.		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerk- oder Hostzugriff für die Quell- und Zieldaten banken.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie eine Liste der Betriebssystembenutzer, die für die Installation der MySQL-Software erforderlich sind.		DBA, SysAdmin
Legen Sie eine Backup-St rategie fest.		DBA
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA
Identifizieren Sie die Strategie für die Anwendungsmigration oder den Umstieg.		DBA, SysAdmin

Konfiguration der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten (ACLs).		SysAdmin
Konfigurieren und starten Sie eine EC2-Instanz.		SysAdmin

Installieren Sie die MySQL-Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Betriebss ystembenutzer und -gruppen, die für das Funktionieren der MySQL-Software erforderlich sind.		DBA, SysAdmin
Laden Sie die erforderliche Version der MySQL-Software herunter.		DBA, SysAdmin
Installieren Sie die MySQL-Software auf der EC2-Insta nce und konfigurieren Sie den Server.		DBA, SysAdmin

Daten migrieren — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbi etern, um Datenbankobjekte und Daten zu migrieren.	Zu diesen Tools gehören mysqldbcopy und mysqldump.	DBA

Daten migrieren — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Umstellung oder Umstellung der Anwendung.		DBA, Besitzer der App SysAdmin

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.	Fahren Sie die AWS DMS-Replikationsinstanz herunter.	DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Daten im Vergleich zum Tool, zu Kosteneinsparungen usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA SysAdmin, Besitzer der App

Zugehörige Ressourcen

Referenzen

- Amazon EC2 EC2-Webseite
- AWS DMS-Webseite
- Amazon EC2 – Preise
- Schrittweise Anleitungen zu AWS DMS

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Reduzieren Sie die homogene Cutover-Zeit für die SAP-Migration mithilfe von Application Migration Service

Erstellt von Pavel Rubin (AWS), Diego Bolrde (AWS) und Sunil Yadav (AWS)

Umgebung: Produktion	Quelle: On-Premises-SAP-ASE-Datenbank	Ziel: SAP-Datenbank auf Amazon EC2
R-Typ: Hostwechsel	Workload: SAP	Technologien: Migration; Datenbanken
AWS-Services: AWS Application Migration Service; Amazon EBS		

Übersicht

Dieses Muster beschreibt die Schritte zur Migration von SAP-Workloads mithilfe von AWS Application Migration Service. Application Migration Service erleichtert Cutover, indem die Replikation auf Blockebene verwendet wird, um Replikations-Volumes aufrechtzuerhalten, die kontinuierlich von ihren Quellen synchronisiert werden.

SAP-Workloads umfassen die Anwendungen SAP Customer Relationship Management (SAP CRM), SAP Enterprise Resource Planning (ERP) und SAP Business Warehouse (SAP EO).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit stabiler Netzwerkkonnektivität zwischen Quell-SAP-Servern und der Ziel-VPC (Virtual Private Cloud) in AWS
- Eine Quelldatenbank von SAP Adaptive Server Enterprise (ASE) für Linux oder Windows in einem On-Premises-Rechenzentrum

Einschränkungen

- Das Zielbetriebssystem muss von Amazon Elastic Compute Cloud (Amazon EC2) unterstützt werden. Weitere Informationen finden Sie unter Häufig FAQs zu Amazon EC2.

Architektur

Quelltechnologie-Stack

- Eine SAP-ASE-Datenbank

Zieltechnologie-Stack

- Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Migration von den On-Premises-Servern über den Replication Agent zum Application Migration Service-Endpunkt. Ein Amazon Simple Storage Service (Amazon S3)-Endpunkt wird für den Zugriff auf Installations- und Konfigurationsdateien verwendet. Die Subnetze für den Staging-Bereich und die migrierten Ressourcen enthalten EC2-Instances mit Datenspeicherung auf EBS-Volumes. Port TCP 443 wird verwendet, um das Quellcomputernetzwerk mit Application Migration Service zu verbinden und die Staging-Bereich-Subnetze mit den regionalen Endpunkten von Application Migration Service, Amazon EC2 und Amazon S3 zu verbinden. Port TCP 1500 wird für die Datenreplikation zwischen dem lokalen Netzwerk und dem Staging-Bereich verwendet.

Tools

- AWS Application Migration Service unterstützt Sie beim Hostwechsel von (lift-and-shift)-Anwendungen in der AWS Cloud ohne Änderungen und mit minimalen Ausfallzeiten.
- Amazon Elastic Block Store (Amazon EBS) stellt Volumes für die Speicherung auf Blockebene für die Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2)-Instances bereit.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Token Service (AWS STS) hilft Ihnen, temporäre Anmeldeinformationen mit eingeschränkten Berechtigungen für Benutzer anzufordern.

Polen

Initialisieren des Application Migration Service

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Application Migration Service.	Initialisieren Sie Application Migration Service in der AWS-Region, in der Sie die SAP ASE-Datenbank bereitstellen möchten. AWS bietet eine automatisierte Einrichtung, wenn Sie zum ersten Mal in jeder Region zur Seite Application Migration Service navigieren.	AWS-Administrator
Erstellen Sie manuell Servicerollen.	(Optional) Wenn Sie Automatisierung (z. B. AWS Control Tower) verwenden möchten, um das Konto einzurichten, können Sie die sechs AWS Identity and Access Management (IAM)-Rollen, die für Installation, Replikation und Starts erforderlich sind, manuell erstellen. Anweisungen finden Sie in der AWS-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Vorlage für Replikationseinstellungen.	Die Vorlage für Replikationseinstellungen definiert das Subnetz, den Instance-Typ, die Amazon-EBS-Verschlüsselung und die Weiterleitung von Daten. Ausführliche Informationen zu Einstellungen finden Sie in der AWS-Dokumentation.	Allgemeines AWS

Generieren von Anmeldeinformationen für die Agent-Installation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue IAM-Rolle.	Navigieren Sie in der IAM-Konsole zu Rollen und wählen Sie Rolle erstellen aus. Wählen Sie für den Typ Vertrauenswürdige Entität die Option AWS-Konto und dann Weiter aus.	AWS-Systemadministrator
Fügen Sie AWSApplicationMigrationAgentPolicy an die IAM-Rolle an.	Die von AWS verwaltete `AWSApplicationMigrationAgentPolicy` Richtlinie enthält die erforderlichen Berechtigungen zum Durchführen der Installation des Application Migration Service Agent. Nachdem Sie die Richtlinie angefügt haben, wählen Sie Weiter aus.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Rollenerstellung ab.	Weisen Sie einen Anzeigenamen zu und wählen Sie Rolle erstellen aus.	AWS-Systemadministrator
Generieren Sie temporäre Anmeldeinformationen.	Um die Zugriffsschlüssel-ID, den geheimen Zugriffsschlüssel und das Sitzungstoken zu generieren, folgen Sie den Anweisungen in der AWS STS-Dokumentation. Diese Anmeldeinformationen werden bei der Installation des Agenten verwendet.	AWS-Systemadministrator

Installieren des Application Migration Service Agent auf dem SAP-Quellcomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Agent-Installationsprogramm auf den SAP-Quellcomputer herunter.	Laden Sie das Agent-Installationsprogramm herunter, das für Ihr Quellbetriebssystem geeignet ist: Windows oder Linux.	App-Besitzer
Installieren Sie den AWS Replication Agent.	Wenn Sie die Agent-Installationsprogrammdatei auf einem Quellcomputer ausführen, werden Sie zunächst aufgefordert, Ihren Zugriffsschlüssel, den geheimen Zugriffsschlüssel, das Sitzungstoken und die Region einzugeben, in die repliziert werden soll. Verwenden Sie die temporäre	App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n Anmeldeinformationen aus der zuvor erstellten IAM-Rolle und derselben Region, die Sie während der Initialisierung konfiguriert haben.	
Warten Sie auf die erste Datenreplikation.	Nachdem der Agent installie rt wurde, wird der Quellcomp uter auf der Registerkarte Maschinen in der Applicati on Migration Service-Konsole angezeigt.	App-Besitzer

Konfigurieren der Startvorlage des Zielcomputers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Startvorl age für den Quellserver.	Jeder Quellserver verwendet eine eindeutige EC2-Start vorlage, die die Konfiguration des Ziel-EC2-Servers angibt. Sie können diese Vorlage bearbeiten, wenn Sie die Amazon EC2-Konfiguration Ihres migrierten Servers anpassen möchten.	Allgemeines AWS
Legen Sie die Standardversion der Startvorlage fest.	Nachdem Sie die erforderl ichen Änderungen an der Startvorlage vorgenommen haben, geben Sie an, um diese aktualisierte Version als Standardstartvorlage zu verwenden. Weitere Informati	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen finden Sie in der AWS-Dokumentation.	
Deaktivieren Sie die rechte Dimensionierung des Instance-Typs.	(Optional) Die richtige Größe des Instance-Typs bietet automatische Empfehlungen für Instance-Typen, die auf der Konfiguration des Quell-SAP-Servers basieren. Wir empfehlen, diese Einstellu ng zu deaktivieren, damit Sie benutzerdefinierte Instance-Typen in der Startvorlage angeben können.	Allgemeines AWS

Durchführen eines Tests

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie einen Teststart.	Wählen Sie in der Applicati on Migration Service-Konsole einen oder mehrere Server aus und wählen Sie dann Test-Instances starten unter Test und Cutover aus.	Allgemeines AWS, Migration singenieur, Migrationsleiter
Warten Sie, bis der Konvertie rungs- und Startvorgang abgeschlossen ist.	Sie können den Startvorgang auf der Registerkarte Startverl auf überprüfen. Nachdem der Computer erfolgreich als EC2-Instance gestartet wurde, wird die Registerkarte Alerts auf Launched aktualisiert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob der Test erfolgreich abgeschlossen wurde.	Stellen Sie über Remote Desktop Protocol (RDP) oder SSH (Secure Shell) eine Verbindung mit der gestartet en Instance her und führen Sie die entsprechenden Anwendungsprüfungen durch. Melden Sie sich beispiels weise bei der SAP-Schni ttstelle an und validieren Sie die Funktionalität.	Migrationsingenieur, App-Besit zer
Aktualisieren Sie den Quelllebenszyklus.	Wenn der Test erfolgreich war, aktualisieren Sie den Lebenszyklus des Quellcomp uters auf der Registerkarte Test und Cutover auf „Bereit für den Cutover“ als „Bereit“ markieren.	Migrationsingenieur, Migration sleiter

Planen und Durchführen eines Cutovers auf das Amazon EC2-Ziel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie ein Cutover-F enster.		Cutover-Verantwortlicher, Migrationsleiter, App-Eigen tümer
Starten Sie einen Cutover-S tart.	Wählen Sie einen oder mehrere Server aus. Wählen Sie auf der Registerkarte Test und Cutover unter Test und Cutover in der Application Migration Service-Konsole	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Option Cutover-Instances starten aus.	
Warten Sie, bis die Konvertierungs- und Startprozesse abgeschlossen sind.	Sie können den Startvorgang auf der Registerkarte Startverlauf überprüfen. Nachdem der Computer erfolgreich als EC2-Instance gestartet wurde, wird die Registerkarte Alerts auf Launched aktualisiert.	
Überprüfen Sie, ob der Cutover erfolgreich abgeschlossen wurde.	Stellen Sie über RDP oder SSH eine Verbindung mit der gestarteten Instance her und führen Sie die entsprechenden Anwendungsprüfungen durch.	App-Besitzer, Migrationsingenieur
Aktualisieren Sie den Quelllebenszyklus.	Wenn der Cutover erfolgreich war, aktualisieren Sie den Lebenszyklus des Quellcomputers, indem Sie auf der Registerkarte Test und Cutover die Option Cutover abschließen auswählen.	Migrationsingenieur

Zugehörige Ressourcen

Referenzen

- AWS Application Migration Service
- Häufig gestellte Fragen zur AWS-Anwendungsmigration

Video

- AWS Application Migration Service-Architektur

Rehosten Sie lokale Workloads in der AWS-Cloud: Migrationscheckliste

Erstellt von Srikanth Rangavajhala (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Workloads vor Ort	Ziel: AWS Cloud
R-Typ: Rehost	Arbeitslast: Microsoft	Technologien: Migration ; Hybrid Cloud; Betriebssysteme
AWS-Services: AWS-Anwendungsmigrationsservice; Amazon EC2; Amazon Connect		

Übersicht

Das Rehosten von lokalen Workloads in der Amazon Web Services (AWS) -Cloud umfasst die folgenden Migrationsphasen: Planung, Pre-Discovery, Discovery, Build, Test und Cutover. Dieses Muster beschreibt die Phasen und die damit verbundenen Aufgaben. Die Aufgaben werden ausführlich beschrieben und unterstützen etwa 75% aller Anwendungsworkloads. Sie können diese Aufgaben über einen Zeitraum von zwei bis drei Wochen in einem agilen Sprintzyklus implementieren.

Sie sollten diese Aufgaben mit Ihrem Migrationsteam und Ihren Beratern besprechen und überprüfen. Nach der Überprüfung können Sie die Informationen sammeln, Aufgaben streichen oder neu bewerten, falls dies Ihren Anforderungen entspricht, und andere Aufgaben so ändern, dass sie mindestens 75% der Anwendungs-Workloads in Ihrem Portfolio unterstützen. Anschließend kannst du ein agiles Projektmanagement-Tool wie Atlassian Jira oder Rally Software verwenden, um die Aufgaben zu importieren, sie Ressourcen zuzuweisen und deine Migrationsaktivitäten zu verfolgen.

Das Muster geht davon aus, dass Sie AWS Cloud Migration Factory verwenden, um Ihre Workloads neu zu hosten, aber Sie können das Migrationstool Ihrer Wahl verwenden.

Macie kann Ihnen helfen, sensible Daten in Ihren Wissensdatenbanken zu identifizieren, die als Datenquellen gespeichert sind, Aufrufprotokolle zu modellieren und sie in S3-Buckets zu speichern.

Bewährte Sicherheitsmethoden für Macie finden Sie im vorherigen Abschnitt Macie in dieser Anleitung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Projektmanagement-Tool zur Nachverfolgung von Migrationsaufgaben (z. B. Atlassian Jira oder Rally Software)
- Migrationstool zum Rehosten Ihrer Workloads auf AWS (z. B. Cloud Migration Factory)

Architektur

Quellplattform

- Lokaler Quellstapel (einschließlich Technologien, Anwendungen, Datenbanken und Infrastruktur)

Zielplattform

- AWS-Cloud-Zielstapel (einschließlich Technologien, Anwendungen, Datenbanken und Infrastruktur)

Architektur

Das folgende Diagramm veranschaulicht das Rehosting (Erkennung und Migration von Servern aus einer lokalen Quellumgebung zu AWS) mithilfe von Cloud Migration Factory und AWS Application Migration Service.

Tools

- Sie können ein Migrations- und Projektmanagement-Tool Ihrer Wahl verwenden.

Epen

Planungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pflegen Sie den Rückstand vor der Entdeckung.	Führen Sie die Arbeitssitzung mit Abteilungsleitern und Anwendungsbesitzern durch, bevor der Rückstand erkannt wird.	Projektmanager, Leiter von Agile Scrum
Führen Sie die Arbeitssitzung zur Sprint-Planung durch.	Verteilen Sie die Anwendung en, die Sie migrieren möchten, als Übung für den Umfang auf mehrere Sprints und Wellen.	Projektmanager, Leiter von Agile Scrum

Phase vor der Entdeckung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Anwendung skenntnisse.	Bestätigen und dokumenti eren Sie den Inhaber der Anwendung und dessen Kenntnisse über die Anwendung. Stellen Sie fest, ob es einen anderen Ansprechpartner für technisch e Fragen gibt.	Migrationsspezialist (Intervie wer)
Ermitteln Sie die Compliance-Anforderungen für Anwendung en.	Erkundigen Sie sich beim Eigentümer der Anwendung, dass die Anwendung nicht den Anforderungen des Payment Card Industry Data Security Standard (PCI DSS), des Sarbanes-Oxley Act (SOX),	Migrationsspezialist (Intervie wer)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	personenbezogener Daten (PII) oder anderer Standards entsprechen muss. Wenn Compliance-Anforderungen bestehen, müssen die Teams ihre Konformitätsprüfungen auf den Servern abschließen, die migriert werden sollen.	
Bestätigen Sie die Anforderungen für die Produktionsfreigabe.	Bestätigen Sie die Anforderungen für die Freigabe der migrierten Anwendung für die Produktion (z. B. Veröffentlichungsdatum und Dauer der Ausfallzeit) mit dem Eigentümer der Anwendung oder dem technischen Ansprechpartner.	Migrationsspezialist (Interviewer)
Serverliste abrufen.	Ruft die Liste der Server ab, die der Zielanwendung zugeordnet sind.	Migrationsspezialist (Interviewer)
Holen Sie sich das logische Diagramm, das den aktuellen Status zeigt.	Rufen Sie das aktuelle Statusdiagramm für die Anwendung vom Unternehmensarchitekten oder dem Anwendungsbesitzer ab.	Migrationsspezialist (Interviewer)
Erstellen Sie ein logisches Diagramm, das den Zielstatus zeigt.	Erstellen Sie ein logisches Diagramm der Anwendung, das die Zielarchitektur auf AWS zeigt. Dieses Diagramm sollte Server, Konnektivität und Zuordnungsfaktoren veranschaulichen.	Unternehmensarchitekt, Geschäftsinhaber

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Serverinformationen abrufen.	Sammeln Sie Informationen über die Server, die der Anwendung zugeordnet sind, einschließlich ihrer Konfigurationsdetails.	Migrationsspezialist (Interviewer)
Fügen Sie Serverinformationen zur Discovery-Vorlage hinzu.	Fügen Sie der Vorlage für die Anwendungserkennung detaillierte Serverinformationen hinzu (dieses Muster finden Sie `mobilize-application-questionnaire.xlsx` im Anhang). Diese Vorlage enthält alle anwendungsbezogenen Sicherheits-, Infrastruktur-, Betriebssystem- und Netzwerkdetails.	Migrationsspezialist (Interviewer)
Veröffentlichen Sie die Vorlage für die Anwendungserkennung.	Teilen Sie die Vorlage für die Anwendungserkennung mit dem Anwendungseigentümer und dem Migrationsteam, damit sie gemeinsam darauf zugreifen und sie verwenden können.	Migrationsspezialist (Interviewer)

Entdeckungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Serverliste.	Bestätigen Sie die Serverliste und den Zweck der einzelnen Server mit dem Besitzer	Spezialist für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Anwendung oder dem technischen Leiter.	
Identifizieren und fügen Sie Servergruppen hinzu.	Identifizieren Sie Servergruppen wie Webserver oder Anwendungsserver und fügen Sie diese Informationen der Vorlage für die Anwendungserkennung hinzu. Wählen Sie die Ebene der Anwendung (Web, Anwendung, Datenbank) aus, zu der jeder Server gehören soll.	Spezialist für Migration
Füllen Sie die Vorlage für die Anwendungserkennung aus.	Vervollständigen Sie die Details der Vorlage für die Anwendungserkennung mit Hilfe des Migrationsteams, des Anwendungsteams und AWS.	Spezialist für Migration
Fügen Sie fehlende Serverdetails hinzu (Middleware- und Betriebssystemteams).	Bitten Sie Middleware- und Betriebssystemteams (OS), die Vorlage für die Anwendungserkennung zu überprüfen und alle fehlenden Serverdetails, einschließlich Datenbankinformationen, hinzuzufügen.	Spezialist für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich die Regeln für eingehenden/ausgehenden Verkehr (Netzwerkteam).	Bitten Sie das Netzwerkteam, die Regeln für eingehenden/ausgehenden Verkehr für die Quell- und Zielserver zu ermitteln. Das Netzwerkteam sollte außerdem bestehende Firewallregeln hinzufügen, diese in ein Sicherheitsgruppenformat exportieren und bestehende Load Balancer zur Vorlage für die Anwendungserkennung hinzufügen.	Spezialist für Migration
Identifizieren Sie das erforderliche Tagging.	Ermitteln Sie die Tagging-Anforderungen für die Anwendung.	Spezialist für Migration
Erstellen Sie Details zur Firewall-Anforderung.	Erfassen und filtern Sie die Firewallregeln, die für die Kommunikation mit der Anwendung erforderlich sind.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter
Aktualisieren Sie den EC2-Instanztyp.	Aktualisieren Sie den Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Typ, der in der Zielumgebung verwendet werden soll, basierend auf Infrastruktur- und Serveranforderungen.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie das Diagramm mit dem aktuellen Status.	Identifizieren oder erstellen Sie das Diagramm, das den aktuellen Status der Anwendung zeigt. Dieses Diagramm wird in der Anfrage zur Informationssicherheit (InfoSec) verwendet.	Migrationsspezialist, Lösungsarchitekt
Finalisieren Sie das future Zustandsdiagramm.	Finalisieren Sie das Diagramm, das den future (Ziel-) Status der Anwendung zeigt. Dieses Diagramm wird auch in der InfoSec Anfrage verwendet.	Migrationsspezialist, Lösungsarchitekt
Erstellen Sie Serviceanfragen für Firewalls oder Sicherheitsgruppen.	Erstellen Sie Firewall- oder Sicherheitsgruppen-Serviceanfragen (für Entwicklung/Qualitätssicherung, Vorproduktion und Produktion). Wenn Sie Cloud Migration Factory verwenden, fügen Sie replikationsspezifische Ports hinzu, sofern diese noch nicht geöffnet sind.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter
Überprüfen Sie die Anfragen von Firewalls oder Sicherheitsgruppen (InfoSec Team).	In diesem Schritt überprüft und genehmigt das InfoSec Team die Firewall- oder Sicherheitsgruppenanfragen, die im vorherigen Schritt erstellt wurden.	InfoSec Ingenieur, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie Firewall-Sicherheitsgruppenanfragen (Netzwerkteam).	Nachdem das InfoSec Team die Firewallanfragen genehmigt hat, implement iert das Netzwerkteam die erforderlichen Firewallregeln für eingehende/ausgehende Verbindungen.	Migrationsspezialist, Lösungsarchitekt, Netzwerkl eiter

Erstellungsphase (Wiederholung für Entwicklungs- und QA-, Vorproduktions- und Produktionsumgebungen)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie die Anwendungs- und Serverdat en.	1. Stellen Sie sicher, dass Sie bei Ihrem Server für die Ausführung der Migration als Domänenbenutzer mit lokalen Administratorrecht en auf den Quellservern im Geltungsbereich angemelde t sind. 2. Verwenden Sie das Eingabeformular für die Migration, um die Attribute für die Quellserv er im Geltungsbereich zu importieren. Weitere Informationen finden Sie im Cloud Migration Factory-I mplementierungsleitfaden. Wenn Sie Cloud Migration Factory nicht verwenden,	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgen Sie den Anweisungen zur Einrichtung Ihres Migration stools.	
Überprüfen Sie die Vorausset zungen für Quellserver.	Connect mit den Quellserv ern im Geltungsbereich her, um Voraussetzungen wie TCP-Port 1500, TCP-Port 443, freien Speicherp latz auf dem Stammvolu me, .NET Framework-Version und andere Parameter zu überprüfen. Diese sind für die Replikation erforderl ich. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungslei tfaden.	Migrationsspezialist, Cloud-Administrator
Erstellen Sie eine Servicean frage zur Installation von Replikationsagenten.	Erstellen Sie eine Servicean frage zur Installation von Replikationsagenten auf den im Lieferumfang enthaltenen Servern für Entwicklung/Qualit ätssicherung, Vorproduktion oder Produktion.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Replikationsagenten.	Installieren Sie die Replikationsagenten auf den Quellservern im Leistungsumfang auf den Entwicklungs-, QA-, Vorproduktions- oder Produktionsrechnern. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Push die Skripte nach dem Start.	Der Application Migration Service unterstützt Skripts nach dem Start, um Sie bei der Automatisierung von Aktivitäten auf Betriebssystemebene zu unterstützen, z. B. die Installation oder Deinstallation von Software nach dem Start von Ziel-Instances. In diesem Schritt werden die Skripts nach dem Start auf Windows- oder Linux-Computer übertragen, je nachdem, welche Server für die Migration identifiziert wurden. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Replikationsstatus.	Bestätigen Sie den Replikationsstatus für die Quellserver im Geltungsbereich automatisch mithilfe des bereitgestellten Skripts. Das Skript wird alle fünf Minuten wiederholt, bis sich der Status aller Quellserver in der angegebenen Welle auf Fehlerfrei ändert. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Erstellen Sie den Admin-Benutzer.	Möglicherweise ist ein lokaler Administrator oder Sudo-Benutzer auf den Quellcomputern erforderlich, um Probleme nach der Umstellung von den Quellservern im Geltungsbereich auf AWS zu beheben. Das Migrationsteam verwendet diesen Benutzer, um sich beim Zielserver anzumelden, wenn der Authentifizierungsserver (z. B. der DC- oder LDAP-Server) nicht erreichbar ist. Anweisungen für diesen Schritt finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Startvorlage.	Überprüfen Sie die Server-Metadaten, um sicherzustellen, dass sie erfolgreich funktionieren und keine ungültigen Daten enthalten. In diesem Schritt werden sowohl die Test- als auch die Cutover-Metadaten validiert. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Testphase (Wiederholung für Entwicklungs- und QA-, Vorproduktions- und Produktionsumgebungen)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Servicean frage.	Erstellen Sie eine Servicean frage für das Infrastrukturteam und andere Teams, um die Anwendung auf Entwicklungs-/QA-, Vorproduktions- oder Produktionsinstanzen umzustellen.	Migrationsspezialist, Cloud-Administrator
Konfigurieren Sie einen Load Balancer (optional).	Konfigurieren Sie die erforderlichen Load Balancer, z. B. einen Application Load Balancer oder einen F5-Load Balancer, mit iRules.	Migrationsspezialist, Cloud-Administrator
Starten Sie Instanzen zum Testen.	Startet alle Zielcomputer für eine bestimmte Welle im Application Migration Service im Testmodus. Weitere Informationen finden Sie im	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cloud Migration Factory-Implementierungsleitfaden.	
Überprüfen Sie den Status der Zielinstanz.	Überprüfen Sie den Status der Zielinstanz, indem Sie den Startvorgang für alle Quellserver im Geltungsbereich in derselben Welle überprüfen. Es kann bis zu 30 Minuten dauern, bis die Ziel-Instances hochgefahren sind. Sie können den Status manuell überprüfen, indem Sie sich bei der Amazon EC2-Konsole anmelden, nach dem Namen des Quellservers suchen und die Spalte Statusprüfung überprüfen. Die bestandenen Statusprüfungen 2/2 deuten darauf hin, dass die Instance aus Sicht der Infrastruktur fehlerfrei ist.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
DNS-Einträge ändern.	Ändern Sie DNS-Einträge (Domain Name System). (Verwenden Sie `resolv.conf` oder `host.conf` für eine Microsoft Windows-Umgebung.) Konfigurieren Sie jede EC2-Instanz so, dass sie auf die neue IP-Adresse dieses Hosts verweist. Hinweis: Stellen Sie sicher, dass es keine DNS-Konflikte zwischen lokalen Servern und AWS-Cloud-Servern gibt. Dieser Schritt und die folgenden Schritte sind optional, abhängig von der Umgebung, in der der Server gehostet wird.	Migrationsspezialist, Cloud-Administrator
Testen Sie die Konnektivität zu Backend-Hosts von EC2-Instanzen aus.	Überprüfen Sie die Anmeldungen anhand der Domänenanmeldedaten für die migrierten Server.	Migrationsspezialist, Cloud-Administrator
Aktualisieren Sie den DNS-A-Eintrag.	Aktualisieren Sie den DNS-A-Eintrag für jeden Host so, dass er auf die neue private Amazon EC2 EC2-IP-Adresse verweist.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den DNS-CNAME-Eintrag.	Aktualisieren Sie den DNS-CNAME-Eintrag für virtuelle IPs (Load Balancer-Namen) so, dass er auf den Cluster für Web- und Anwendungsserver verweist.	Migrationsspezialist, Cloud-Administrator
Testen Sie die Anwendung in den entsprechenden Umgebungen.	Melden Sie sich bei der neuen EC2-Instance an und testen Sie die Anwendung in den Entwicklungs-, QA-, Vorproduktions- und Produktionsumgebungen.	Migrationsspezialist, Cloud-Administrator
Als bereit für die Umstellung markieren.	Wenn der Test abgeschlossen ist, ändern Sie den Status des Quellservers, um anzuzeigen, dass er bereit für die Übernahme ist, sodass Benutzer eine Übernahmeinstanz starten können. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Umstellungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Bereitstellungsplan für die Produktion.	Erstellen Sie einen Bereitstellungsplan für die Produktion (einschließlich eines Notfallplans).	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Informieren Sie das Betriebsteam über Ausfallzeiten.	Informieren Sie das Betriebsteam über den Zeitplan für die Ausfallzeiten der Server. Einige Teams benötigen für diese Benachrichtigung möglicherweise eine Änderungsanfrage oder ein Ticket für eine Serviceanfrage (CR/SR).	Migrationsspezialist, Cloud-Administrator
Replizieren Sie Produktionsmaschinen.	Replizieren Sie Produktionsmaschinen mithilfe des Application Migration Service oder eines anderen Migrationstools.	Migrationsspezialist, Cloud-Administrator
Fahren Sie die Quellserver im Geltungsbereich herunter.	Nachdem Sie den Replikationsstatus der Quellserver überprüft haben, können Sie die Quellserver herunterfahren, um Transaktionen von Client-Anwendungen zu den Servern zu stoppen. Sie können die Quellserver im Übernahmefenster herunterfahren. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Instanzen für die Umstellung.	Startet alle Zielcomputer für eine bestimmte Welle im Application Migration Service im Übernahmemodus. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Rufen Sie die IPs der Zielinstanz ab.	Rufen Sie die IPs für Zielinstanzen ab. Wenn das DNS-Update in Ihrer Umgebung ein manueller Prozess ist, müssten Sie die neuen IP-Adressen für alle Zielinstanzen abrufen. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Überprüfen Sie die Verbindungen zum Zielserver.	Nachdem Sie die DNS-Einträge aktualisiert haben, stellen Sie mit dem Hostnamen eine Verbindung zu den Zielinstanzen her, um die Verbindungen zu überprüfen. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Zugehörige Ressourcen

- Wie migriert man
- Implementierungsleitfaden für AWS Cloud Migration Factory
- Automatisierung umfangreicher Servermigrationen mit Cloud Migration Factory

- AWS Application Migration Service — Benutzerhandbuch
- AWS Migration Acceleration Program

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Einrichten einer Multi-AZ-Infrastruktur für eine SQL Server Always On FCI mithilfe von Amazon FSx

Erstellt von Manish Garg (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Nishad Mankar (AWS) und RAJNEESH TYAGI (AWS)

Code-Repository: aws-windows-failover-cluster– Automatisierung	Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises SQL Server-Datenbank
Ziel: Microsoft SQL Server auf EC2	R-Typ: Hostwechsel	Workload: Microsoft
Technologien: Migration; Infrastruktur; DevOps	AWS-Services: AWS Managed Microsoft AD; Amazon EC2; Amazon FSx ;AWS Systems Manager	

Übersicht

Wenn Sie schnell eine große Anzahl von Microsoft SQL Server Always On Failover Cluster Instances (FCIs) migrieren müssen, kann dieses Muster Ihnen helfen, die Bereitstellungszeit zu minimieren. Durch die Verwendung von Automatisierung und Amazon FSx für Windows File Server reduziert es manuelle Bemühungen, menschliche Fehler und die Zeit, die für die Bereitstellung einer großen Anzahl von Clustern benötigt wird.

Dieses Muster richtet die Infrastruktur für SQL Server FCIs in einer Multi-Availability Zone (Multi-AZ)-Bereitstellung auf Amazon Web Services (AWS) ein. Die Bereitstellung der für diese Infrastruktur erforderlichen AWS-Services wird mithilfe von AWS CloudFormation-Vorlagen automatisiert. Die SQL Server-Installation und Cluster-Knoten-Erstellung auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance wird mithilfe von - PowerShell Befehlen durchgeführt.

Diese Lösung verwendet ein hochverfügbares Multi-AZ-Amazon-FSx-für-Windows-Dateisystem als gemeinsamen Zeugen zum Speichern der SQL-Server-Datenbankdateien. Das Amazon FSx-Dateisystem und EC2-Windows-Instances, die SQL Server hosten, sind mit derselben AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)-Domain verbunden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein AWS-Benutzer mit ausreichenden Berechtigungen zum Bereitstellen von Ressourcen mithilfe von AWS- CloudFormation Vorlagen
- AWS Directory Service für Microsoft Active Directory
- Anmeldeinformationen in AWS Secrets Manager zur Authentifizierung bei AWS Managed Microsoft AD in einem Schlüssel-Wert-Paar:
  - `ADDomainName`: <Domänenname>
  - `ADDomainJoinUserName`: <Domain-Benutzername>
  - `ADDomainJoinPassword`:<Domain-Benutzerpasswort>
  - `TargetOU`: <Ziel-OU-Wert>

  Hinweis: Sie verwenden denselben Schlüsselnamen in der AWS Systems Manager-Automatisierung für die AWS Managed Microsoft AD-Join-Aktivität.
- SQL Server-Mediendateien für die SQL Server-Installation und erstellte Windows-Service- oder Domainkonten, die während der Clustererstellung verwendet werden
- Eine Virtual Private Cloud (VPC) mit zwei öffentlichen Subnetzen in separaten Availability Zones, zwei privaten Subnetzen in den Availability Zones, einem Internet-Gateway, NAT-Gateways, Routing-Tabellenzuordnungen und einem Sprungserver

Produktversionen

- Windows Server 2012 R2 und Microsoft SQL Server 2016

Architektur

Quelltechnologie-Stack

- On-Premises SQL Server mit FCIs, die ein freigegebenes Laufwerk verwenden

Zieltechnologie-Stack

- AWS EC2-Instances

- Amazon FSx für Windows File Server
- AWS Systems Manager Automation-Runbook
- Netzwerkkonfigurationen (VPC, Subnetze, Internet-Gateway, NAT-Gateways, Jumpserver, Sicherheitsgruppen)
- AWS Secrets Manager
- AWS Managed Microsoft AD
- Amazon EventBridge
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt ein AWS-Konto in einer einzelnen AWS-Region mit einer VPC, die zwei Availability Zones, zwei öffentliche Subnetze mit NAT-Gateways, einen Sprungserver im ersten öffentlichen Subnetz, zwei private Subnetze mit jeweils einer EC2-Instance für einen SQL Server-Knoten in einer Knotensicherheitsgruppe und ein Amazon FSx-Dateisystem umfasst, das eine Verbindung zu jedem der SQL Server-Knoten herstellt. AWS Directory Service , Amazon EventBridge, AWS Secrets Manager und AWS Systems Manager sind ebenfalls enthalten.

Automatisierung und Skalierung

- Sie können AWS Systems Manager verwenden, um AWS Managed Microsoft AD beizutreten und die SQL Server-Installation durchzuführen.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Directory Service bietet mehrere Möglichkeiten, Microsoft Active Directory (AD) mit anderen AWS-Services wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) für SQL Server und Amazon FSx für Windows File Server zu verwenden.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mit API-Zielen oder Event Buses in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang.

Andere Tools

- PowerShell ist ein Microsoft-Automatisierungs- und Konfigurationsmanagementprogramm, das unter Windows, Linux und macOS ausgeführt wird. Dieses Muster verwendet PowerShell Skripts.

Code-Repository

Der Code für dieses Muster ist im GitHub aws-windows-failover-cluster-Automation-Repository verfügbar.

Bewährte Methoden

- Die IAM-Rollen, die für die Bereitstellung dieser Lösung verwendet werden, sollten dem Prinzip der geringsten Berechtigung entsprechen. Weitere Informationen finden Sie in der IAM-Dokumentation.
- Folgen Sie den CloudFormation bewährten Methoden von AWS .

Sekunden

Bereitstellen der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Systems Manager- CloudFormation Stack bereit.	1. Melden Sie sich bei Ihrem AWS-Konto an und öffnen Sie die AWS-Manag ementkonsole. 2. Navigieren Sie zur - CloudFormation Konsole und erstellen Sie den Systems Manager-CloudFormation Stack, indem Sie die `ssm.yaml` Vorlage hochladen. Geben Sie Werte für die folgenden Parameter an: • StateUnJoinAssocia tionLoggingBucketN ame – Geben Sie einen Namen für den S3-Bucket an, den die Vorlage zu Protokollierungszwecken erstellt. • SSMAssociationADUn joinName – Geben Sie einen Namen für die `AWS::SSM::Associat ion` Ressource an. • SSMAutomationDocum entName – Geben Sie einen Namen für das Systems Manager Automation-Runbook an.	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• EventBridgeName – Geben Sie einen Namen für den EventBridge Event Bus an. 3. Stellen Sie den Systems Manager- CloudFormationStack bereit, indem Sie die `ssm.yaml` CloudFormation Vorlage starten. Die Vorlage erstellt den Systems Manager Atomation Runboook, der initiiert wird, wenn eine neue EC2-Instance mit dem Tag `ADJoined: FSXADD` gestartet wird. Das Automation-Runbook fügt die Instance zum AWS Managed Microsoft AD-Verzeichnis hinzu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Infrastruktur-Stack bereit.	Erstellen Sie nach erfolgreicher Bereitstellung des Systems Manager-Stacks den `infra`Stack, der EC2-Instance-Knoten, Sicherheitsgruppen, das Dateisystem von Amazon FSx für Windows File Server und die IAM-Rolle umfasst. 1. Navigieren Sie zur -CloudFormation Konsole und starten Sie die `infra-cf.yaml` Vorlage. Um diesen Stack bereitzustellen, sind die folgenden Parameter erforderlich: • `ActiveDirectoryId` – ID für AWS Managed Microsoft AD • `ADDnsIpAddresses1` – Primäre DNS-IP-Adresse von AWS Managed Microsoft AD • `ADDnsIpAddresses2` – Sekundäre DNS-IP-Adresse von AWS Managed Microsoft AD • `FSxSecurityGroupName` – Name der Amazon-FSx-Sicherheitsgruppe	AWS DevOps, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `FSxWindowsFileSystemName` – Name des Amazon-FSx-Laufwerks • `ImageID` – ID des Windows 2012 R2-Basis-Images oder Amazon Machine Image (AMI), das zum Erstellen des SQL Server-Instance-Knotens verwendet wird • `KeyPairName` – Schlüssel-Wert-Paar, das an die EC2-Instance-Knoten für den Zugriff angefügt werden soll • `Node1SecurityGroupName` – Name der ersten Knoten-Sicherheitsgruppe • `Node2SecurityGroupName` – Name der Sicherheitsgruppe des zweiten Knotens • `OUSecretName` – Name des Secrets, das die AWS Managed Microsoft AD-Informationen enthält • `PrivateSubnet1` – ID des ersten privaten Subnetzes	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `PrivateSubnet2` – ID des zweiten privaten Subnetzes • `SqlFSxFCIName` – Name des Tags, das auf den primären und sekundären Knoten und auf Amazon FSx angewendet wird. • `SqlFSxServerNetBIOSName1` – Name des primären EC2-Instance-Knotens (maximal 15 Zeichen) • `SqlFSxServerNetBIOSName2` – Name des sekundären EC2-Instance-Knotens (maximal 15 Zeichen) • `VPC` – VPC-ID • `WorkloadInstanceType` – Typ der EC2-Instance Stellen Sie den `infra`Stack bereit. Der Stack erstellt alle Infrastrukturkomponenten, die zum Einrichten von Windows SQL Server FCI erforderlich sind. 2. Nachdem die EC2-Instance-Knoten gestartet wurden, wird das Systems Manager Automation-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokument aufgerufen, um diese Instances mit AWS Managed Microsoft AD zu verbinden. Sie können den Fortschritt auf der Seite Automatisierung der Systems Manager-Konsole verfolgen.	

Einrichten von Windows SQL Server Always On FCI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Windows-Tools.	1. Melden Sie sich bei der primären EC2-Instance an, bei der es sich um Knoten 1 handelt. Führen Sie das folgende PowerShell Skript aus, um die Windows-Funktionen (Active Directory und FCI-Tools) zu installieren.
	`Install-WindowsFeature -Name RSAT-AD-Powershell,Failover-Clustering -IncludeManagementTools`
	`Install-WindowsFeature -Name RSAT-Clustering,RSAT-ADDS-Tools,RSAT-AD-Powershell,RSAT-DHCP,RSAT-DNS-Server`
		AWS DevOps, DevOps Techniker, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Melden Sie sich bei der sekundären EC2-Instance an, bei der es sich um Knoten 2 handelt, und führen Sie dasselbe Skript aus, um Funktionen auf Knoten 2 zu aktivieren.	
Stellen Sie die Cluster-Computerobjekte in Active Directory Domain Services bereit.	Um das Cluster Name Object (CNO) in Active Directory Domain Services (AD DS) und ein virtuelles Computerobjekt (VCO) für eine gruppierte Rolle vorab bereitzustellen, folgen Sie den Anweisungen in der Windows Server-Dokumentation.	AWS DevOps, DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den WSFC.	Gehen Sie wie folgt vor, um den Windows Server Failover Clustering (WSFC)-Cluster zu erstellen: 1. Melden Sie sich bei der primären EC2-Instance an, bei der es sich um Knoten 1 handelt. Führen Sie den folgenden Code aus, um die Amazon-FSx-Dateifreigabe zu erstellen und vollen Zugriff auf das aufgeführte AD-Servicekonto zu gewähren. `Invoke-Command -ComputerName "<FSx Windows Remote PowerShell Endpoint>" -ConfigurationName FSxRemoteAdmin -scriptblock { New-FSxSmbShare -Name "SQLDB" -Path "D:\share" -Description "SQL Databases Share" -ContinuouslyAvailable $true -FolderEnumerationMode AccessBased -EncryptData $true grant-fsxsmbshareaccess -name SQLDB -AccountName "<domain\user>" -accessRight Full }`	AWS DevOps, DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mit diesem Befehl wird auch die kontinuierlich verfügbare (CA)-Dateifreigabe erstellt, die für die Verwendung durch Microsoft SQL Server optimiert ist. 2. Führen Sie den folgenden Befehl aus, um den Failover-Cluster auf der primären Instance (Knoten 1) zu erstellen. `New-Cluster -Name <CNO Name> -Node <Node1 Name>, <Node2 Name> -StaticAddress <Node1 Secondary Private IP>, <Node2 Secondary Private IP>` Der Befehl erfordert die folgenden Parameter: • `Name` – Der Name des Clusters (CNO) • `Node` – Die Namen der primären bzw. sekundären Knoten • `StaticAddress` – Die sekundären IP-Adressen der primären bzw. sekundären Knoten Wichtig: Ein Domainadministrator oder regulärer Benutzer muss über	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Administratorberechtigung für beide Knoten verfügen, um den Windows Server Failover Clustering (WSFC)-Cluster zu erstellen. Andernfalls schlägt der vorherige Befehl fehl und gibt die Meldung zurückYou do not have administrator privilege on servers. 3. Nachdem der Cluster erstellt wurde, führen Sie den folgenden Befehl aus, um den Dateifreigabezeugen anzuhängen. `Set-ClusterQuorum -FileShareWitness \ \<FSx Windows Remote PowerShell Endpoint> \share\witness`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den SQL Server-Failover-Cluster.	Nachdem der WSFC-Cluster eingerichtet wurde, installieren Sie den SQL Server-Cluster auf der primären Instance (node1). 1. Erstellen Sie im T-Laufwerk auf beiden Knoten die `log` Ordner `tempdb` und . Die Ordner werden in den PowerShell Befehlen verwendet. 2. Nachdem Sie die SQL Server-Mediendateien für die SQL Server-Installation auf beiden Knoten kopiert haben, führen Sie den folgenden PowerShell Befehl auf Knoten 1 aus, um SQL Server auf Knoten 1 zu installieren. `D:\setup.exe /Q ` `/ACTION=InstallFailoverCluster ` `/IACCEPTSQLSERVERLICENSETERMS ` `/FEATURES="SQL,IS,BC,Conn" ` `/INSTALLSHAREDDIR="C:\Program Files\Microsoft SQL Server” ` `/INSTALLSHAREDWOWDIR="C:\Program Files (x86)\Microsoft SQL Server" `	AWS DevOps, DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`/RSINSTALLMODE="FilesOnlyMode" ` `/INSTANCEID="MSSQLSERVER" ` `/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node1>;Cluster Network 1;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/INSTANCEDIR="C:\Program Files\Microsoft SQL Server" ` `/ENU="True" ` `/ERRORREPORTING=0 ` `/SQMREPORTING=0 ` `/SAPWD="<Domain User password>" ` `/SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS" ` `/SQLSYSADMINACCOUNTS="<domain\username>" ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="<domain\username>" /AGTSVCPASSWORD="<Domain User password>" `	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	/ISSVCACCOUNT="<domain\username>" /ISSVCPASSWORD="<Domain User password>" ` /FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` /INSTALLSQLDATADIR="\\<FSX DNS name>\share\Program Files\Microsoft SQL Server" ` /SQLUSERDBDIR="\\<FSX DNS name>\share\data" ` /SQLUSERDBLOGDIR="\\<FSX DNS name>\share\log" ` /SQLTEMPDBDIR="T:\tempdb" ` /SQLTEMPDBLOGDIR="T:\log" ` /SQLBACKUPDIR="\\<FSX DNS name>\share\SQLBackup" ` /SkipRules=Cluster_VerifyForErrors ` /INDICATEPROGRESS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie dem Cluster einen sekundären Knoten hinzu.	Führen Sie den folgenden PowerShell Befehl aus, um dem sekundären Knoten (Knoten 2) SQL Server hinzuzufügen. `D:\setup.exe /Q ` `/ACTION=AddNode ` `/IACCEPTSQLSERVERLICENSETERMS ` `/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node2>;Cluster Network 2;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/CONFIRMIPDEPENDENCYCHANGE=1 ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/SkipRules=Cluster_VerifyForErrors `	AWS DevOps, DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`/INDICATEPROGRESS`	
Testen Sie die SQL Server-FCI.	1. Starten Sie auf der Windows-Instance für einen der Knoten in Administrative Tools den Failover Cluster Manager . 2. Navigieren Sie zu Knoten und bestätigen Sie, dass der Knotenstatus Status Wird ausgeführt lautet. 3. Wählen Sie Rollen aus, öffnen Sie das Kontextmenü (rechte Maustaste) für SQL Server (MSSQLSERVER) und wählen Sie Verschieben und Knoten auswählen aus. 4. Nach der Knotenauswahl sollte SQL Server auf dem anderen Knoten ausgeführt werden.	DBA, DevOps Techniker

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie Ressourcen.	Um die Ressourcen zu bereinigen, verwenden Sie den AWS- CloudFormation Stack-Löschvorgang: 1. Öffnen Sie die AWS-CloudFormation Konsole .	AWS DevOps, DBA, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Seite Stacks den `infra`Stack aus. Der Stack muss aktuell ausgeführt werden. 3. Wählen Sie im Stack-Detailbereich Delete (Löschen) aus. 4. Wählen Sie Delete stack (Stack löschen) aus, wenn Sie dazu aufgefordert werden. 5. Wiederholen Sie die Schritte 2-4 für den `ssm`Stack. Nachdem das Löschen des Stacks abgeschlossen ist, befinden sich die Stacks im `DELETE_COMPLETE` Status . Stacks mit dem `DELETE_COMPLETE` Status werden standardmäßig nicht in der - CloudFormation Konsole angezeigt. Um gelöschte Stacks anzuzeigen, müssen Sie den Filter für die Stack-Ansicht ändern, wie unter Anzeigen gelöschter Stacks in der AWS- CloudFormation Konsole beschrieben. Wenn der Löschvorgang fehlgeschlagen ist, befindet sich ein Stack im `DELETE_FA`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ILED` Status . Lösungen finden Sie unter Delete stack fail in der - CloudFormation Dokumentation.	

Fehlerbehebung

Problem	Lösung
AWS- CloudFormation Vorlagenfehler	Wenn die CloudFormation Vorlage während der Bereitstellung fehlschlägt, gehen Sie wie folgt vor: 1. Öffnen Sie die AWS- CloudFormation Konsole . 2. Wählen Sie auf der Seite Stacks in der - CloudFormation Konsole den Stack aus. 3. Wählen Sie Ereignisse und überprüfen Sie den Stack-Status .
AWS Managed Microsoft AD-Join-Fehler	Gehen Sie wie folgt vor, um die Verbindun gsprobleme zu beheben: 1. Öffnen Sie die Systems Manager-Konsole. 2. Wählen Sie die Bereitstellungsregion aus. 3. Wählen Sie im linken Bereich Automation aus und suchen Sie das fehlgeschlagene Automation-Runbook. 4. Öffnen Sie das Automation-Runbook und suchen Sie nach dem Ausführungsstatus und den Ausführungsschritten .

Problem	Lösung
	5. Untersuchen Sie die Details des fehlgeschlagenen Schritts, um den genauen Fehler oder Fehler zu sehen.

Zugehörige Ressourcen

- Vereinfachen Sie Ihre Microsoft SQL Server-Hochverfügbarkeitsbereitstellungen mit Amazon FSx für Windows File Server
- Verwenden von FSx for Windows File Server mit Microsoft SQL Server

Verwenden Sie Bol Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren

Erstellt von Ben Bol-Hamblin (AWS), Bol Cunningham (AWS), Emma Baldry (AWS) und Shabnam Khan (AWS)

Umgebung: Produktion	Quelle: Discovery	Ziel: Migrationsplan
R-Typ: Hostwechsel	Workload: Alle anderen Workloads	Technologien: Migration; Management und Governance; Netzwerk; Hybrid Cloud
AWS-Services: AWS Migration Hub		

Übersicht

Dieses Handbuch enthält Abfragebeispiele und Schritte, mit denen Sie mithilfe von Discovery Daten aus Ihrer On-Premises-Infrastruktur und Anwendungen extrahieren können. Das Muster zeigt Ihnen, wie Sie mithilfe von Discovery-Abfragen Ihre Infrastruktur scannen und Software-, Service- und Abhängigkeitsinformationen extrahieren. Die extrahierten Daten sind für die Bewertungs- und Mobilisierungsphase einer groß angelegten Migration zur Amazon Web Services (AWS) Cloud erforderlich. Sie können diese Daten verwenden, um wichtige Entscheidungen darüber zu treffen, welche Anwendungen im Rahmen Ihres Migrationsplans zusammen migriert werden sollen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Lizenz für Discovery (früher Bol ADDM) oder die Software as a Service (SaaS)-Version von Helix Discovery
- On-Premises- oder SaaS-Version von Discovery, installiert (Hinweis: Bei On-Premises-Versionen von Discovery müssen Sie die Anwendung in einem Client-Netzwerk mit Zugriff auf alle Netzwerk- und Servergeräte installieren, die für eine Migration über mehrere Rechenzentren hinweg vorgesehen sind. Der Zugriff auf das Client-Netzwerk muss gemäß den Installationsanweisungen der Anwendung bereitgestellt werden. Wenn das Scannen von Windows Server-Informationen erforderlich ist, müssen Sie ein Windows-Proxy-Manager-Gerät im Netzwerk einrichten.)

- Netzwerkzugriff, damit die Anwendung Geräte über Rechenzentren hinweg scannen kann, wenn Sie Helix Discovery verwenden

Produktversionen

- Discovery 22.2 (12.5)
- Discovery 22.1 (12.4)
- Discovery 21.3 (12.3)
- Discovery 21.05 (12.2)
- Discovery 20.08 (12.1)
- Discovery 20.02 (12.0)
- Discovery 11.3
- Discovery 11.2
- Discovery 11.1
- Discovery 11.0
- Bol A Discovery 10.2
- Bol A Discovery 10.1
- Bol A Discovery 10.0

Architektur

Das folgende Diagramm zeigt, wie Asset-Manager Discovery-Abfragen verwenden können, um von modellierte Anwendungen sowohl in SaaS- als auch On-Premises-Umgebungen zu scannen.

Das Diagramm zeigt den folgenden Workflow: Ein Komponentenmanager verwendet Discovery oder Helix Discovery, um Datenbank- und Software-Instances zu scannen, die auf virtuellen Servern ausgeführt werden, die auf mehreren physischen Servern gehostet werden. Das Tool kann Anwendungen mit Komponenten modellieren, die sich über mehrere virtuelle und physische Server erstrecken.

Technologie-Stack

- Discovery

- Bol Helix Discovery

Tools

- Discovery ist ein Tool zur Erkennung von Rechenzentren, mit dem Sie Ihr Rechenzentrum automatisch erkennen können.
- Bol Helix Discovery ist ein SaaS-basiertes Erkennungs- und Abhängigkeitsmodellierungssystem, mit dem Sie Ihre Datenressourcen und ihre Abhängigkeiten dynamisch modellieren können.

Bewährte Methoden

Es hat sich bewährt, Anwendungs-, Abhängigkeits- und Infrastrukturdaten zuzuordnen, wenn Sie in die Cloud migrieren. Die Zuordnung hilft Ihnen, die Komplexität Ihrer aktuellen Umgebung und die Abhängigkeiten zwischen verschiedenen Komponenten zu verstehen.

Die Komponenteninformationen, die diese Abfragen bereitstellen, sind aus mehreren Gründen wichtig:

1. Planung – Wenn Sie die Abhängigkeiten zwischen Komponenten verstehen, können Sie den Migrationsprozess effektiver planen. Beispielsweise müssen Sie möglicherweise zuerst bestimmte Komponenten migrieren, um sicherzustellen, dass andere erfolgreich migriert werden können.
2. Risikobewertung – Die Zuordnung der Abhängigkeiten zwischen Komponenten kann Ihnen helfen, potenzielle Risiken oder Probleme zu identifizieren, die während des Migrationsprozesses auftreten können. Sie könnten beispielsweise feststellen, dass bestimmte Komponenten auf veralteten oder nicht unterstützten Technologien basieren, die zu Problemen in der Cloud führen könnten.
3. Cloud-Architektur – Die Zuordnung Ihrer Anwendungs- und Infrastrukturdaten kann Ihnen auch dabei helfen, eine geeignete Cloud-Architektur zu entwerfen, die Ihren organisatorischen Anforderungen entspricht. Beispielsweise müssen Sie möglicherweise eine mehrstufige Architektur entwerfen, um Hochverfügbarkeits- oder Skalierbarkeitsanforderungen zu unterstützen.

Insgesamt sind die Zuordnung von Anwendungs-, Abhängigkeits- und Infrastrukturdaten ein entscheidender Schritt im Cloud-Migrationsprozess. Die Mapping-Übung kann Ihnen helfen, Ihre aktuelle Umgebung besser zu verstehen, potenzielle Probleme oder Risiken zu identifizieren und eine geeignete Cloud-Architektur zu entwerfen.

Polen

Identifizieren und Auswerten von Erkennungstools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie ITSM-Besitzer.	Identifizieren Sie die IT Service Management (ITSM)-Besitzer (in der Regel wenden Sie sich an die Betriebsunterstützungsteams).	Migrationsleiter
Überprüfen Sie CMDB.	Identifizieren Sie die Anzahl der Konfigurationsverwaltungsdatenbanken (CMDBs), die Komponenteninformationen enthalten, und identifizieren Sie dann die Quellen dieser Informationen.	Migrationsleiter
Identifizieren Sie Erkennungstools und überprüfen Sie, ob Bol Discovery verwendet wird.	Wenn Ihre Organisation Bol Discovery verwendet, um Daten über Ihre Umgebung an das CMDB-Tool zu senden, überprüfen Sie den Umfang und die Abdeckung der Scans. Überprüfen Sie beispielsweise, ob Bol Discovery alle Rechenzentren scannt und ob sich die Zugriffsserver in Perimeterzonen befinden.	Migrationsleiter
Überprüfen Sie den Grad der Anwendungsmodellierung.	Überprüfen Sie, ob Anwendungen in Discovery modelliert sind. Falls nicht, empfehlen Sie die Verwendung des Discovery-Tools, um zu modellieren, welche	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	laufenden Software-Instances eine Anwendung und einen Geschäftsservice bereitstellen.	

Extrahieren von Infrastrukturdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten auf physischen und virtuellen Servern.	Um Daten auf den physische n und virtuellen Servern zu extrahieren, die von Discovery gescannt wurden, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Host show key as 'Serverid', virtual, name as 'HOSTNAME', os_type as 'osName', os_version as 'OS Version', num_logical_processors as 'Logical Processor Counts', cores_per_processor as 'Cores per Processor', logical_ram as 'Logical RAM', #Consumer:StorageUse:Provider:DiskDrive.size as 'Size'` Hinweis: Sie können extrahier te Daten verwenden, um die geeigneten Instance-Größen für die Migration zu ermitteln.	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten aus modellierten Anwendungen.	Wenn Ihre Anwendungen in Ker Discovery modellier t sind, können Sie Daten über die Server extrahieren, auf denen die Anwendung ssoftware ausgeführt wird. Um die Servernamen abzurufen, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search SoftwareInstance show key as 'ApplicationID', #RunningSoftware:HostedSoftware:Host:Host.key as 'ReferenceID', type, name` Hinweis: Anwendungen werden in Ker Discovery durch eine Sammlung von laufenden Software-Instances modellier t. Die Anwendung hängt von allen Servern ab, auf denen die Anwendungssoftware ausgeführt wird.	Besitzer der Discovery-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten in Datenbanken.	Um eine Liste aller gescannten Datenbanken und der Server abzurufen, auf denen diese Datenbanken ausgeführt werden, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Database show key as 'Key', name, type as 'Source Engine Type', #Detail:Detail:ElementWithDetail:SoftwareInstance.name as 'Software Instance', #Detail:Detail:ElementWithDetail:SoftwareInstance.product_version as 'Product Version', #Detail:Detail:ElementWithDetail:SoftwareInstance.edition as 'Edition', #Detail:Detail:ElementWithDetail:SoftwareInstance.#RunningSoftware:HostedSoftware:Host:Host.key as 'ServerID'`	App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten zur Serverkommunikation.	Um Informationen zur gesamten Netzwerkk ommunikation zwischen Servern zu erhalten, die von Discovery anhand historisc her Netzwerkkommunikat ionsprotokolle erfasst werden, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Host TRAVERSE InferredElement:Inference:Associate:DiscoveryAccess TRAVERSE DiscoveryAccess:DiscoveryAccessResult:DiscoveryResult:NetworkConnectionList TRAVERSE List:List:Member:DiscoveredNetworkConnection PROCESS WITH networkConnectionInfo`	Besitzer der Discovery-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten zur Anwendungserkennung.	Um Informationen zu Anwendungsabhängigkeiten zu erhalten, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search SoftwareInstance show key as 'SRC App ID', #Dependant:Dependency:DependedUpon:SoftwareInstance.key as 'DEST App ID'`	Besitzer der Discovery-Anwendung
Extrahieren Sie Daten zu Geschäftsservices.	Um Daten auf Geschäftsservices zu extrahieren, die von Hosts bereitgestellt werden, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Host show name, #Host:HostedSoftware:AggregateSoftware:BusinessService.name as 'Name'`	Besitzer der Discovery-Anwendung

Fehlerbehebung

Problem	Lösung
Eine Abfrage kann nicht ausgeführt werden oder enthält nicht ausgefüllte Spalten.	Überprüfen Sie die Komponentendatensätze in Bol Discovery und bestimmen Sie, welche Felder Sie benötigen. Ersetzen Sie dann diese

Problem	Lösung
	Felder in der Abfrage mithilfe von Query Builder .
Die Details einer abhängigen Komponente werden nicht ausgefüllt.	Dies ist wahrscheinlich auf Zugriffsb erechtigungen oder Netzwerkkonnektivität zurückzuführen. Das Erkennungstool verfügt möglicherweise nicht über die erforderlichen Berechtigungen für den Zugriff auf bestimmte Komponenten, insbesondere wenn sie sich in verschiedenen Netzwerken oder in verschied enen Umgebungen befinden. Wir empfehlen Ihnen, eng mit Experten für Ermittlungsthemen zu arbeiten, um sicherzus tellen, dass alle relevanten Komponenten identifiziert werden.

Zugehörige Ressourcen

Referenzen

- Berechtigung zur Lizenzierung von Discovery (BMC-Dokumentation)
- Features und Komponenten von Discovery (BMC-Dokumentation)
- Benutzerhandbuch für Discovery (BMC-Dokumentation)
- Suchen nach Daten (on Bol Discovery) (BMC-Dokumentation)
- Portfolioerkennung und -analyse für die Migration (AWS Prescriptive Guidance)

Tutorials und Videos

- Discovery: Webinar – Bewährte Methoden für Berichtsabfragen (Teil 1) (YouTube)

Umziehen

Themen

Migrieren Sie eine Amazon RDS for Oracle Oracle-Datenbank auf ein anderes AWS-Konto und eine andere AWS-Region mithilfe von AWS DMS für die laufende Replikation

Erstellt von Durga Prasad Cheepuri (AWS) und Eduardo Valentim (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for Oracle
R-Typ: Umziehen	Arbeitslast: Oracle	Technologien: Migration; Datenbanken
AWS-Dienste: Amazon RDS		

Übersicht

> Warnung: IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Dieses Muster führt Sie durch die Schritte zur Migration einer Quelldatenbank von Amazon Relational Database Service (Amazon RDS) für Oracle zu einer anderen AWS-Konto und. AWS-Region Das Muster verwendet einen DB-Snapshot für eine einmalige vollständige Datenladung und aktiviert AWS Database Migration Service (AWS DMS) für die fortlaufende Replikation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive Datenbank AWS-Konto , die die Amazon RDS for Oracle Oracle-Quelldatenbank enthält, die mit einem anderen Schlüssel AWS Key Management Service (AWS KMS) verschlüsselt wurde
- Aktiv AWS-Konto in einer anderen Datenbank als AWS-Region der Quelldatenbank, die für die Amazon RDS for Oracle Oracle-Zieldatenbank verwendet werden soll

- Virtual Private Cloud (VPC) -Peering zwischen Quell- und Ziel-VPCs
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Ziel für AWS DMS

Produktversionen

- Oracle-Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen und Editionen finden Sie in der Dokumentation unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und mit Verwenden einer Oracle-Datenbank als Ziel für. AWS DMS AWS Informationen zu den von Amazon RDS unterstützten Oracle-Versionen finden Sie unter Oracle auf Amazon RDS.

Architektur

Quell- und Zieltechnologie-Stacks

- Amazon RDS for Oracle Oracle-DB-Instance

Architektur für fortlaufende Replikation

Tools

Tools, die für das einmalige vollständige Laden von Daten verwendet werden

- Amazon Relational Database Service (Amazon RDS) erstellt einen Speicher-Volume-Snapshot Ihrer DB-Instance und sichert dabei die gesamte DB-Instance und nicht nur einzelne Datenbanken. Beim Erstellen eines DB-Snapshots wählen Sie die DB-Instance aus, die gesichert werden soll, und benennen den DB-Snapshot, damit Sie später mit diesem eine Wiederherstellung ausführen können. Die Zeit, die für die Erstellung eines Snapshots benötigt wird, hängt von der Größe Ihrer Datenbanken ab. Da der Snapshot das gesamte Speichervolume umfasst, wirkt sich die Größe von Dateien, wie z. B. temporäre Dateien, auch auf die Zeit aus, die zum Erstellen des Snapshots benötigt wird. Weitere Informationen zur Verwendung von DB-Snapshots finden Sie unter Erstellen eines DB-Snapshots in der Amazon RDS-Dokumentation.

- AWS Key Management Service (AWS KMS) erstellt einen Schlüssel für die Amazon RDS-Verschlüsselung. Wenn Sie eine verschlüsselte DB-Instance erstellen, können Sie auch die AWS KMSSchlüssel-ID für Ihren Verschlüsselungsschlüssel angeben. Wenn Sie keine AWS KMSSchlüssel-ID angeben, verwendet Amazon RDS Ihren Standard-Verschlüsselungsschlüssel für Ihre neue DB-Instance. AWS KMSerstellt Ihren Standard-Verschlüsselungsschlüssel für Ihre AWS-Konto. Ihr AWS-Konto hat für jeden einen anderen Standard-Verschlüsselungsschlüssel AWS-Region. Für dieses Muster sollte die Amazon RDS-DB-Instance mit dem nicht standardmäßigen AWS KMSSchlüssel verschlüsselt werden. Weitere Informationen zur Verwendung von AWS KMSSchlüsseln für die Amazon RDS-Verschlüsselung finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen in der Amazon RDS-Dokumentation.

Tools, die für die laufende Replikation verwendet werden

- AWS Database Migration Service (AWS DMS) wird verwendet, um laufende Änderungen zu replizieren und die Quell- und Zieldatenbank synchron zu halten. Weitere Informationen zur Verwendung AWS DMS für die laufende Replikation finden Sie in der AWS DMS Dokumentation unter Arbeiten mit einer AWS DMS Replikationsinstanz.

Epen

Konfiguriere deine Quelle AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Oracle-DB-Quellinstanz vor.	Lassen Sie die Amazon RDS for Oracle DB-Instance im ARCHIVELOG-Modus laufen und legen Sie den Aufbewahrungszeitraum fest. Einzelheiten finden Sie unter Arbeiten mit einer AWS verwalteten Oracle-Datenbank als Quelle für. AWS DMS	DBA
Legen Sie die zusätzliche Protokollierung für die Oracle-DB-Quellinstanz fest.	Legen Sie die zusätzliche Protokollierung auf Datenbank- und Tabellenebene für die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon RDS for Oracle Oracle-DB-Instance fest. Einzelheiten finden Sie unter Arbeiten mit einer AWS verwalteten Oracle-Datenbank als Quelle für. AWS DMS	
Aktualisieren Sie die AWS KMS Schlüsselrichtlinie im Quellkonto.	Aktualisieren Sie die AWS KMS Schlüsselrichtlinie in der Quelle AWS-Konto , damit das Ziel AWS-Konto den verschlüsselten Amazon AWS KMS RDS-Schlüssel verwenden kann. Einzelheiten finden Sie in der AWS KMS Dokumentation.	SysAdmin
Erstellen Sie einen manuellen Amazon RDS-DB-Snapshot der Quell-DB-Instance.		AWS IAM-Benutzer
Teilen Sie den manuellen, verschlüsselten Amazon RDS-Snapshot mit dem Ziel AWS-Konto.	Einzelheiten finden Sie unter Einen DB-Snapshot teilen.	AWS IAM-Benutzer

Konfigurieren Sie Ihr Ziel AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Richtlinie bei.	Fügen Sie im Ziel AWS-Konto dem Root-IAM-Benutzer eine AWS Identity and Access Management (IAM-) Richtlinie hinzu, damit der IAM-Benut	SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zer mithilfe des gemeinsam en Schlüssels einen verschlüs selten DB-Snapshot kopieren kann. AWS KMS	
Wechseln Sie zur Quelle. AWS-Region		AWS IAM-Benutzer
Kopieren Sie den geteilten Snapshot.	Wählen Sie in der Amazon RDS-Konsole im Bereich Snapshots die Option Für mich freigegeben und wählen Sie den geteilten Snapshot aus. Kopieren Sie den Snapshot in dieselbe Datenbank AWS-Region wie die Quelldatenbank, indem Sie den Amazon-Ressourcenn amen (ARN) für den von der Quelldatenbank verwendet en AWS KMS Schlüssel verwenden. Einzelheiten finden Sie unter Kopieren eines DB-Snapshots.	AWS IAM-Benutzer
Wechseln Sie zum Ziel AWS-Region und erstellen Sie einen neuen AWS KMS Schlüssel.		AWS IAM-Benutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie den Snapshot.	Wechseln Sie zur Quelle AWS-Region. Wählen Sie auf der Amazon RDS-Konsole im Bereich Snapshots die Option Owned by Me und wählen Sie den kopierten Snapshot aus. Kopieren Sie den Snapshot auf das Ziel, AWS-Region indem Sie den AWS KMS Schlüssel für das neue Ziel AWS-Region verwenden.	AWS IAM-Benutzer
Stellen Sie den Snapshot wieder her.	Wechseln Sie zum Ziel AWS-Region. Wählen Sie auf der Amazon RDS-Konsole im Bereich Snapshots die Option Owned by Me aus. Wählen Sie den kopierten Snapshot aus und stellen Sie ihn in einer Amazon RDS for Oracle DB-Instance wieder her. Einzelheiten finden Sie unter Aus einem DB-Snapshot wiederherstellen.	AWS IAM-Benutzer

Bereiten Sie Ihre Quelldatenbank für die laufende Replikation vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Oracle-Benutzer mit den entsprechenden Berechtigungen.	Erstellen Sie einen Oracle-Benutzer mit den erforderlichen Rechten für Oracle als Quelle für AWS DMS. Einzelheiten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der AWS DMS Dokumentation.	
Konfigurieren Sie die Quelldatenbank für Oracle LogMiner oder Oracle Binary Reader.		DBA

Bereiten Sie Ihre Zieldatenbank für die laufende Replikation vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Oracle-Benutzer mit den entsprechenden Berechtigungen.	Erstellen Sie einen Oracle-Benutzer mit den erforderlichen Rechten für Oracle als Ziel für AWS DMS. Einzelheiten finden Sie in der AWS DMS Dokumentation.	DBA

Komponenten erstellen AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz im Ziel AWS-Region.	Erstellen Sie eine Replikationsinstanz in der VPC des Ziels AWS-Region. Einzelheiten finden Sie in der AWS DMS Dokumentation.	AWS IAM-Benutzer
Erstellen Sie Quell- und Zielendpunkte mit der erforderlichen Verschlüsselung und testen Sie Verbindungen.	Einzelheiten finden Sie in der AWS DMS Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Replikationsaufgaben.	1. Wählen Sie als Migrationstyp die Option Laufende Replikation aus. 2. Verwenden Sie für den Startpunkt der Change Data Capture (CDC) die Oracle-Systemänderungsnummer (SCN), als der Amazon RDS-Snapshot vollständig geladen wurde, oder den Zeitstempel, als der Vollladevorgang ausgeführt wurde. 3. Wählen Sie für **`TargetTablePrepMode`** DO_NOTHING. Wenn die Aufgabe LOB-Datentabellen (Large Binary Object) enthält, wählen Sie den Modus Limitiert aus und legen Sie die maximale LOB-Größe auf die maximale Größe der LOB-Daten in der Tabelle fest. 4. Aktivieren Sie die Protokollierung. 5. Gruppieren Sie Tabellen, die über Schlüssel miteinander verknüpft sind, zu einer einzigen Aufgabe. Wenn es Tabellen mit einer großen Menge an LOB-Daten gibt und die	IAM-Benutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Tabelle keine Beziehung zu anderen Tabellen hat, erstellen Sie dafür eine separate Aufgabe mit den zuvor beschriebenen LOB-Einstellungen. Einzelheiten finden Sie in der AWS DMS Dokumentation.	
Starten Sie die Aufgaben und überwachen Sie sie.	Einzelheiten finden Sie in der AWS DMS Dokumentation.	AWS IAM-Benutzer
Aktivieren Sie bei Bedarf die Validierung der Aufgabe.	Beachten Sie, dass die Aktivierung der Validierung Auswirkungen auf die Leistung der Replikation hat. Einzelhei ten finden Sie in der AWS DMS Dokumentation.	AWS IAM-Benutzer

Zugehörige Ressourcen

- Änderung einer wichtigen Richtlinie
- Manuellen Amazon RDS-DB-Snapshot erstellen
- Einen manuellen Amazon RDS-DB-Snapshot teilen
- Einen Snapshot kopieren
- Wiederherstellung aus einem Amazon RDS-DB-Snapshot
- Erste Schritte mit AWS DMS
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwendung einer Oracle-Datenbank als Ziel für AWS DMS
- AWS DMS Einrichtung mit VPC-Peering
- Wie teile ich manuelle Amazon RDS-DB-Snapshots oder DB-Cluster-Snapshots mit anderen? AWS-Konto (Artikel im AWS Knowledge Center)

Migrieren Sie VMware SDDC mit VMware HCX zu VMware Cloud on AWS

Erstellt von Deepak Kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Networking	Ziel: VMware Cloud on AWS
R-Typ: Umziehen	Technologien: Migration; Infrastruktur	

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt die Verwendung von VMware Hybrid Cloud Extension (HCX) zur Migration Ihrer lokalen virtuellen Maschinen (VMs) und Anwendungen zu VMware Cloud on Amazon Web Services (AWS). Bei der Migration wird Software-Defined Data Center (SDDC) -Software der Enterprise-Klasse von VMware in der AWS-Cloud verwendet, um einen optimierten Zugriff auf AWS-Services zu ermöglichen.

VMware Cloud on AWS integriert Rechen-, Speicher- und Netzwerkvirtualisierungsprodukte (vSphere, vSAN und VMware NSX) in das VMware vCenter Servermanagement, das für die Ausführung auf einer dedizierten, elastischen Bare-Metal-AWS-Infrastruktur optimiert ist. Die daraus resultierende Infrastruktur ist wartungsarm, vereinfacht und hyperkonvergiert.

Mit diesem Service können IT-Teams ihre Cloud-Ressourcen mit vertrauten VMware-Tools verwalten. Weitere Informationen finden Sie unter VMware Cloud on AWS auf der VMware-Website.

VMware HCX unterstützt drei Arten von Cloud-Migrationen:

- Hybridität (Rechenzentrumserweiterung): Erweiterung eines vorhandenen, lokalen VMware-SDDC auf AWS, um eine Erweiterung des Platzbedarfs, On-Demand-Kapazität, eine Test-/Entwicklungsumgebung und virtuelle Desktops bereitzustellen.

- Cloud-Evakuierung (Aktualisierung der Infrastruktur im gesamten Rechenzentrum): Konsolidierung von Rechenzentren und vollständige Umstellung auf die AWS-Cloud (einschließlich der Verwaltung der Rechenzentrumszusammenlegung oder der Beendigung des Leasingvertrags).
- Anwendungsspezifische Migration: Verschieben einzelner Anwendungen in die AWS-Cloud, um spezifische Geschäftsanforderungen zu erfüllen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eröffnen Sie ein AWS-Konto (erforderlich für die Erstellung von VMware Cloud SDDC).
- Eröffnen Sie ein My VMware-Konto. Registrieren Sie sich unter https://my.vmware.com/web/vmware/ und füllen Sie alle Felder aus.
- Überprüfen Sie die Version von vCenter und Hosts und erfassen Sie die Anzahl der VMs. Bitten Sie nach Möglichkeit um einen RVTools-Export, um Informationen zu Ihren virtuellen Umgebungen anzuzeigen. Wir empfehlen vCenter Version 6.0 oder höher.
- Sie müssen verteilte virtuelle Switches bereitstellen, wenn Sie Rechenzentrumsnetzwerke (L2) erweitern, vMotion mithilfe von HCX testen oder Anwendungsabhängigkeiten mithilfe von vRealize Network Insight analysieren möchten.
- Wählen Sie ein konfliktfreies lokales aktuelles Management-Subnetzwerk aus, um das SDDC auf VMware Cloud on AWS zu erstellen.
- Überprüfen Sie die HCX-Anforderungen, indem Sie die Voraussetzungen im VMware HCX-Benutzerhandbuch überprüfen.
- Identifizieren und gruppieren Sie VMs für Migrationswellen. Suchen Sie nach VMs, die Sie zum Testen verwenden können.
- Sammeln Sie alle Daten über den relativen Bandbreitenverbrauch, die WAN-Komprimierung und die Datenübertragungsgeschwindigkeit.

Hinweise

- VMware NSX-V oder NSX-T vor Ort ist nicht erforderlich.
- Keine zusätzlichen Kosten für HCX (es ist in VMware Cloud on AWS enthalten).

Architektur

Das folgende Diagramm zeigt die HCX-Lösung, die auf Services aus mehreren Komponenten basiert. Jede Komponente unterstützt eine bestimmte Funktion in der HCX-Lösung. Weitere Informationen zu den einzelnen HCX-Komponenten finden Sie im Blogbeitrag Migrieren von Workloads zu VMware Cloud on AWS with Hybrid Cloud Extension (HCX).

Quelltechnologie-Stack

- Lokale VMs und Anwendungen, die von VMware vSphere verwaltet werden

Zieltechnologie-Stack

- VMware Cloud in AWS

Tools

- VMware HCX — VMware HCX ist ein Tool, mit dem Sie Ihre Anwendungen und Workloads zwischen Rechenzentren und Cloud-Umgebungen migrieren können. Es ist in VMware Cloud on AWS enthalten.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Migration sstrategie.	Entscheiden Sie, ob Sie Ihr Rechenzentrum erweitern (Hybridität), alle Ihre Rechenzentren verlagern (Cloud-Evakuierung) oder bestimmte Anwendungen zu AWS verlagern möchten.	SysAdmin, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die HCX-Anforderungen.	Informationen zur Migration finden Sie im VMware HCX-Benutzerhandbuch.	SysAdmin, Besitzer der App

Migrieren Sie zu VMware Cloud on AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Ihre VMs oder Anwendungen.	Weitere Informationen finden Sie unter Hybridmigration mit VMware HCX in der VMware-Dokumentation.	SysAdmin, Besitzer der App

Zugehörige Ressourcen

- VMware Cloud on AWS: Erste Schritte
- Hybridmigration mit VMware HCX
- Benutzerhandbuch für VMware HCX
- Preise für VMware Cloud on AWS
- Roadmap für VMware Cloud on AWS

Migrieren einer Amazon RDS-DB-Instance zu einer anderen VPC oder einem anderen Konto

Erstellt von Dhr Boljioti Mukherjee (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Amazon RDS	Ziel: Amazon RDS
R-Typ: Verschieben	Technologien: Migration; Datenbanken	AWS-Services: Amazon RDS; Amazon VPC

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS)-DB-Instance von einer Virtual Private Cloud (VPC) zu einer anderen im selben AWS-Konto oder von einem AWS-Konto zu einem anderen AWS-Konto.

Dieses Muster ist nützlich, wenn Sie Ihre Amazon-RDS-DB-Instances aus Trennungs- oder Sicherheitsgründen zu einer anderen VPC oder einem anderen Konto migrieren möchten (z. B. wenn Sie Ihren Anwendungs-Stack und Ihre Datenbank in verschiedenen VPCs platzieren möchten).

Die Migration einer DB-Instance zu einem anderen AWS-Konto umfasst Schritte wie das Erstellen eines manuellen Snapshots, dessen Freigabe und das Wiederherstellen des Snapshots im Zielkonto. Dieser Prozess kann je nach Datenbankänderungen und Transaktionsraten zeitaufwändig sein. Es führt auch zu Datenbankausfallzeiten. Planen Sie daher für die Migration voraus. Ziehen Sie eine Blau/Grün-Bereitstellungsstrategie in Betracht, um Ausfallzeiten zu minimieren. Alternativ können Sie AWS Data Migration Service (AWS DMS) bewerten, um Ausfallzeiten für die Änderung zu minimieren. Dieses Muster deckt diese Option jedoch nicht ab. Weitere Informationen finden Sie in der AWS DMS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Für die VPC, Subnetze und Amazon RDS-Konsole erforderliche AWS Identity and Access Management (IAM)-Berechtigungen

Einschränkungen

- Änderungen an einer VPC führen zu einem Neustart der Datenbank, was zu Anwendungsausfällen führt. Wir empfehlen Ihnen, in niedrigen Spitzenzeiten zu migrieren.
- Einschränkungen bei der Migration von Amazon RDS zu einer anderen VPC:
  - Die DB-Instance, die Sie migrieren, muss eine einzelne Instance ohne Standby sein. Es darf kein Mitglied eines Clusters sein.
  - Amazon RDS darf sich nicht in mehreren Availability Zones befinden.
  - Amazon RDS darf keine Lesereplikate haben.
  - Die in der Ziel-VPC erstellte Subnetzgruppe muss über Subnetze aus der Availability Zone verfügen, in der die Quelldatenbank ausgeführt wird.
- Einschränkungen bei der Migration von Amazon RDS zu einem anderen AWS-Konto:
  - Die Freigabe von Snapshots, die mit dem Standard-Serviceschlüssel für Amazon RDS verschlüsselt sind, wird derzeit nicht unterstützt.

Architektur

Migrieren zu einer VPC im selben AWS-Konto

Das folgende Diagramm zeigt den Workflow für die Migration einer Amazon RDS-DB-Instance zu einer anderen VPC im selben AWS-Konto.

Die Schritte bestehen aus Folgendem. Detaillierte Anweisungen finden Sie im Abschnitt „Epics“.

1. Erstellen Sie eine DB-Subnetzgruppe in der Ziel-VPC. Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen, mit denen Sie beim Erstellen von DB-Instances eine bestimmte VPC angeben können.
2. Konfigurieren Sie die Amazon RDS-DB-Instance in der Quell-VPC für die Verwendung der neuen DB-Subnetzgruppe.
3. Wenden Sie die Änderungen an, um die Amazon RDS-DB zur Ziel-VPC zu migrieren.

Migrieren zu einem anderen AWS-Konto

Das folgende Diagramm zeigt den Workflow für die Migration einer Amazon RDS-DB-Instance zu einem anderen AWS-Konto.

Die Schritte bestehen aus Folgendem. Detaillierte Anweisungen finden Sie im Abschnitt „Epics“.

1. Greifen Sie auf die Amazon RDS-DB-Instance im AWS-Quellkonto zu.
2. Erstellen Sie einen Amazon RDS-Snapshot im AWS-Quellkonto.
3. Teilen Sie den Amazon RDS-Snapshot mit dem AWS-Zielkonto.
4. Greifen Sie auf den Amazon RDS-Snapshot im AWS-Zielkonto zu.
5. Erstellen Sie eine Amazon RDS-DB-Instance im AWS-Zielkonto.

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) hilft Ihnen beim Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Bewährte Methoden

- Wenn die Datenbankausfallzeit bei der Migration einer Amazon RDS-DB-Instance zu einem anderen -Konto ein Problem darstellt, empfehlen wir Ihnen, AWS DMS zu verwenden. Dieser Service bietet eine Datenreplikation, was zu einer Ausfallzeit von weniger als fünf Minuten führt.

Polen

Migrieren zu einer anderen VPC im selben AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer neuen VPC.	Erstellen Sie in der Amazon-VPC-Konsole eine neue VPC und Subnetze mit den	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gewünschten Eigenschaften und IP-Adressbereichen. Detaillierte Anweisungen finden Sie in der Amazon-VPC-Dokumentation.	
Erstellen Sie eine DB-Subnetzgruppe.	In der Amazon-RDS-Konsole: 1. Wählen Sie Subnetzgruppen, DB-Subnetzgruppe erstellen aus. 2. Geben Sie den Namen der Subnetzgruppe, die Beschreibung und die VPC-ID ein. 3. Fügen Sie die Subnetze hinzu, die zur Subnetzgruppe gehören. Fügen Sie Subnetze hinzu, um mindestens zwei Availability Zones abzudecken. 4. Wählen Sie Erstellen. Weitere Informationen finden Sie in der Amazon-RDS-Dokumentation.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Amazon RDS-DB-Instance, um die neue Subnetzgruppe zu verwenden.	In der Amazon-RDS-Konsole: 1. Wählen Sie im Navigationsbereich Datenbanken und dann die zu migrierende Amazon-RDS-DB-Instance aus. 2. Wählen Sie im Abschnitt Konnektivität die Subnetzgruppe aus, die der Ziel-VPC zugeordnet ist. 3. Wählen Sie im Abschnitt Änderungen planen die Option Sofort anwenden aus. Wenn die Migration zur Ziel-VPC abgeschlossen ist, wird der Amazon RDS-DB-Instance die Standardsicherheitsgruppe der Ziel-VPC zugewiesen. Sie können eine neue Sicherheitsgruppe für diese VPC mit den erforderlichen Regeln für ein- und ausgehenden Datenverkehr für Ihre DB-Instance konfigurieren. Alternativ können Sie die AWS Command Line Interface (AWS CLI) verwenden, um die Migration zur Ziel-VPC durchzuführen, indem Sie explizit die neue VPC-Siche	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rheitsgruppen-ID angeben. Beispielsweise: `aws rds modify-db-instance \ --db-instance-identifier testrds \ --db-subnet-group-name new-vpc-subnet-group \ --vpc-security-group-ids sg-idxxxx \ --apply-immediately`	

Migrieren zu einem anderen AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue VPC und Subnetzgruppe im AWS-Zielkonto.	1. Erstellen Sie in der Amazon-VPC-Konsole eine neue VPC mit den gewünschten Eigenschaften und IP-Adressbereichen. Detaillierte Anweisungen finden Sie in der Amazon-VPC-Dokumentation. 2. Erstellen Sie Subnetze für die neue VPC, indem Sie den Anweisungen in der Amazon-VPC-Dokumentation folgen. 3. Erstellen Sie in der Amazon-RDS-Konsole DB-Subnetzgruppen.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie in der Amazon-RDS-Dokumentation.	
Teilen Sie einen manuellen Snapshot der Datenbank und geben Sie ihn für das Zielkonto frei.	1. Erstellen Sie einen manuellen Snapshot der Quelldatenbank, indem Sie den Anweisungen in der Amazon-RDS-Dokumentation folgen. 2. Teilen Sie den Snapshot mit dem AWS-Zielkonto, indem Sie die ID des Zielkontos angeben. Anweisungen finden Sie im re:Post-Artikel zur Freigabe von DB-Snapshots für andere -Konten.	Administrator
Starten Sie eine neue Amazon RDS-DB-Instance.	Starten Sie eine neue Amazon RDS-DB-Instance aus dem freigegebenen Snapshot im AWS-Zielkonto. Anweisungen finden Sie in der Amazon-RDS-Dokumentation.	Administrator

Zugehörige Ressourcen

- Amazon-VPC-Dokumentation
- Dokumentation zu Amazon RDS
- Wie ändere ich die VPC für eine RDS-DB-Instance? (AWS re:Post-Artikel)
- Wie übertrage ich den Besitz von Amazon RDS-Ressourcen auf ein anderes AWS-Konto? (AWS re:Post-Artikel)

- Wie teile ich manuelle Amazon RDS-DB-Snapshots oder Aurora-DB-Cluster-Snapshots mit einem anderen AWS-Konto? (AWS re:Post-Artikel)
- AWS DMS-Dokumentation

Migrieren einer DB-Instance von Amazon RDS für Oracle zu einer anderen VPC

Erstellt von Pinesh Singal (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS für Oracle
R-Typ: Verschieben	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Migrationsmuster bietet step-by-step Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) for Oracle Database (DB)-Instance von einer Virtual Private Cloud (VPC) zu einer anderen VPC im selben Amazon Web Services (AWS)-Konto. Sie können dieses Muster beispielsweise verwenden, wenn Ihr Unternehmen erfordert, dass sich die Datenbank und der Amazon Elastic Compute Cloud (Amazon EC2)-Anwendungsserver in derselben VPC befinden.

Das Muster beschreibt eine Online-Migrationsstrategie ohne Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen.

Um eine DB-Instance von Amazon RDS für Oracle in eine andere VPC zu verschieben, müssen Sie die Amazon-RDS-Subnetzgruppe ändern. Diese Subnetzgruppe muss mit der neuen VPC und den erforderlichen Subnetzen vorkonfiguriert sein. Während der VPC-Änderung von einem Netzwerk zu einem anderen wird die Amazon-RDS-Instance neu gestartet, sodass die Datenbank nicht zugänglich ist, während die Bewegung ausgeführt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Zwei VPCs mit privaten Subnetzen

- Eine Datenbank-Instance von Amazon RDS für Oracle (in Betrieb), konfiguriert mit ein- und ausgehenden Sicherheitsgruppen

Einschränkungen

- Eine DB-Instance, die sich über mehrere Availability Zones (Multi-AZ) erstreckt, wird nicht unterstützt. Dieses Muster bietet jedoch eine Möglichkeit, diese Einschränkung zu umgehen.
- Die DB-Instance kann nicht migriert werden, während ein Lesereplikat aktiviert ist.
- Die Subnetzgruppe in der neuen VPC sollte sich in derselben Availability Zone wie die Datenbank befinden.
- Die Migration sollte während des geplanten Wartungszeitraums oder Zeiten mit geringem Datenverkehr erfolgen, da das Verschieben der DB in eine andere VPC zu einem Neustart der Datenbank führt, was zu Anwendungsausfällen für einige Minuten führt.

Produktversionen

- DB-Instance von Amazon RDS für Oracle, 12.1.0.2 und höher

Architektur

Quelltechnologie-Stack

- Eine DB-Instance von Amazon RDS für Oracle 12.1.0.2.v22 in einer VPC
- Eine VPC, die in einer separaten Routing-Tabelle konfiguriert ist
- In einer VPC konfigurierte Amazon-RDS-Subnetzgruppen
- Amazon-RDS-Optionsgruppen (falls erforderlich)

Zieltechnologie-Stack

- Datenbank-Instance von Amazon RDS für Oracle mit Version 12.1.0.2.v22 in einer anderen VPC
- Amazon VPC in separater Route konfiguriert
- Amazon-RDS-Subnetzgruppen, die in einer neuen VPC konfiguriert sind
- Amazon-RDS-Optionsgruppen (falls erforderlich)

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Verwendung der Konsole, um die DB von Amazon RDS für Oracle von einem privaten Subnetz in einer VPC in ein privates Subnetz in einer anderen VPC zu verschieben.

1. Verwenden Sie die Konsole, um die Quell-DB-Instance von Amazon RDS für Oracle zu ändern.
2. Ändern Sie in der Ziel-VPC die Subnetzgruppe und bei Verwendung die Optionsgruppe.

Tools

- Amazon RDS – Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud vereinfacht. Es bietet kostengünstige, anpassbare Kapazität für eine relationale Datenbank und verwaltet allgemeine Datenbankverwaltungsaufgaben. Dieses Muster verwendet Amazon RDS für Oracle.

Polen

Ändern der Konfiguration der Datenbank von Amazon RDS für Oracle in der vorhandenen VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Subnetzgruppe.	Konfigurieren Sie eine Subnetzgruppe in Amazon RDS.	Allgemeines AWS
Erstellen Sie eine Optionsgruppe.	(Optional) Konfigurieren Sie eine Optionsgruppe in Amazon RDS.	Allgemeines AWS
Ändern Sie die DB-Instance von Amazon RDS für Oracle.	Ändern Sie die Datenbank mit der Subnetzgruppe und der Optionsgruppe.	Allgemeines AWS, DBA
Aktualisieren Sie die Oracle-Datenbank, falls erforderlich.	Um die Quelldatenbank von Amazon RDS für Oracle zu migrieren, nehmen Sie die folgenden Änderungen vor:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Entfernen Sie Lesereplikate, falls vorhanden. • Deaktivieren Sie die Multi-AZ-Funktion, falls sie aktiviert ist.	

Konfigurieren der Datenbank von Amazon RDS für Oracle in der Ziel-VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Subnetzgruppe.	Konfigurieren Sie in Amazon RDS eine Subnetzgruppe mithilfe des Subnetzes der neuen VPC und der Availability Zone der Datenbank.	Allgemeines AWS
Erstellen Sie eine Optionsgruppe.	(Optional) Konfigurieren Sie eine Optionsgruppe in Amazon RDS.	Allgemeines AWS
Ändern Sie die Datenbank von Amazon RDS für Oracle.	Ändern Sie die Datenbank mit der neuen Subnetzgruppe und Optionsgruppe der neuen VPC. Sie können diese Änderungen sofort oder in einem Wartungsfenster anwenden. Die Änderung kann einige Minuten dauern. Während der Änderung werden die folgenden Statusänderungen angezeigt: • moving-to-vpc	Allgemeines AWS, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Configuring-enhanced-monitoring • Ändern • Verfügbar Die Änderung fügt die Standardsicherheitsgruppe der neuen VPC hinzu. Fügen Sie nach Bedarf von Amazon RDS für Oracle eine neue Sicherhei tsgruppe an.	
Aktualisieren Sie die Datenbank von Amazon RDS für Oracle, falls erforderlich.	Nehmen Sie nach der Migration zur Zieldatenbank von Amazon RDS für Oracle in der neuen VPC bei Bedarf die folgenden Änderungen vor: • Aktivieren Sie Lesereplikate, falls sie in der Quelldate nbank vorhanden waren. • Aktivieren Sie die Multi-AZ-Funktion, wenn sie in der Quelldatenbank aktiviert war.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendung skonnektivität.	Führen Sie von jeder Anwendung aus einen Datenbankkonnektivitätstest durch. Vergewissern Sie sich, dass die geänderte DB von Amazon RDS für Oracle in der neuen VPC verbunden ist und von der Anwendung aus zugänglich ist.	App-Besitzer

Zugehörige Ressourcen

- Amazon-VPC-Dokumentation
- VPCs und Subnetze
- Arbeiten mit einer DB-Instance in einer VPC
- Dokumentation zu Amazon RDS
- Oracle auf Amazon RDS
- Amazon-RDS-Konsole
- Wie ändere ich die VPC einer Amazon RDS-DB-Instance?

Migrieren eines Amazon-Redshift-Clusters zu einer AWS-Region in China

Erstellt durch Jing Yan (AWS)

R-Typ: Verschieben	Umgebung: Produktion	Technologien: Datenbanken; Migration
Workload: Alle anderen Workloads	AWS-Services: Amazon Redshift	Quelle: AWS Redshift
Ziel: AWS Redshift		

Übersicht

Dieses Muster bietet einen step-by-step Ansatz für die Migration eines Amazon-Redshift-Clusters zu einer AWS-Region in China aus einer anderen AWS-Region.

Dieses Muster verwendet SQL-Befehle, um alle Datenbankobjekte neu zu erstellen, und verwendet den Befehl UNLOAD, um diese Daten von Amazon Redshift in einen Amazon Simple Storage Service (Amazon S3)-Bucket in der -Quellregion zu verschieben. Die Daten werden dann in einen S3-Bucket in der AWS-Region in China migriert. Der COPY-Befehl wird verwendet, um Daten aus dem S3-Bucket zu laden und sie an den Amazon-Redshift-Ziel-Cluster zu übertragen.

Amazon Redshift unterstützt derzeit keine regionsübergreifenden Funktionen wie das Kopieren von Snapshots in AWS-Regionen in China. Dieses Muster bietet eine Möglichkeit, diese Einschränkung zu umgehen. Sie können die Schritte in diesem Muster auch rückgängig machen, um Daten von einer AWS-Region in China in eine andere AWS-Region zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktive AWS-Konten sowohl in einer Region China als auch in einer AWS-Region außerhalb Chinas
- Bestehende Amazon Redshift-Cluster sowohl in einer Region China als auch in einer AWS-Region außerhalb Chinas

Einschränkungen

- Dies ist eine Offline-Migration, was bedeutet, dass der Amazon-Redshift-Quellcluster während der Migration keine Schreibvorgänge ausführen kann.

Architektur

Quelltechnologie-Stack

- Amazon-Redshift-Cluster in einer AWS-Region außerhalb Chinas

Zieltechnologie-Stack

- Amazon-Redshift-Cluster in einer AWS-Region in China

Zielarchitektur

Tools

Tools

- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Sie können Amazon S3 verwenden, um Daten aus Amazon Redshift zu speichern, und Sie können Daten aus einem S3-Bucket in Amazon Redshift kopieren.
- Amazon Redshift – Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud.
- psql – psql ist ein Terminal-basiertes Frontend für PostgreSQL .

Polen

Vorbereiten der Migration in der -Quellregion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten und konfigurieren Sie eine EC2-Instance in der -Quellregion.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Elastic Compute Cloud (Amazon EC2)-Konsole. Ihre aktuelle Region wird in der Navigationsleiste oben auf dem Bildschirm angezeigt. Bei dieser Region darf es sich nicht um eine AWS-Region in China handeln. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option „Instance starten“ aus und erstellen und konfigurieren Sie eine EC2-Instance. Wichtig: Stellen Sie sicher, dass Ihre EC2-Sicherheitsgruppen für eingehende Regeln uneingeschränkten Zugriff auf TCP-Port 22 von Ihrem Quellcomputer zulassen. Anweisungen zum Starten und Konfigurieren einer EC2-Instance finden Sie im Abschnitt „Verwandte Ressourcen“.	
Installieren Sie das psql-Tool.	Laden Sie PostgreSQL herunter und installieren Sie es. Amazon Redshift stellt das psql-Tool nicht bereit, es wird mit PostgreSQL installiert. Weitere Informationen zur Verwendung von psql und zur Installation von PostgreSQL-Tools finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich die Details des Amazon-Redshift-Clusters.	Öffnen Sie die Amazon-Redshift-Konsole und wählen Sie im Navigationsbereich „Cluster“ aus. Wählen Sie dann den Namen des Amazon-Redshift-Clusters aus der Liste aus. Notieren Sie auf der Registerkarte „Eigenschaften“ im Abschnitt „Datenbankkonfigurationen“ den „Datenbanknamen“ und „Port“. Öffnen Sie den Abschnitt „Verbindungsdetails“ und notieren Sie sich den „Endpunkt“, der im Format „Endpunkt:<Port>/<Datenbankname>“ vorliegt. Wichtig: Stellen Sie sicher, dass Ihre Amazon-Redshift-Sicherheitsgruppen für eingehende Regeln uneingeschränkten Zugriff auf TCP-Port 5439 von Ihrer EC2-Instance zulassen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbinden Sie psql mit dem Amazon-Redshift-Cluster.	Geben Sie an einer Eingabeaufforderung die Verbindungsinformationen an, indem Sie den Befehl „psql -h <endpoint> -U <userid> -d <database name> -p <port>“ ausführen. Geben Sie in der psql-Eingabeaufforderung das Passwort für den Benutzer „<userid>“ ein. Sie sind dann mit dem Amazon-Redshift-Cluster verbunden und können interaktiv Befehle eingeben.	DBA
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3-Konsole und erstellen Sie einen S3-Bucket, der die aus Amazon Redshift exportierten Dateien enthält. Anweisungen zum Erstellen eines S3-Buckets finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA, AWS General

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie, die das Entladen von Daten unterstützt.	Öffnen Sie die AWS Identity and Access Management (IAM)-Konsole und wählen Sie „Richtlinien“. Wählen Sie „Richtlinie erstellen“ und dann die Registerkarte „JSON“. Kopieren Sie die IAM-Richtlinie zum Entladen von Daten aus dem Abschnitt „Zusätzliche Informationen“. Wichtig: Ersetzen Sie „s3_bucket_name“ durch den Namen Ihres S3-Buckets. Wählen Sie „Richtlinie überprüfen“ und geben Sie einen Namen und eine Beschreibung für die Richtlinie ein. Wählen Sie „Richtlinie erstellen“.	DBA
Erstellen Sie eine IAM-Rolle, um den UNLOAD-Vorgang für Amazon Redshift zuzulassen.	Öffnen Sie die IAM-Konsole und wählen Sie „Rollen“. Wählen Sie „Rolle erstellen“ und „AWS-Service“ unter „Typ der vertrauenswürdigen Entität auswählen“. Wählen Sie für den Service „Redshift“, wählen Sie „Redshift – Anpassbar“ und dann „Nächstes“. Wählen Sie die Richtlinie „Entladen“, die Sie zuvor erstellt haben, und wählen Sie „Nächstes“. Geben Sie einen „Rollennamen“ ein und wählen Sie „Rolle erstellen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie dem Amazon-Redshift-Cluster eine IAM-Rolle zu.	Öffnen Sie die Amazon-Redshift-Konsole und wählen Sie „IAM-Rollen verwalten“. Wählen Sie im Dropdown-Menü die Option „Verfügbare Rollen“ und dann die Rolle aus, die Sie zuvor erstellt haben. Wählen Sie „Änderungen anwenden“. Wenn der „Status“ für die IAM-Rolle auf der „IAM-Rollen verwalten“ als „In Synchronisierung“ angezeigt wird, können Sie den Befehl UNLOAD ausführen.	DBA
Stoppen Sie Schreibvorgänge in den Amazon-Redshift-Cluster.	Sie müssen daran denken, alle Schreibvorgänge im Amazon-Redshift-Quellcluster zu beenden, bis die Migration abgeschlossen ist.	DBA

Vorbereiten der Migration in der Zielregion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten und konfigurieren Sie eine EC2-Instance in der -Zielregion.	Melden Sie sich bei der AWS-Managementkonsole für eine Region in China an, entweder Peking oder Ningxia. Wählen Sie in der Amazon EC2-Konsole „Instance starten“ aus und erstellen und konfigurieren Sie eine EC2-Instance. Wichtig:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass Ihre Amazon EC2-Sicherheitsgruppen für eingehende Regeln uneingeschränkten Zugriff auf TCP-Port 22 von Ihrem Quellcomputer zulassen. Weitere Anweisungen zum Starten und Konfigurieren einer EC2-Instance finden Sie im Abschnitt „Verwandte Ressourcen“.	
Notieren Sie sich die Details des Amazon-Redshift-Clusters.	Öffnen Sie die Amazon-Redshift-Konsole und wählen Sie im Navigationsbereich „Cluster“ aus. Wählen Sie dann den Namen des Amazon-Redshift-Clusters aus der Liste aus. Notieren Sie auf der Registerkarte „Eigenschaften“ im Abschnitt „Datenbankkonfigurationen“ den „Datenbanknamen“ und „Port“. Öffnen Sie den Abschnitt „Verbindungsdetails“ und notieren Sie sich den „Endpunkt“, der im Format „Endpunkt:<Port>/<Datenbankname>“ vorliegt. Wichtig: Stellen Sie sicher, dass Ihre Amazon-Redshift-Sicherheitsgruppen für eingehende Regeln uneingeschränkten Zugriff auf TCP-Port 5439 von Ihrer EC2-Instance zulassen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbinden Sie psql mit dem Amazon-Redshift-Cluster.	Geben Sie an einer Eingabeaufforderung die Verbindungsinformationen an, indem Sie den Befehl „psql -h <endpoint> -U <userid> -d <database name> -p <port>“ ausführen. Geben Sie in der psql-Eingabeaufforderung das Passwort für den Benutzer „<userid>“ ein. Sie sind dann mit dem Amazon-Redshift-Cluster verbunden und können interaktiv Befehle eingeben.	DBA
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3-Konsole und erstellen Sie einen S3-Bucket, der die exportierten Dateien aus Amazon Redshift enthält. Hilfe zu dieser und anderen Artikeln finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie, die das Kopieren von Daten unterstützt.	Öffnen Sie die IAM-Konsole und wählen Sie „Richtlinien“. Wählen Sie „Richtlinie erstellen“ und dann die Registerkarte „JSON“. Kopieren Sie die IAM-Richtlinie zum Kopieren von Daten aus dem Abschnitt „Zusätzliche Informationen“. Wichtig: Ersetzen Sie „s3_bucket_name“ durch den Namen Ihres S3-Buckets. Wählen Sie „Richtlinie überprüfen“ und geben Sie einen Namen und eine Beschreibung für die Richtlinie ein. Wählen Sie „Richtlinie erstellen“.	DBA
Erstellen Sie eine IAM-Rolle, um den COPY-Vorgang für Amazon Redshift zuzulassen.	Öffnen Sie die IAM-Konsole und wählen Sie „Rollen“. Wählen Sie „Rolle erstellen“ und „AWS-Service“ unter „Typ der vertrauenswürdigen Entität auswählen“. Wählen Sie für den Service „Redshift“, wählen Sie „Redshift – Anpassbar“ und dann „Nächstes“. Wählen Sie die Richtlinie „Kopieren“, die Sie zuvor erstellt haben, und wählen Sie „Weiter“. Geben Sie einen „Rollennamen“ ein und wählen Sie „Rolle erstellen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie dem Amazon-Redshift-Cluster eine IAM-Rolle zu.	Öffnen Sie die Amazon-Redshift-Konsole und wählen Sie „IAM-Rollen verwalten“. Wählen Sie im Dropdown-Menü die Option „Verfügbare Rollen“ und dann die Rolle aus, die Sie zuvor erstellt haben. Wählen Sie „Änderungen anwenden“. Wenn der „Status“ für die IAM-Rolle auf der „IAM-Rollen verwalten“ als „In Synchronisierung“ angezeigt wird, können Sie den Befehl „COPY“ ausführen.	DBA

Überprüfen Sie die Quelldaten und Objektinformationen, bevor Sie mit der Migration beginnen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Zeilen in den Amazon-Redshift-Quelltabellen.	Verwenden Sie die Skripts im Abschnitt „Zusätzliche Informationen“, um die Anzahl der Zeilen in den Amazon-Redshift-Quelltabellen zu überprüfen und aufzuzeichnen. Denken Sie daran, die Daten für die UNLOAD- und COPY-Skripte gleichmäßig aufzuteilen. Dies verbessert die Effizienz beim Entladen und Laden von Daten, da die von jedem Skript abgedeckte Datenmenge ausgeglichen wird.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Anzahl der Datenbankobjekte im Amazon-Redshift-Quellcluster.	Verwenden Sie die Skripts im Abschnitt „Zusätzliche Informationen“, um die Anzahl der Datenbank en, Benutzer, Schemata, Tabellen, Ansichten und benutzerdefinierten Funktione n (UDFs) in Ihrem Amazon-Redshift-Quellcluster zu überprüfen und aufzuzeic hnen.	DBA
Überprüfen Sie die Ergebniss e der SQL-Anweisung vor der Migration.	Einige SQL-Anweisungen für die Datenvalidierung sollten nach tatsächlichen Geschäfts - und Datensituationen sortiert werden. Dadurch werden die importierten Daten überprüft , um sicherzustellen, dass sie konsistent sind und korrekt angezeigt werden.	DBA

Migrieren von Daten und Objekten in die Zielregion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie Amazon-Re dshift-DDL-Skripts.	Generieren Sie Data Definitio n Language (DDL)-Skripte, indem Sie die Links aus dem Abschnitt „SQL-Anwe isungen zum Abfragen von Amazon Redshift“ im Abschnitt „Zusätzliche Informationen“ verwenden. Diese DDL-	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Skripte sollten die Abfragen „Benutzer erstellen“, „Schema erstellen“, „Berechtigungen für das Schema für Benutzer erstellen“, „Tabelle/Ansicht erstellen“, „Berechtigungen für Objekte für Benutzer“ und „Funktion erstellen“ enthalten.	
Erstellen Sie Objekte im Amazon-Redshift-Cluster für die Zielregion.	Führen Sie die DDL-Skripte mithilfe der AWS Command Line Interface (AWS CLI) in der AWS-Region in China aus. Diese Skripts erstellen Objekte im Amazon-Redshift-Cluster für die Zielregion.	DBA
Entladen Sie Amazon-Redshift-Quell-Clusterdaten in den S3-Bucket.	Führen Sie den Befehl UNLOAD aus, um Daten aus dem Amazon-Redshift-Cluster in der Quellregion in den S3-Bucket zu entladen.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die S3-Bucket-Daten der Quellregion in den S3-Bucket der Zielregion.	Übertragen Sie die Daten aus dem S3-Bucket Ihrer Quellregion in den S3-Ziel-Bucket. Da der Befehl „$ aws s3 sync“ nicht verwendet werden kann, stellen Sie sicher, dass Sie den Prozess verwenden, der im Artikel „Übertragung von Amazon S3-Daten von AWS-Regionen in AWS-Regionen in China“ im Abschnitt „Verwandte Ressourcen“ beschrieben ist.	Developer
Laden Sie Daten in den Amazon-Redshift-Ziel-Cluster.	Führen Sie im psql-Tool für Ihre Zielregion den COPY-Befehl aus, um Daten aus dem S3-Bucket in den Amazon-Redshift-Zielcluster zu laden.	DBA

Überprüfen der Daten in den Quell- und Zielregionen nach der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und vergleichen Sie die Anzahl der Zeilen in den Quell- und Zieltabellen.	Überprüfen und vergleichen Sie die Anzahl der Tabellenzeilen in den Quell- und Zielregionen, um sicherzustellen, dass alle migriert werden.	DBA
Überprüfen und vergleichen Sie die Anzahl der Quell- und Zieldatenbankobjekte.	Überprüfen und vergleichen Sie alle Datenbankobjekte in den Quell- und Zielregionen,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um sicherzustellen, dass alle migriert werden.	
Überprüfen und vergleichen Sie die SQL-Skriptergebnisse in den Quell- und Zielregionen.	Führen Sie die SQL-Skript aus, die vor der Migration vorbereitet wurden. Überprüfen und vergleichen Sie die Daten, um sicherzustellen, dass die SQL-Ergebnisse korrekt sind.	DBA
Setzen Sie die Passwörter aller Benutzer im Amazon-Redshift-Ziel-Cluster zurück.	Nachdem die Migration abgeschlossen und alle Daten verifiziert wurden, sollten Sie alle Benutzerpasswörter für den Amazon Redshift-Cluster in der AWS-Region in China zurücksetzen.	DBA

Zugehörige Ressourcen

- Übertragen von Amazon S3-Daten aus AWS-Regionen in AWS-Regionen in China
- Erstellen eines S3-Buckets
- Zurücksetzen eines Amazon-Redshift-Benutzerpassworts
- psql-Dokumentation

Zusätzliche Informationen

IAM-Richtlinie zum Entladen von Daten

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

IAM-Richtlinie zum Kopieren von Daten

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

SQL-Anweisungen zur Abfrage von Amazon Redshift

```
##Database

select * from pg_database where datdba>1;

##User

select * from pg_user where usesysid>1;

##Schema

SELECT n.nspname AS "Name",
```

```
  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"

FROM pg_catalog.pg_namespace n

WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'

ORDER BY 1;

##Table

select count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema');

select schemaname,count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema') group by schemaname order by 1;

##View

SELECT

    n.nspname AS schemaname,c.relname AS
 viewname,pg_catalog.pg_get_userbyid(c.relowner) as "Owner"

FROM

    pg_catalog.pg_class AS c

INNER JOIN

    pg_catalog.pg_namespace AS n

    ON c.relnamespace = n.oid

WHERE relkind = 'v' and n.nspname not in ('information_schema','pg_catalog');

##UDF

SELECT

   n.nspname AS schemaname,

   p.proname AS proname,

   pg_catalog.pg_get_userbyid(p.proowner) as "Owner"
```

```
FROM pg_proc p

LEFT JOIN pg_namespace n on n.oid = p.pronamespace

WHERE p.proowner != 1;
```

SQL-Skripte zum Generieren von DDL-Anweisungen

- Get_schema_priv_by_user-Skript
- Generate_tbl_ddl-Skript
- Generate_view_ddl
- Generate_user_grant_revoke_ddl
- Generate_udf_ddl

Migrieren Sie Workloads mithilfe von VMware HCX zur VMware Cloud on AWS

Erstellt von Deepak Kumar (AWS), Derek Cox (AWS) und Himanshu Gupta (AWS)

Umgebung: Produktion	Quelle: Lokale VMware-Workloads	Ziel: VMware Cloud on AWS
R-Typ: Umziehen	Arbeitslast: Alle anderen Workloads	Technologien: Migration; Hybrid-Cloud
AWS-Dienste: VMware Cloud auf AWS; Amazon VPC		

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster erklärt, wie Sie VMware Hybrid Cloud Extension (HCX) verwenden können, um Workloads von Ihrer lokalen VMware-Umgebung zu VMware Cloud on AWS zu migrieren, ohne die zugrunde liegende Plattform zu ändern. VMware HCX optimiert die Migration, hilft beim Ausgleich von Workloads, schützt Daten und optimiert Disaster Recovery-Prozesse sowohl für lokale Rechenzentren als auch für Cloud-Server. Das Muster beschreibt die Schritte zur Installation, Konfiguration, Aktualisierung und Deinstallation von HCX.

HCX unterstützt Folgendes:

- Ältere Versionen von VMware vSphere — HCX unterstützt Sie bei der Migration virtueller Maschinen (VMs) von älteren Versionen von vSphere zu VMware Cloud on AWS. Die Hosts werden automatisch aktualisiert und repariert, sodass zeitaufwändige Updates zur Vorbereitung der Migration entfallen.

- Massenmigrationen — Sie können HCX mit einem WAN-Optimierungsservice verwenden, um eine große Anzahl von VMs in einem Schritt ohne Ausfallzeiten zu migrieren und Ihre lokalen Netzwerke auf die Cloud auszudehnen.
- Heterogene Netzwerkumgebungen — Ihr aktuelles Netzwerk (wie vSphere, NSX, VXLAN oder NSX-T) bestimmt die Komplexität Ihrer Migration. HCX extrahiert die Grundlagen Ihrer Netzwerkanwendung und erweitert Ihr aktuelles Netzwerk auf die Cloud, ohne dass komplizierte Verfahren erforderlich sind.
- Langsame Netzwerkgeschwindigkeiten — Migrationen erfordern im Allgemeinen Verbindungsgeschwindigkeiten von über 250 Mbit/s. HCX kann Ihre Workloads mit viel niedrigeren Geschwindigkeiten migrieren, etwa 100 Mbit/s.

HCX unterstützt drei Arten von Cloud-Migrationen:

- Hybridität (Rechenzentrumserweiterung) — Erweiterung eines bestehenden, lokalen VMware-Software-Defined Data Centers (SDDC) auf AWS, um eine Erweiterung des Platzbedarfs, On-Demand-Kapazität, eine Test-/Entwicklungsumgebung und virtuelle Desktops bereitzustellen.
- Cloud-Evakuierung (Aktualisierung der Infrastruktur im gesamten Rechenzentrum) — Konsolidierung von Rechenzentren und vollständige Umstellung auf die AWS-Cloud (einschließlich der Verwaltung der Rechenzentrumszusammenlegung oder der Beendigung des Leasingvertrags).
- Anwendungsspezifische Migration — Verschieben einzelner Anwendungen in die AWS-Cloud, um spezifische Geschäftsanforderungen zu erfüllen.

Sie können HCX verwenden, um Workloads bidirektional zwischen Ihrer lokalen Umgebung und VMware Cloud on AWS zu migrieren. HCX bietet mehrere Möglichkeiten, Ihre Workloads zwischen Quell- und Zielstandorten zu migrieren:

- HCX Cold-Migration migriert virtuelle Maschinen, die offline sind. Diese Methode eignet sich für ausgeschaltete VMs, da sie erhebliche Ausfallzeiten erfordert.
- HCX vMotion verwendet das VMware vMotion-Protokoll, um VMs zu verschieben. HCX vMotion bietet eine Migration ohne Ausfallzeiten, kann jedoch jeweils nur eine VM migrieren.
- HCX Bulk Migration verwendet VMware vSphere-Replikationsprotokolle, um VMs an das Ziel zu verschieben. Sie können mehrere VMs parallel migrieren und einen Switchover planen. Die Ausfallzeit entspricht einem Serverneustart, und der Switchover für alle VMs erfolgt parallel.
- HCX Replication Assisted vMotion (RAV) ist eine Kombination aus HCX Bulk Migration und HCX vMotion. Es bietet parallel Migrationen, Zeitplanung und keine Ausfallzeiten.

- HCX OS Assisted Migration hilft Ihnen, mehrere VMs gleichzeitig zu migrieren, wenn Sie mehrere Hypervisoren und Nicht-vSphere-VMs vor Ort verwenden. HCX OS Assisted Migration ist kostenlos, wenn Sie es für die Migration von lokal zu VMware Cloud on AWS verwenden, erfordert jedoch zusätzliche Lizenzen, wenn Sie zwischen zwei lokalen Umgebungen oder von lokalen Umgebungen zu anderen Cloud-Anbietern migrieren möchten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein VMware-Konto für den Zugriff auf die VMware-Konsole unter vmware.com.
  - Die folgenden Firewall-Ports sind für HCX erforderlich.

Quelle	Ziel	Port
HCX Manager und IP-Appliances vor Ort	HCX Manager und Appliances IP auf VMware Cloud on AWS	UDP 500, UDP 4500 und ICMP
HCX Manager und IP-Appliances vor Ort	connect.hcx.vmware.com | hybridity-depot.vmware.com	TCP 443
HCX Manager und IP-Appliances vor Ort	HCX-Cloud-URL	TCP 443

Wenn das lokale Netzwerk über interne Firewalls verfügt, müssen Sie einige weitere Ports lokal im Rechenzentrum zulassen. Eine vollständige Liste der Portanforderungen für HCX finden Sie in der VMware HCX-Dokumentation.

- Um HCX zu konfigurieren, benötigen Sie die DNS-IP (Domain Name System), den vollqualifizierten vCenter-Domänennamen (FQDN), den NTP-Server-FQDN, den Single Sign-On-Benutzer (SSO) und ähnliche Informationen. Erfassen Sie diese Informationen im Voraus, um Verzögerungen bei der Bereitstellung zu vermeiden.

Einschränkungen

Sie können die Network Extension Appliance verwenden, um maximal acht Netzwerke zwischen der lokalen Umgebung und VMware Cloud on AWS zu erweitern. Eine vollständige Liste der HCX-Servicebeschränkungen finden Sie in der VMware HCX-Dokumentation.

Architektur

Quelltechnologie-Stack

- Lokale VMware-Workloads

Zieltechnologie-Stack

- VMware Cloud in AWS

Tools

Tools

- VMware Cloud on AWS ist ein Service, der gemeinsam von AWS und VMware entwickelt wurde, um Sie bei der Migration und Erweiterung Ihrer lokalen VMware vSphere-basierten Umgebungen in die AWS-Cloud zu unterstützen.
- VMware Hybrid Cloud Extension (HCX) ist ein VMware-Hilfsprogramm für die Migration von Workloads aus Ihrer lokalen VMware-Umgebung zu VMware Cloud on AWS, ohne die zugrunde liegende Plattform zu ändern.

Epen

Stellen Sie HCX bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
HCX-Service in VMware Cloud on AWS aktivieren	1. Melden Sie sich bei der VMware Cloud on AWS AWS-Konsole an. 2. Navigieren Sie zu Ihrem SDCC und wählen Sie Details anzeigen aus.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie den Tab Add Ons. 4. Wählen Sie HCX öffnen. 5. Wählen Sie Deploy HCX und bestätigen Sie. Die HCX-Bereitstellung wird beginnen.	
Generieren Sie den HCX-Aktivierungsschlüssel.	1. Auf der VMware Cloud on AWS AWS-Konsole. 2. Navigieren Sie zu Ihrem SDCC und wählen Sie Details anzeigen aus. 3. Wählen Sie den Tab Add Ons. 4. Wählen Sie „HCX öffnen“ und anschließend „Aktivierungsschlüssel“. 5. Wählen Sie Aktivierungsschlüssel erstellen und kopieren Sie den Schlüssel.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Firewallregeln für HCX auf dem Cloud-SDDC hinzu.	Nach der Bereitstellung des HCX Managers müssen Sie Firewallregeln konfiguri eren, um die Kommunika tion zwischen der lokalen Umgebung und dem SDDC zu ermöglichen. Sie müssen zwei Firewallregeln erstellen: eine für eingehende und eine für ausgehende Kommunikation. 1. Wählen Sie auf der VMware Cloud on AWS AWS-Konsole Ihr SDDC aus und navigieren Sie zu Networkin g & Security. 2. Wählen Sie Gateway Firewall und dann die Registerkarte Management Gateway aus. 3. Wählen Sie Regel hinzufügen und erstellen Sie eine ausgehende Regel: a. Geben Sie den Namen der Regel ein. b. Bearbeiten Sie die Quelle und wählen Sie HCX aus. c. Bearbeiten Sie das Ziel und geben Sie die lokale IP und das Subnetz an, über das auf HCX zugegriffen werden kann.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	d. Wählen Sie für Dienste die Option Any aus. e. Wählen Sie für Aktion die Option Zulassen aus. f. Wählen Sie Publish. 4. Wählen Sie Regel hinzufügen und erstellen Sie eine Regel für eingehenden Datenverkehr: a. Geben Sie den Namen der Regel ein. b. Bearbeiten Sie die Quelle und geben Sie die lokale IP und das Subnetz an, über das auf HCX zugegriffen werden kann. c. Bearbeiten Sie das Ziel und wählen Sie HCX aus. d. Wählen Sie für Dienste SSH, HTTPS, TCP (9443) und ICMP aus. e. Wählen Sie für Aktion die Option Allow aus. f. Wählen Sie Publish.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie HCX Manager vor Ort.	1. Melden Sie sich beim Cloud-vCenter an und navigieren Sie im Menü zu HCX. 2. Wählen Sie im HCX-Dashboard Administration, Systemupdates aus. 3. Fordern Sie den Download-Link für VMware HCX Connector an und laden Sie die lokale OVA-Datei herunter. 4. Melden Sie sich bei Ihrem lokalen vCenter an und stellen Sie die OVF-Vorla ge mithilfe der herunterg eladenen OVA-Datei bereit. 5. Geben Sie bei der Bereitste llung der Vorlage statische IP-, NTP-, DNS-, DNS-Suchlisten und andere Details an, wenn Sie dazu aufgefordert werden. 6. Überprüfen Sie alle Details, um die HCX Manager-B ereitstellung abzuschließen.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie HCX Manager vor Ort.	1. Öffnen Sie HCX Manager in einem Browser:. `https://<HCX_Manager_IP>:9433` 2. Melden Sie sich mit dem Benutzernamen und dem Passwort an, die Sie bei der Bereitstellung angegeben haben. 3. Geben Sie den zuvor erstellten Aktivierungsschlüssel ein und wählen Sie Aktivieren, um Ihre HCX-Instanz zu aktivieren. 4. Wählen Sie Bestätigen, um mit dem nächsten Schritt fortzufahren. 5. Wählen Sie den Standort Ihres lokalen Rechenzentrums und dann Weiter aus. 6. Geben Sie als Systemname den Hostnamen ein und wählen Sie dann Weiter, um die Aktivierung abzuschließen. 7. Geben Sie die Informationen ein, um Ihre vCenter-Verbindung zu konfigurieren. 8. Geben Sie die Informationen zur Konfiguration der SSO/PSC-Details ein.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Neu starten, damit Ihre Änderungen wirksam werden.	
Konfigurieren Sie die Site-Kopplung.	Nachdem Sie HCX in der Cloud und vor Ort konfiguriert haben, gehen Sie wie folgt vor, um das Site-Pairing zwischen beiden zu konfigurieren. 1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie im linken Navigationsbereich Site Pairing und dann Connect to Remote Site aus. 3. Fügen Sie im Dialogfeld Mit Remote-Site verbinden die HCX-Cloud-URL und die Anmeldeinformationen hinzu, und wählen Sie dann Connect aus. Wenn die Site-Kopplung abgeschlossen ist, zeigt das Site-Pairing-Dashboard das verbundene lokale und das Cloud-SDDC an.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Netzwerkprofil.	Ein Netzwerkprofil ist eine Abstraktion der Layer-3-Komponenten eines Netzwerks. Dieses Profil ist eine Voraussetzung für die Erstellung eines Rechenprofils. 1. Melden Sie sich bei Ihrem Cloud-vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie Interconnect, wählen Sie die Registerkarte Netzwerkprofile und dann Netzwerkprofil erstellen aus. 3. Konfigurieren Sie das Netzwerkprofil: a. Wählen Sie den vCenter Server aus. b. Wählen Sie das Netzwerk aus. c. Fügen Sie einen Namen für das Profil hinzu. d. Geben Sie den IP-Pool, die Präfixlänge, das Gateway, den DND und die MTU an. e. Wählen Sie Erstellen. 4. Gehen Sie genauso vor, um ein Netzwerkprofil vor Ort zu erstellen.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Rechenprofil.	Das Rechenprofil besteht aus Netzwerk-, Speicher- und Rechendetails für HCX. HCX verwendet diese Einstellungen, wenn es HCX-Appliances während der Erstellung des Service Mesh erstellt. 1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie Interconnect, klicken Sie auf die Registerkarte Computing-Profile und dann auf Computing-Profil erstellen. 3. Geben Sie einen Namen für das Rechenprofil an. 4. Wählen Sie die HCX-Dienste aus, die Sie aktivieren möchten, und klicken Sie dann auf Weiter. 5. Wählen Sie die Serviceressourcen aus. Wenn es mehrere Cluster gibt, wählen Sie jeden Cluster aus, für den HCX-Dienste aktiviert werden sollen, und klicken Sie dann auf Weiter. 6. Wählen Sie Rechen- und Speicherressourcen für die Bereitstellung von HCX-	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Appliances aus und klicken Sie dann auf Weiter. 7. Wählen Sie ein Verwaltungsnetzwerkprofil aus, mit dem Sie auf die Verwaltungsschnittstelle von vCenter- und ESXi-Hosts zugreifen können, und wählen Sie dann Weiter aus. 8. Wählen Sie ein Uplink-Netzwerkprofil aus, das verwendet werden kann, um Interconnect-Appliances auf der Remote-Site zu erreichen, und über das Appliances am Remotestandort die lokalen Interconnect-Appliances erreichen können, und wählen Sie dann Weiter. 9. Wählen Sie das vMotion-Netzwerkprofil und dann Weiter aus. 10. Wählen Sie das vSphere Replication-Netzwerkprofil und dann Weiter aus. 11. Wählen Sie den entsprechenden Distributed Switch für Netzwerkerweiterungen aus und klicken Sie dann auf Weiter. 12. Überprüfen Sie alle Ports, die für WAN- und LAN-Verbindungen geöffnet	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden müssen, und wählen Sie dann Weiter. 13. Um das Rechenprofil zu erstellen, wählen Sie Fertig stellen. 14. Gehen Sie genauso vor, um ein Rechenprofil auf der Cloud-Site zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Service Meshs	Das Service Mesh bietet die HCX-Servicekonfiguration sowohl für die lokale Site als auch für die Cloud-Site. Durch die Erstellung eines Service Mesh wird die Bereitstellung von virtuellen HCX Interconnect-Appliances an beiden Standorten initiiert. Der Interconnect-Dienst muss auf der Quell-Site erstellt werden. 1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie Interconnect, wählen Sie die Registerkarte Service Mesh und dann Create Service Mesh aus. 3. Wählen Sie den Quell- und Zielstandort aus, zwischen dem das Service Mesh erstellt werden soll, und klicken Sie dann auf Weiter. 4. Wählen Sie das Computing-Profil für die Quell- und Ziel-Sites aus, das Sie zuvor erstellt haben, und klicken Sie dann auf Weiter. 5. Wählen Sie den HCX-Dienst aus, den Sie aktivieren	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten, und klicken Sie dann auf Weiter. 6. Wählen Sie das Uplink-Pr ofil sowohl für die Quell- als auch für die Zielsite aus, und klicken Sie dann auf Weiter. 7. Überprüfen Sie die Ressourcen und Netzwerke und wählen Sie dann Weiter aus. 8. Geben Sie einen Namen für das Service Mesh ein, und klicken Sie dann auf Fertig stellen. Die Bereitstellung von Service Mesh wird gestartet. Sie können den Fortschritt auf der Registerkarte Aufgaben für das Service Mesh verfolgen . Wenn die Bereitstellung abgeschlossen ist, wird der Status aller HCX-Services angezeigt, die Sie für das Service Mesh aktiviert haben.	

Erweitern Sie das Netzwerk mithilfe von HCX

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Netzwerke rweiterung.	Sie können die HCX-Netzw erkerweiterungsfunktionen	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, um eine L2-Netzwerkerweiterung am Cloud-SDDC-HCX-Standort zu erstellen und die Remote- und Quellnetzwerke miteinander zu verbinden. Auf diese Weise können Sie Server von lokalen Servern zu VMware Cloud on AWS migrieren und dabei dieselben IP-Adressen beibehalten. 1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie Dienste, Netzwerkerweiterung aus. 3. Wählen Sie Netzwerke erweitern oder Netzwerke rweiterung erstellen. 4. Wählen Sie das entsprech ende Service Mesh, die verteilte Portgruppe oder den logischen NSX-Switch aus. 5. Geben Sie die Gateway-IP-Adresse ein und wählen Sie dann Submit. Wenn die Netzwerkerweiterun g abgeschlossen ist, zeigt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das System die Erweiterung abgeschlossen an.	

Konfigurieren Sie einen Replikationsjob mithilfe von HCX

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Replikation.	So replizieren Sie virtuelle Maschinen mithilfe von HCX: 1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie Migration und dann die Registerkarte Migrieren aus. 3. Geben Sie einen Namen für die Mobilitätsgruppe ein, wählen Sie die VM aus, die Sie migrieren möchten, und klicken Sie dann auf Hinzufügen. 4. Wählen Sie den Ziel-Computing-Container, den Speicherordner, den Migrationstyp (Cold, Bulk, RAV, vMotion) und den Switchover-Zeitplan aus. 5. Wählen Sie Validieren aus, warten Sie, bis die Validierung abgeschlossen ist, und	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Go, um die Replizierung zu starten.	

HCX aktualisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lesen Sie die Empfehlungen und Schritte.	Ein großes Migrationsprojekt kann sechs bis acht Monate dauern, manchmal auch länger. VMware veröffentlicht regelmäßig HCX-Updates, die aus Softwarekorrekture n, Sicherheitsupdates und Bugfixes bestehen. Wir empfehlen Ihnen, HCX und Ihre Appliances auf dem neuesten Stand zu halten, um Sicherheitslücken zu schließen und neue Funktione n zu nutzen. Hinweis: Wenn Ihre aktuelle HCX-Version drei Versionen hinter der neuesten Version oder älter liegt, können Sie HCX nicht aktualisieren und müssen sie erneut bereitste llen. Ein HCX-Upgrade besteht aus drei Schritten: 1. Sichern Sie HCX Manager vor Ort und in der Cloud.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Führen Sie ein Upgrade von HCX Manager vor Ort und in der Cloud durch. 3. Aktualisieren Sie Service Mesh-Appliances vor Ort und in der Cloud. In den folgenden Geschichten werden diese Schritte ausführlicher beschrieben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sichern Sie HCX Cloud Manager.	HCX Cloud Manager for VMware Cloud on AWS wird von VMware verwaltet, sodass Sie keine Snapshots erstellen können. Um HCX Cloud Manager zu sichern, müssen Sie ein Backup von der HCX-Konsole herunterladen und dieses Backup verwenden , um die HCX-Konfiguration wiederherzustellen, falls das Upgrade fehlschlägt oder Sie zu einer vorherigen Phase zurückkehren müssen. 1. Melden Sie sich bei HCX Cloud Manager an unter. `https://<HCX_cloud manager_ip_or_fqdn >:9433` 2. Navigieren Sie zu Administr ation, Problembehandlung, Backup & Restore. 3. Wählen Sie im Abschnitt Backup die Option Generieren, um eine Sicherungsdatei zu erstellen. 4. Wählen Sie Herunterladen, um die Sicherungsdatei zu speichern. HCX-Service-Appliances wie HCX-IX, HCX-NE und HCX-	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	WO benötigen keine individue llen Backups.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sichern Sie HCX Manager vor Ort.	Sie können HCX Manager lokal auf zwei Arten sichern: indem Sie einen VM-Snapsh ot erstellen oder indem Sie die Konfigurationsdatei sichern. Um einen VM-Snapshot zu erstellen: 1. Melden Sie sich bei Ihrem lokalen vCenter an. 2. Gehen Sie zu VM und Vorlagen und navigieren Sie zu HCX Manager VM. 3. Wählen Sie Aktionen, Snapshots, Snapshot erstellen aus. Um die Konfigurationsdatei zu sichern: 1. Melden Sie sich bei HCX Cloud Manager an unter`https://<HCX_cloudmanager_ip_or_fqdn>:9433` . 2. Navigieren Sie zu Administr ation, Problembehandlung, Backup & Restore. 3. Wählen Sie im Abschnitt Backup die Option Generieren, um eine Sicherungsdatei zu erstellen.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Herunterladen, um die Sicherungsdatei zu speichern. HCX-Service-Appliances wie HCX-IX, HCX-NE und HCX-WO benötigen keine individuellen Backups.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie ein Upgrade von HCX Manager vor Ort und in der Cloud durch.	Sie müssen zuerst HCX Manager lokal und dann HCX Cloud Manager aktualisieren. Um HCX Manager vor Ort zu aktualisieren: 1. Melden Sie sich bei vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie System, Administration. 3. Wählen Sie auf der Verwaltungsseite die Registerkarte Systemupdates aus. In der Spalte Verfügbare Service-Update-Versionen werden ausstehende Updates angezeigt. 4. Wählen Sie Service-Update auswählen, Herunterladen, um das Update für ein späteres Upgrade herunterzuladen, oder wählen Sie Herunterladen und Upgrade, um das Update sofort herunterzuladen und bereitzustellen. Wenn Sie Herunterladen ausgewählt haben, wählen Sie Upgrade und bestätigen Sie, um das Upgrade zu	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	starten, wenn Sie bereit sind. 5. Wenn das Upgrade abgeschlossen ist: • Überprüfen Sie auf der HCX Manager-Administrationsseite, ob die neueste HCX-Version angezeigt wird. • Vergewissern Sie sich im HCX-Dashboard, dass die Site-Kopplung aktiviert ist. • Wählen Sie Infrastruktur, Service Mesh und vergewissern Sie sich, dass alle HCX-Dienste fehlerfrei sind. Folgen Sie den gleichen Schritten, um HCX Cloud Manager zu aktualisieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Service Mesh-Appliances.	Das Service Mesh wird unabhängig von HCX Manager am Quellstandort aktualisiert. Service Mesh-Appliances auf der Ziel-Site werden automatisch aktualisiert. Um Service Mesh-Appliances am Quellstandort zu aktualisieren: 1. Melden Sie sich bei vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie Infrastruktur und dann die Registerkarte Service Mesh aus. 3. Wenn Sie das Banner „Neue Version für Service Mesh-Appliances ist verfügbar“ sehen. Klicken Sie auf „Geräte aktualisieren, um auf die neueste Version zu aktualisieren“ und wählen Sie „Appliances aktualisieren“. 4. Wählen Sie im Dialogfeld, in dem Appliances angezeigt werden, eine oder mehrere Appliances aus und klicken Sie dann auf OK, um den Upgrade-Vorgang zu starten. (Wir empfehlen,	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dass Sie alle Service Mesh-Appliances aktualisieren.) 5. Wählen Sie Aufgaben für jedes Service Mesh anzeigen, um das Upgrade zu überwachen. 6. Wenn das Upgrade abgeschlossen ist, wird für jede Appliance und jeden Service ein Banner angezeigt, das den erfolgreichen Abschluss bestätigt. 7. Überprüfen Sie den Tunnelstatus nach dem Upgrade: • Wählen Sie Infrastruktur, Service Mesh, Appliance anzeigen. • In der Spalte mit dem Tunnelstatus sollte Up angezeigt werden und auf dem Bildschirm sollten keine anderen verfügbaren Versionen für die Appliance angezeigt werden.	

Entfernen Sie HCX-Netzwerkerweiterungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Netzwerk nicht erweitern.	In einem früheren Schritt wurde erklärt, wie die HCX-	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Netzwerkerweiterungsfunktionen verwendet werden können, um L2-Netzwerkerweiterungen zu erstellen und bestehende IPs während der Migration von lokal zur VMware-Cloud auf AWS beizubehalten. Wenn alle VMs aus einem bestimmten VLAN zu VMware Cloud on AWS verschoben wurden, müssen Sie die Erweiterung des Netzwerks zwischen dem lokalen Standort und dem Cloud-SDDC aufheben und das Netzwerk im SDDC routingfähig machen. Wir empfehlen, dass Sie das erweiterte Netzwerk entfernen, sobald alle VMs von lokal auf VMware Cloud on AWS migriert wurden, um Latenzen zu vermeiden. 1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zum HCX-Dashboard. 2. Wählen Sie im HCX-Dashboard Dienste, Netzwerkerweiterung aus. 3. Wählen Sie das Netzwerk aus, dessen Erweiterung Sie rückgängig machen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten, und wählen Sie dann Netzwerk aufheben. 4. Wählen Sie Cloud-Netzwerk mit Cloud Edge-Gateway verbinden, nachdem Sie die Erweiterung aufgehoben haben. Dadurch wird das Netzwerk auf der Cloud-Seite aktiviert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Das verschobene Netzwerk im Cloud-SDDC weiterleiten.	1. Melden Sie sich beim VMC-Portal an. 2. Navigieren Sie zum SDCC und wählen Sie dann Details anzeigen aus. 3. Wählen Sie die Registerk arte Netzwerk und Sicherheit. 4. Gehen Sie auf der Seite Netzwerk und Sicherheit wie folgt vor: • Wählen Sie Netzwerk, Segmente und vergewiss ern Sie sich, dass das Subnetz, das kürzlich nicht erweitert wurde, als routingfähig angezeigt wird. • Wählen Sie Inventar und Gruppen aus und fügen Sie das Subnetz einer Gruppe hinzu. • Wählen Sie Sicherhei t, Verteilte Firewall und vergewissern Sie sich, dass die Gruppe Teil der gewünschten Firewallr egel ist.	Cloud-Administrator, Systemadministrator

Deinstallieren Sie HCX

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Vorausset zungen.	Im Falle eines Ausstiegs des Rechenzentrums empfehlen wir, HCX zu deinstallieren und die zugehörigen Komponent en am Ende Ihres Migration sprojekts zu entfernen. Wenn Sie jedoch weiterhin lokal arbeiten, möchten Sie HCX möglicherweise weiter ausführen. Stellen Sie vor der Deinstall ation von HCX sicher, dass: • Es gibt keine aktiven Migrationen. • Alle Netzwerkerweiterungen wurden entfernt.	Cloud-Administrator, Systemadministrator
Deinstallieren Sie HCX vor Ort.	1. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zur HCX-Konsole. 2. Wählen Sie Dienste, Migration und vergewiss ern Sie sich, dass Sie keine aktiven Migrationen haben. 3. Wählen Sie Dienste, Netzwerkerweiterung und vergewissern Sie sich, dass kein erweitertes Netzwerk vorhanden ist.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Infrastruktur, Site-Pairing, Service Mesh aus. 5. Identifizieren Sie das Service Mesh und wählen Sie dann Löschen. 6. Wählen Sie in der Bestätigungsaufforderung erneut Löschen aus. Das Banner „Service Mesh entfernen“ erscheint auf dem Service Mesh-Bildschirm. 7. Wiederholen Sie die Schritte 5 bis 6 für alle anderen Service Meshes, die Sie haben. 8. Um die Standortkopplung zu entfernen, wählen Sie Infrastruktur, Standortkopplung und trennen Sie dann die Verbindung aller gekoppelten Standorte. 9. Entfernen Sie die HCX Manager-Appliance: a. Melden Sie sich bei Ihrem lokalen vCenter an und navigieren Sie zur HCX Manager-Appliance. b. Wählen Sie Aktionen, Einschalten, Ausschalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Wählen Sie „Aktionen“, „Von Festplatte löschen“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Heben Sie die Registrierung des HCX-Plug-ins vom lokalen vCenter Server auf.	1. Melden Sie sich bei der vCenter MOB-Benut zeroberfläche unter an. `https://<vc_fqdn>/mob` 2. Wählen Sie im Abschnitt Eigenschaften den Inhalt in der Spalte Wert aus. 3. Wählen Sie auf der Inhaltsseite aus, ob ExtensionManageralle registrierten Plugins angezeigt werden sollen. 4. Beachten Sie die Erweiterungen, die mit `com.vmware.hybridity com.vmware.hcsp.alarm` , und beginnen`com.vmware.vca.marketing.ngc.ui` . 5. Entfernen Sie die Erweiterungen: • Wählen Sie im Abschnitt Methoden die Option UnregisterExtension. • Geben Sie den in Schritt 4 angegebenen Erweiterungsschlüssel ein, und wählen Sie dann Invoke Method, um die Erweiterung zu entfernen.	Cloud-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn alle Erweiterungen entfernt wurden, verschwindet das HCX-Plug-In aus dem vSphere Web Client.	
Deinstallieren Sie HCX in der Cloud.	Um das HCX-Service Mesh und die Site-Kopplung in der Cloud zu entfernen, wiederholen Sie die zuvor unter HCX vor Ort deinstallieren beschriebenen Schritte. In VMware Cloud on AWS wird HCX Manager von VMware verwaltet. Sie können es nicht aus vCenter löschen, aber Sie können die Bereitstellung über die VMC-Verwaltungsschnittstelle aufheben. Um die Bereitstellung von HCX Manager aufzuheben: 1. Melden Sie sich bei der VMC-Verwaltungsschnittstelle an. 2. Wählen Sie Ihre Organisation und Ihr SDDC aus. 3. Wählen Sie Add Ons, um alle SDDCs anzuzeigen, auf denen HCX bereitgestellt wurde. 4. Wählen Sie Undeploy HCX aus.	Cloud-Administrator, Systemadministrator

Fehlerbehebung

Problem	Lösung
Sie können die zu migrierenden Server nicht auswählen, wenn Sie die HCX-Massenmigration konfigurieren.	Ursache: Die Migration für diese Server wurde abgebrochen, aber die HCX-Datenbank wurde während der Bereinigung nicht aktualisiert. HCX betrachtet die Datenbankmigration als noch im Gange und hat daher den Status „Switchover läuft“ gesperrt. Lösung: Wenden Sie sich an das VMware-Support-Team, um die HCX-Datenbank zu bereinigen.
Switchover schlägt fehl, funktioniert aber mit der Option Force Power Off.	Ursache: Die Version von VMware Tools erfüllte nicht die Voraussetzungen für die HCX-Massenmigration, sodass HCX die Quell-VM nicht herunterfahren konnte. Lösung: Aktualisieren Sie das VMware-Tool auf die empfohlene Version für Ihren Migrationstyp.
Das Upgrade der HCX-Site-Pairing-Appliance schlägt mit dem Fehler „Operation not allowed for ongoing bulk migration“ fehl, während die Migration läuft.	Ursache: Die HCX-Datenbank wurde nach dem Switchover nicht aktualisiert. Lösung: Stellen Sie sicher, dass keine laufenden Migrationen stattfinden. Wählen Sie beim Upgrade der Site Pairing-Appliance die Option Upgrade erzwingen aus.
Die Umstellung schlägt mit dem Fehler „Niedrige Ressourcenverfügbarkeit“ fehl.	Ursache: Wenig Speicherplatz auf der Host-VM. Lösung: Überprüfen Sie vor der Migration die Speicher- und Rechenressourcen.

Zugehörige Ressourcen

Referenzen

- Funktionen von VMware Cloud on AWS
- Überblick und Betriebsmodell von VMware Cloud on AWS (AWS Prescriptive Guidance)
- Migrieren Sie VMware SDDC mithilfe von VMware HCX zu VMware Cloud on AWS (AWS Prescriptive Guidance)
- VMware HCX in der VMware Cloud on AWS (VMware-Dokumentation)
- HCX HCX-Versionshinweise (VMware-Dokumentation)
- SDDC-Bereitstellungs- und Best Practices-Leitfaden auf AWS (AWS-Whitepaper)

Tools

- Automatisierung von VMware Cloud on AWS mithilfe von PowerCLI (VMware Cloud Tech Zone)

Partner

- Partnerinitiative VMware Cloud on AWS

Videos

- VMware Cloud on AWS (YouTube Video)

Transportieren von PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport

Erstellt von Raunak Rishabh (AWS) und Jitender Kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS für PostgreSQL
R-Typ: Verschieben	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster beschreibt die Schritte zur Migration extrem großer Datenbanken zwischen zwei Amazon Relational Database Service (Amazon RDS) for PostgreSQL-DB-Instances mithilfe der Erweiterung pg_transport. Diese Erweiterung bietet einen physischen Transportmechanismus, um jede Datenbank zu verschieben. Durch das Streamen der Datenbankdateien mit minimaler Verarbeitung bietet sie eine extrem schnelle Methode für die Migration großer Datenbanken zwischen DB-Instances mit minimaler Ausfallzeit. Diese Erweiterung verwendet ein Pull-Modell, bei dem die Ziel-DB-Instance die Datenbank aus der Quell-DB-Instance importiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Beide DB-Instances müssen dieselbe Hauptversion von PostgreSQL ausführen.
- Die Datenbank darf nicht auf dem Ziel vorhanden sein. Andernfalls schlägt der Transport fehl.
- Andere Erweiterungen als pg_transport müssen in der Quelldatenbank aktiviert werden.
- Alle Quelldatenbankobjekte müssen sich im standardmäßigen Tabellenraum pg_default befinden.
- Die Sicherheitsgruppe der Quell-DB-Instance sollte Datenverkehr von der Ziel-DB-Instance zulassen.
- Installieren Sie einen PostgreSQL-Client wie psql oder , PgAdmin um mit der Amazon RDS PostgreSQL-DB-Instance zu arbeiten. Sie können den Client entweder in Ihrem lokalen System

installieren oder eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance verwenden. In diesem Muster verwenden wir psql auf einer EC2-Instance.

Einschränkungen

- Sie können keine Datenbanken zwischen verschiedenen Hauptversionen von Amazon RDS for PostgreSQL transportieren.
- Die Zugriffsrechte und der Besitz der Quelldatenbank werden nicht in die Zieldatenbank übertragen.
- Sie können keine Datenbanken auf Lesereplikaten oder auf übergeordneten Instances von Lesereplikaten transportieren.
- Sie können keine Reg-Datentypen in Datenbanktabellen verwenden, die Sie mit dieser Methode transportieren möchten.
- Sie können insgesamt bis zu 32 Transporte (einschließlich Importe und Exporte) gleichzeitig auf einer DB-Instance ausführen.
- Sie können Tabellen nicht umbenennen oder einschließen/ausschließen. Alles wird unverändert migriert.

Kabel

- Erstellen Sie Backups, bevor Sie die Erweiterung entfernen, da durch das Entfernen der Erweiterung auch abhängige Objekte und einige Daten entfernt werden, die für den Betrieb der Datenbank von entscheidender Bedeutung sind.
- Betrachten Sie die Instance-Klasse und Prozesse, die in anderen Datenbanken auf der Quell-Instance ausgeführt werden, wenn Sie die Anzahl der Worker und `work_mem` Werte für pg_transport ermitteln.
- Wenn der Transport gestartet wird, werden alle Verbindungen zur Quelldatenbank beendet und die Datenbank wird in den schreibgeschützten Modus versetzt.

Hinweis: Wenn der Transport auf einer Datenbank ausgeführt wird, hat dies keine Auswirkungen auf andere Datenbanken auf demselben Server.

Produktversionen

- Amazon RDS für PostgreSQL 10.10 und höher sowie Amazon RDS für PostgreSQL 11.5 und höher. Die neuesten Versionsinformationen finden Sie unter Transportieren von PostgreSQL-Datenbanken zwischen DB-Instances in der Amazon-RDS-Dokumentation.

Architektur

Tools

- pg_transport bietet einen physischen Transportmechanismus zum Verschieben jeder Datenbank. Durch das Streamen der Datenbankdateien mit minimaler Verarbeitung bewegt der physische Transport Daten viel schneller als herkömmliche Dump- und Ladeprozesse und erfordert minimale Ausfallzeiten. PostgreSQL-Transportdatenbanken verwenden ein Pull-Modell, bei dem die Ziel-DB-Instance die Datenbank aus der Quell-DB-Instance importiert. Sie installieren diese Erweiterung auf Ihren DB-Instances, wenn Sie die Quell- und Zielumgebungen vorbereiten, wie in diesem Muster beschrieben.
- Mit psql können Sie eine Verbindung zu Ihren PostgreSQL-DB-Instances herstellen und damit arbeiten. Informationen zum Installieren von psql auf Ihrem System finden Sie auf der Seite PostgreSQL-Downloads.

Polen

Erstellen der Zielparametergruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Parameter gruppe für das Zielsystem.	Geben Sie einen Gruppenna men an, der ihn als Zielparam etergruppe identifiziert, z. B. `pgtarget-param-group` . Anweisungen finden Sie in der Amazon-RDS-Dokumentation.	DBA
Ändern Sie die Parameter für die Parametergruppe.	Legen Sie die folgenden Parameter fest:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Fügen Sie `pg_transport` dem `shared_preload_libraries` Parameter hinzu. `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Legen Sie den Parameter `pg_transport.num_workers` fest. Wählen Sie die Anzahl der Worker aus, mit denen Sie den Transport ausführen möchten. Der von Ihnen festgelegte Wert bestimmt die Anzahl der `transport.send_file` Worker, die in der Quelle erstellt werden. 3. Erhöhen Sie den Wert von `max_worker_processes` auf mehr als das Dreifache des Werts von `pg_transport.num_workers` . Wenn Sie beispielsweise den Wert von `pg_transport.num_workers` auf 4 setzen, sollte der `max_worker_processes` Wert mindestens 13 betragen. Wenn dies	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	fehlschlägt, empfiehlt pg_transport einen Mindestwert. 4. Setzen Sie `pg_transport.timing` auf 1. Diese Einstellung ermöglicht die Meldung von Zeitinformationen während des Transports. 5. Legen Sie den Parameter `pg_transport.work_mem` fest. Dieser Parameter gibt den maximalen Arbeitsspeicher an, der jedem Worker zugewiesen werden soll. Der Standardwert lautet 128 MB. Weitere Informationen zu diesen Parametern finden Sie in der Amazon-RDS-Dokumentation.	

Erstellen der Quellparametergruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Parametergruppe für das Quellsystem.	Geben Sie einen Gruppennamen an, der ihn als Quellparametergruppe identifiziert, z. B. `pgsource-param-group` .	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie in der Amazon-RDS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Parameter für die Parametergruppe.	Legen Sie die folgenden Parameter fest: 1. Fügen Sie `pg_transport` dem `shared_preload_libraries` Parameter hinzu. `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Legen Sie den Parameter `pg_transport.num_workers` fest. Der Wert dieses im Ziel definierten Parameters bestimmt die Anzahl der zu verwendenden `transport.send_file` Worker. Wenn auf dieser Instance ein Import ausgeführt wird, erhöhen Sie diesen Wert, berücksichtigen Sie jedoch die Anzahl der Worker, die bereits ausgeführt werden. 3. Erhöhen Sie den Wert von `max_worker_processes` auf mehr als das Dreifache des Werts von `pg_transport.num_workers` auf dem Ziel. Wenn Sie beispielsweise den Wert für das	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ziel auf `pg_transport.num_workers` 4 setzen, sollte der `max_worker_processes` Wert für die Quelle mindestens 13 betragen. Wenn dies fehlschlägt, empfiehlt pg_transport einen Mindestwert. 4. Legen Sie den Parameter `pg_transport.work_mem` fest. Dieser Parameter gibt den maximalen Arbeitsspeicher an, der jedem Worker zugewiesen werden soll. Der Standardwert lautet 128 MB. Weitere Informationen zu diesen Parametern finden Sie in der Amazon-RDS-Dokumentation.	

Vorbereiten der Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue DB-Instance von Amazon RDS für PostgreSQL, in die Ihre Quelldatenbank transportiert werden soll.	Bestimmen Sie die Instance-Klasse und die PostgreSQL-Version basierend auf Ihren Geschäftsanforderungen.	DBA, Systemadministrator, Datenbankarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Sicherheitsgruppe des Ziels, um Verbindungen am Port der DB-Instance von der EC2-Instance aus zuzulassen.	Standardmäßig ist der Port für die PostgreSQL-Instance 5432. Wenn Sie einen anderen Port verwenden, müssen Verbindungen zu diesem Port für die EC2-Instance geöffnet sein.	DBA, Systemadministrator
Ändern Sie die Instance und weisen Sie die neue Zielparametergruppe zu.	Beispiel: `pgtarget-param-group`	DBA
Starten Sie die Amazon RDS-DB-Ziel-Instance neu.	Die Parameter `shared_preload_libraries` und `max_worker_processes` sind statische Parameter und erfordern einen Neustart der Instance.	DBA, Systemadministrator
Stellen Sie über psql eine Verbindung mit der Datenbank von der EC2-Instance her.	Verwenden Sie den -Befehl: `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Erstellen Sie die Erweiterung pg_transport.	Führen Sie die folgende Abfrage als Benutzer mit der `rds_superuser` Rolle aus: `create extension pg_transport;`	DBA

Vorbereiten der Quellumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern der Sicherheitsgruppe der Quelle, um Verbindungen am Port der DB-Instance von der Amazon EC2-Instance und der Ziel-DB-Instance zuzulassen	Standardmäßig ist der Port für die PostgreSQL-Instance 5432. Wenn Sie einen anderen Port verwenden, müssen Verbindungen zu diesem Port für die EC2-Instance geöffnet sein.	DBA, Systemadministrator
Ändern Sie die Instance und weisen Sie die neue Quellparametergruppe zu.	Beispiel: `pgsource-param-group`	DBA
Starten Sie die Amazon RDS-DB-Quell-Instance neu.	Die Parameter `shared_preload_libraries` und `max_worker_processes` sind statische Parameter und erfordern einen Neustart der Instance.	DBA
Stellen Sie über psql eine Verbindung mit der Datenbank von der EC2-Instance her.	Verwenden Sie den -Befehl: `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Erstellen Sie die Erweiterung pg_transport und entfernen Sie alle anderen Erweiterungen aus den zu transportierenden Datenbanken.	Der Transport schlägt fehl, wenn auf der Quelldatenbank andere Erweiterungen als pg_transport installiert sind. Dieser Befehl muss von einem Benutzer mit der `rds_superuser` Rolle ausgeführt werden.	DBA

Durchführen des Transports

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie einen Testlauf durch.	Verwenden Sie die `transport.import_from_server` Funktion , um zuerst einen Testlauf durchzuführen: `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', 'true');` Der letzte Parameter dieser Funktion (festgelegt auf `true`) definiert den Testlauf. Diese Funktion zeigt alle Fehler an, die beim Ausführen des Haupttransports auftreten würden. Beheben Sie die Fehler, bevor Sie den Haupttransport ausführen.	DBA
Wenn der Testlauf erfolgreich ist, initiieren Sie den Datenbanktransport.	Führen Sie die `transport.import_from_server` Funktion aus, um den Transport durchzuführen. Es stellt eine Verbindung zur	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quelle her und importiert die Daten. `SELECT transport .import_from_serve r( 'source-db-instanc e-endpoint', source- db-instance-port, 'source-db-instance- user', 'source-user- password', 'source- database-name', 'destination-user- password', false);` Der letzte Parameter dieser Funktion (auf gesetzt`false`) gibt an, dass es sich nicht um einen Testlauf handelt.	
Führen Sie Schritte nach dem Transport aus.	Nachdem der Datenbank transport abgeschlossen ist: • Validieren Sie die Daten in der Zielumgebung. • Fügen Sie dem Ziel alle Rollen und Berechtigungen hinzu. • Aktivieren Sie bei Bedarf alle erforderlichen Erweiteru ngen im Ziel und in der Quelle. • Setzen Sie den Wert des `max_worker_process es` Parameters zurück.	DBA

Zugehörige Ressourcen

- Dokumentation zu Amazon RDS
- pg_transport-Dokumentation
- Migrieren von Datenbanken mit RDS PostgreSQL Transportable Databases (Blogbeitrag)
- PostgreSQL-Downloads
- psql-Dienstprogramm
- Erstellen einer DB-Parametergruppe
- Ändern von Parametern in einer DB-Parametergruppe
- PostgreSQL-Downloads

Plattformwechsel

Themen

- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas in der AWS-Cloud
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren einer lokalen Oracle-Datenbank zu Amazon OpenSearch Service mit Logstash
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle Data Pump
- Migrieren von PostgreSQL auf Amazon EC2 zu Amazon RDS für PostgreSQL mit pglogical
- Migrieren einer On-Premises-PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server mithilfe nativer Sicherungs- und Wiederherstellungsmethoden
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB
- Migrieren einer On-Premises-MySQL-Datenbank zu Aurora MySQL
- Migrieren Sie On-Premises-MySQL-Datenbanken zu Aurora MySQL mit Percona XtraBackup, Amazon EFS und Amazon S3
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren gemeinsam genutzter Dateisysteme in einer großen AWS-Migration
- Migrieren einer Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle GoldenGate Flat File Adaptern
- Ändern von Python- und Perl-Anwendungen zur Unterstützung der Datenbankmigration von Microsoft SQL Server zu Amazon Aurora PostgreSQL – Kompatible Edition

Konfigurieren von Links zwischen Oracle Database und Aurora PostgreSQL – kompatibel

Erstellt von Jee Bol Shetty (AWS), Bhanu Ganesh Gudivada (AWS), Sushant Deshmukh (AWS), Uttiya Gupta (AWS) und Vikas Gupta (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Plattformwechsel	Workload: Oracle; Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora; Amazon EC2 Auto Scaling ;Amazon Route 53		

Übersicht

Im Rahmen der Migration zur Amazon Web Services (AWS) Cloud können Sie Ihre Anwendungen für die Verwendung cloudnativer Datenbanken modernisieren. Die Migration von Oracle Database zu Amazon Aurora PostgreSQL – Kompatible Edition ist ein solcher Schritt zur Modernisierung. Im Rahmen dieser Migration müssen native Oracle-Datenbanklinks ebenfalls konvertiert werden.

Mithilfe eines Datenbanklinks kann eine Datenbank auf Objekte in einer anderen Datenbank zugreifen. Nach der Migration von Oracle Database zu Aurora PostgreSQL -kompatibel müssen die Datenbankverbindungen vom Oracle Database-Server zu anderen Oracle Database-Servern in PostgreSQL -to-Oracle-Datenbankverbindungen konvertiert werden.

Dieses Muster zeigt, wie Sie Datenbankverbindungen von einem Oracle-Datenbankserver zur Aurora-PostgreSQL-kompatiblen Datenbank einrichten können. Da Datenbankverbindungen unidirektional sind, umfasst das Muster auch die Konvertierung von Datenbankverbindungen von der PostgreSQL-Datenbank in die Oracle-Datenbank.

Nach der Migration und Konvertierung von Oracle Database in eine Aurora PostgreSQL kompatible Datenbank sind die folgenden Schritte erforderlich, um Datenbankverbindungen zwischen Datenbanken einzurichten:

- Um eine Datenbankverbindung mit Oracle Database als Quelle und Aurora PostgreSQL – kompatibel als Ziel einzurichten, müssen Oracle Database Gateways für die Kommunikation zwischen heterogenen Datenbanken konfiguriert sein.
- Wenn Sie eine Datenbankverbindung zwischen Aurora PostgreSQL – kompatible Version 12.6 und früher als Quelldatenbank und Oracle Database als Ziel einrichten, ist die `oracle_fdw` Erweiterung nicht nativ verfügbar. Stattdessen können Sie die `postgres_fdw` Erweiterung in der Aurora PostgreSQL -kompatiblen Datenbank verwenden und `oracle_fdw` in einer PostgreSQL-Datenbank konfigurieren, die in Amazon Elastic Compute Cloud (Amazon EC2) erstellt wurde. Diese Datenbank fungiert als Vermittler zwischen der Aurora-PostgreSQL-kompatiblen Datenbank und Oracle Database. Dieses Muster enthält zwei Optionen zum Einrichten des Datenbanklinks mit Aurora PostgreSQL 12.6 und früher:
  - Konfigurieren Sie die EC2-Instance in einer Amazon EC2-Auto Scaling-Gruppe mit einem Amazon EC2-Startup-Skript, das einen internen DNS-Eintrag (Domain Name System) in Amazon Route 53 aktualisiert.
  - Konfigurieren Sie die EC2-Instance in einer Amazon EC2 Auto Scaling-Gruppe mit einem Network Load Balancer für Hochverfügbarkeit (HA).

Wenn Sie eine Datenbankverbindung zwischen Aurora PostgreSQL -kompatible Version 12.7 und höher einrichten, können Sie die -`oracle_fdw`Erweiterung verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Amazon Aurora PostgreSQL – Kompatible Datenbank in einer Virtual Private Cloud (VPC)
- Netzwerkkonnektivität zwischen Oracle und Aurora PostgreSQL – kompatible Datenbanken

Einschränkungen

- Derzeit können Datenbanklinks nicht mit Amazon Relational Database Service (Amazon RDS) für Oracle als Quelldatenbank und Aurora PostgreSQL – kompatibel als Zieldatenbank eingerichtet werden.

Produktversionen

- Oracle Database 11g und höher

- Aurora PostgreSQL – kompatibel mit 11 und höher

Architektur

Quelltechnologie-Stack

Vor der Migration kann die Oracle-Quelldatenbank über Datenbanklinks auf Objekte in anderen Oracle-Datenbanken zugreifen. Dies funktioniert nativ zwischen Oracle-Datenbanken vor Ort oder in der AWS Cloud.

Zieltechnologie-Stack

Option 1

- Amazon Aurora PostgreSQL-Compatible Edition
- PostgreSQL-Datenbank auf einer Amazon EC2-Instance
- Amazon EC2 Auto Scaling-Gruppe
- Amazon Route 53
- Amazon Simple Notification Service (Amazon SNS)
- AWS Identity and Access Management (IAM)
- AWS Direct Connect

Option 2

- Amazon Aurora PostgreSQL-Compatible Edition
- PostgreSQL-Datenbank auf einer Amazon EC2-Instance
- Amazon EC2 Auto Scaling-Gruppe
- Network Load Balancer
- Amazon SNS
- Direct Connect

Option 3

- Amazon Aurora PostgreSQL-Compatible Edition
- Direct Connect

Zielarchitektur

Option 1

Das folgende Diagramm zeigt die Einrichtung von Datenbankverbindungen mithilfe der `postgres_fdw` Erweiterungen `oracle_fdw` und mit HA, das von einer Amazon EC2 Auto Scaling-Gruppe und Route 53 bereitgestellt wird.

1. Eine Aurora-PostgreSQL-kompatible Instance mit der `postgres_fdw` Erweiterung stellt eine Verbindung zur PostgreSQL-Datenbank auf Amazon EC2 her.
2. Die PostgreSQL-Datenbank mit der `oracle_fdw` Erweiterung befindet sich in einer Auto Scaling-Gruppe.
3. Die PostgreSQL-Datenbank auf Amazon EC2 verwendet Direct Connect, um eine Verbindung zu Oracle Database On-Premises herzustellen.
4. Oracle Database ist mit Oracle Database Gateways für Verbindungen von Oracle Database zur PostgreSQL-Datenbank in AWS konfiguriert.
5. IAM erteilt Amazon EC2 die Berechtigung, Route 53-Datensätze zu aktualisieren.
6. Amazon SNS sendet Warnungen für Auto-Scaling-Aktionen.
7. Der in Route 53 konfigurierte Domänenname verweist auf die IP-Adresse der PostgreSQL-Amazon EC2-Instance.

Option 2

Das folgende Diagramm zeigt die Einrichtung von Datenbankverbindungen mithilfe der `postgres_fdw` Erweiterungen `oracle_fdw` und mit HA, das von einer Auto Scaling-Gruppe und einem Network Load Balancer bereitgestellt wird.

1. Eine mit Aurora PostgreSQL kompatible Instance mit der `postgres_fdw` Erweiterung stellt eine Verbindung zum Network Load Balancer her.
2. Der Network Load Balancer verteilt die Verbindung von der mit Aurora PostgreSQL kompatiblen Datenbank zur PostgreSQL-Datenbank auf Amazon EC2.
3. Die PostgreSQL-Datenbank mit der `oracle_fdw`Erweiterung befindet sich in einer Auto Scaling-Gruppe.

4. Die PostgreSQL-Datenbank auf Amazon EC2 verwendet Direct Connect, um eine Verbindung zu Oracle Database On-Premises herzustellen.
5. Oracle Database ist mit Oracle Database Gateways für Verbindungen von Oracle Database zur PostgreSQL-Datenbank in AWS konfiguriert.
6. Amazon SNS sendet Warnungen für Auto-Scaling-Aktionen.

Option 3

Das folgende Diagramm zeigt die Einrichtung von Datenbanklinks mithilfe der `-oracle_fdw`Erweiterung in einer Aurora-PostgreSQL-kompatiblen Datenbank.

1. Eine mit Aurora PostgreSQL kompatible Instance mit der `oracle_fdw` Erweiterung verwendet Direct Connect, um eine Verbindung zu Oracle Database herzustellen.
2. Oracle Database Gateways, die auf Oracle Server eingerichtet sind, ermöglichen die Konnektivität über Direct Connect mit der Aurora PostgreSQL kompatiblen Datenbank.

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren. In diesem Muster verwenden die Optionen 1 und 2 eine EC2-Instance, um eine PostgreSQL-Datenbank zu hosten.
- Amazon EC2 Auto Scaling unterstützt Sie bei der Aufrechterhaltung der Anwendungsverfügbarkeit und ermöglicht Ihnen das automatische Hinzufügen oder Entfernen von Amazon EC2-Instances gemäß den von Ihnen definierten Bedingungen.

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Network Load Balancer .

Andere -Services

- Oracle Database Gateways bietet Oracle Database die Möglichkeit, auf Daten in einem Nicht-Oracle-System zuzugreifen.

Polen

Häufige Einrichtungsaufgaben für Option 1 und Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine EC2-Instance und konfigurieren Sie die PostgreSQL-Erweiterung oracle_fdw.	1. Erstellen Sie eine EC2-Instance mit dem Betriebssystem Amazon Linux 2.
	2. Um PostgreSQL zu installieren, melden Sie sich bei der EC2-Instance als ec2-user an und führen Sie die folgenden Befehle aus.
	`sudo su - root`
	`sudo tee /etc/yum.repos.d/pgdg.repo<<EOF`
	`[pgdg12]`
		Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>name=PostgreSQL 12
	 for RHEL/CentOS 7 -
	 x86_64
	baseurl=https://down
	load.postgresql.or
	g/pub/repos/yum/12/
	redhat/rhel-7-x86_64
	enabled=1
	gpgcheck=0
	EOF
	
	sudo yum install -y
	 postgresql12-server
	sudo yum install
	 postgresql12-devel
	
	sudo /usr/pgsql-12/
	bin/postgresql-12-
	setup initdb
	sudo systemctl enable
	 postgresql-12
	sudo systemctl start
	 postgresql-12</pre>	

	3. Laden Sie den `oracle_fdw` Quellcode von herunter GitHub.
	
	<pre>mkdir -p /var/lib/
	pgsql/oracle_fdw/
	cd /var/lib/pgsql/
	oracle_fdw/
	
	wget https://g
	ithub.com/laurenz/
	oracle_fdw/archive
	/refs/heads/master
	.zip
	unzip master.zip</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Installieren Sie Oracle Instant Client und richten Sie die Oracle-Umgebungsvariablen ein.
	
	`yum install https://download.oracle.com/otn_software/linux/instantclient/1912000/oracle-instantclient19.12-basic-19.12.0.0.0-1.x86_64.rpm`
	
	`yum install https://download.oracle.com/otn_software/linux/instantclient/1912000/oracle-instantclient19.12-devel-19.12.0.0.0-1.x86_64.rpm`
	
	`export ORACLE_HOME=/usr/lib/oracle/19.12/client64export LD_LIBRARY_PATH=/usr/lib/oracle/19.12/client64/lib:$LD_LIBRARY_PATH`
	
	5. Stellen Sie sicher, dass auf die richtige Version `pg_config` verweist.
	
	`which pg_config`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	6. Kompilieren Sie `oracle_fdw` .
	
	`cd /var/lib/pgsql/oracle_fdw/oracle_fdw-master`
	`make`
	`make install`
	
	Hinweis: Wenn Sie die Fehlermeldung erhalten, dass `oci.h` fehlt, fügen Sie Folgendes in hinzu`Makefile`:
	• Fügen Sie zu `PG_CPPFLAGS` hinzu `-I/usr/include/oracle/19.12/client64`
	• Fügen Sie zu `SHLIB_LINK` hinzu `-L/usr/lib/oracle/19.12/client64/lib`
	
	Weitere Informationen finden Sie im oracle_fdw-Repository .
	7. Melden Sie sich bei der PostgreSQL-Datenbank an und erstellen Sie die `oracle_fdw` Erweiterung .
	
	`sudo su - postgres`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	psql postgres create extension oracle_fdw; 8. Erstellen Sie einen PostgreSQL-Benutzer, dem die fremden Tabellen gehören. CREATE USER pguser WITH PASSWORD '<password>'; GRANT CONNECT ON DATABASE postgres TO pguser; 9. Erstellen Sie den Fremddaten-Wrapper. Ersetzen Sie die folgenden Werte durch Ihre Oracle Database-Serverdetails: • <Oracle DB Server IP> • <Oracle DB Port> • <Oracle_SID> create server oradb foreign data wrapper oracle_fdw options (dbserver '//<Oracle DB Server IP>:<Oracle DB Port>/<Oracle_SID>'); GRANT USAGE ON FOREIGN SERVER oradb TO pguser;	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Um die Benutzerzuordnung und eine Fremdtabelle zu erstellen, die der Oracle-Tabelle zugeordnet ist, stellen Sie eine Verbindung mit der PostgreSQL-Datenbank als her `pguser` und führen Sie den folgenden Befehl aus. Beachten Sie, dass im Beispielcode als Oracle-Schema verwendet `DMS_SAMPLE` wird, das die `NAME_DATA` Tabelle enthält, und sein Passwort `dms_sample` ist. Ersetzen Sie sie nach Bedarf. `create user mapping for pguser server oradb options (user 'DMS_SAMPLE', password 'dms_sample');` Hinweis: Im folgenden Beispiel wird eine Fremdtabelle in PostgreSQL für eine Tabelle in Oracle Database erstellt. Für jede Oracle-Tabelle, die Zugriff von der PostgreSQL-Instance benötigt, muss eine ähnliche Fremdtabelle erstellt werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	CREATE FOREIGN TABLE
	 name_data(
	  name_type
	 CHARACTER VARYING(1
	5) NOT NULL,
	  name CHARACTER
	 VARYING(45) NOT NULL
	  ) SERVER oradb
	 OPTIONS (schema
	 'DMS_SAMPLE', table
	 'NAME_DATA');
	
	select count(*) from
	 name_data;
	``	

	11. Konfigurieren Sie die PostgreSQL-Datenbank auf der EC2-Instance so, dass sie die Oracle-Bibliotheken beim Start der PostgreSQL-Datenbank finden kann. Dies wird von der `oracle_fdw` Erweiterung benötigt. ``` sudo systemctl stop postgresql-12 ``` Hinweis: Bearbeiten Sie die `/usr/lib/systemd/system/postgresql-12.service` Datei so, dass sie die Umgebungsvariablen enthält, damit der `systemctl` Startup die für erforderlichen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Oracle-Bibliotheken findetoracle_fdw .
	
	`# Oracle Environment Variables`
	`Environment=ORACLE_HOME=/u01/app/oracle/product/12.2.0.1/db_1`
	`Environment=LD_LIBRARY_PATH=/u01/app/oracle/product/12.2.0.1/db_1/lib:/lib:/usr/lib`
	
	`sudo systemctl start postgresql-12`	

Option 1: Einrichten eines Datenbanklinks mit den Erweiterungen oracle_fdw und postgres_fdw, einer Auto Scaling-Gruppe und Route 53

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine privat gehostete Zone in Amazon Route 53 ein.	1. Erstellen Sie eine privat gehostete Zone in Amazon Route 53. Notieren Sie sich den Domainnamen , der einer EC2-Instance zugeordnet wird. 2. Fügen Sie mithilfe einer einfachen Routing-Richtlinie , die in die IP-Adresse der EC2-Instance aufgelöst wird, einen „A“-Datensatz hinzu, der die oracle_fd	DBA, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	w PostgreSQL-Erweiterung enthält. 3. Notieren Sie sich nach dem Speichern des Datensatzes „A“ die ID der gehosteten Zone des Domainnamens aus Schritt 1. Dies wird verwendet, um die entsprechende IAM-Richtlinie zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Rolle , die einer EC2-Instance zugeordnet wird.	Verwenden Sie die folgende Richtlinie, um eine IAM-Rolle zu erstellen, die an die EC2-Instance angehängt wird. Ersetzen Sie durch Informationen<Hosted zone ID> , die in der vorherigen Geschichte erfasst wurden.
	
	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Sid": "VisualEditor0",
	"Effect": "Allow",
	"Action": "route53:ChangeResourceRecordSets",
	"Resource": "arn:aws:route53::
	:hostedzone/<Hosted zone ID>"
	},
	{
	"Sid": "VisualEditor1",
	"Effect": "Allow",
	"Action": "route53:ListHostedZones",
	"Resource": "*"
	}
	]
	}
		Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen einer EC2 Startvorlage.	1. Erstellen Sie ein AMI der EC2-Instance, das die `oracle_fdw` PostgreSQL-Erweiterung enthält.
	2. Verwenden Sie das AMI, um eine EC2-Startvorlage zu erstellen.
	3. Um die Verbindung von der Aurora-PostgreSQL-kompatiblen Instance zur PostgreSQL-Datenbank auf der EC2-Instance zu ermöglichen, ordnen Sie die zuvor erstellte IAM-Rolle zu und fügen Sie Sicherheitsgruppen an.
	4. Fügen Sie im Abschnitt Benutzerdaten die folgenden Befehle hinzu und ändern Sie `Hosted zone ID` und `Domain Name` in die entsprechenden Werte. Wählen Sie dann Startvorlage erstellen aus.
	`#!/bin/bash`
	`v_zone_id='Hosted zone ID'`
	`v_domain_name='Domain Name'`
	`v_local_ipv4=$(curl -s http://169.254.169.254/late`
		Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	st/meta-data/local-ipv4) aws route53 change-resource-record-sets --hosted-zone-id $v_zone_id --change-batch '{"Changes":[{"Action":"UPSERT","ResourceRecordSet":{"Name":"'$v_domain_name'","Type":"A","TTL":10,"ResourceRecords":[{"Value":"'$v_local_ipv4'"}]}}]}'	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Auto Scaling-Gruppe ein.	1. Um eine Auto Scaling-Gruppe einzurichten, verwenden Sie die Startvorlage, die Sie im vorherigen Schritt erstellt haben. 2. Konfigurieren Sie die entsprechende VPC und die entsprechenden Subnetze, die zum Starten der EC2-Instance verwendet werden. Die Einrichtung von Option 1 verwendet nicht den Load Balancer . 3. Legen Sie unter Skalierungsrichtlinien die gewünschte -, Minimal- und Maximalkapazität auf 1 fest. 4. Um Warnungen an das Betriebsteam zu senden, fügen Sie Benachrichtigungen für Ereignisse wie Starten oder Beenden hinzu. 5. Überprüfen Sie die Konfiguration und wählen Sie Auto Scaling-Gruppe erstellen aus. Nach Abschluss startet die Auto Scaling-Gruppe die EC2-Instance, die die `oracle_fdw` PostgreSQL-Erweiterung	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthält, die eine Verbindung mit Oracle Database herstellt. Hinweis: Wenn Sie auf eine neue Oracle-Tabelle zugreifen oder die Struktur einer Oracle-Tabelle ändern müssen, müssen diese Änderungen in der PostgreSQL-Fremdta belle wiedergegeben werden. Nachdem Sie die Änderungen implementiert haben, müssen Sie ein neues AMI der EC2-Instance erstellen und es zum Konfigurieren der Startvorlage verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die postgres_fdw-Erweiterung in der Aurora-PostgreSQL-kompatiblen Instance.	1. Konfigurieren Sie `postgres_fdw` in der mit Aurora PostgreSQL kompatiblen Instance. Dadurch wird eine Verbindung mit der PostgreSQL-Datenbank auf Amazon EC2 hergestellt, die als Zwischenknoten zwischen der Aurora PostgreSQL-kompatiblen Instance und der Oracle-Datenbank fungiert.
	2. Stellen Sie eine Verbindung mit der mit Aurora PostgreSQL kompatiblen Instance her und führen Sie die folgenden Befehle aus.
	`create extension postgres_fdw;`
	`CREATE SERVER pgoradb FOREIGN DATA WRAPPER postgres_fdw OPTIONS (dbname 'postgres', host 'Domain Name', port '5432');`
	`CREATE USER MAPPING for postgres SERVER pgoradb OPTIONS (user 'pguser', password '<password>');`
		Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CREATE FOREIGN TABLE data_mart.name_data(name_type CHARACTER VARYING(15) NOT NULL, name CHARACTER VARYING(45) NOT NULL) SERVER pgoradb OPTIONS (schema_name 'public', table_name 'name_data'); select count(*) from data_mart.name_data; Damit ist die Einrichtung eines Datenbanklinks von Aurora PostgreSQL – kompatibel mit Oracle Database abgeschlossen. Die Lösung bietet eine Notfallwiederherstellungs-Strategie (DR), falls die EC2-Instance, die die PostgreSQL-Datenbank hostet, ausfällt. Die Auto Scaling-Gruppe startet eine neue EC2-Instance und aktualisiert das DNS mit der IP-Adresse der neuen EC2-Instance. Dadurch wird sichergestellt, dass die fremden Tabellen in der Aurora PostgreSQL-kompatiblen Instance ohne manuellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Eingriff auf die Oracle-Ta bellen zugreifen können.	

Option 2: Einrichten eines Datenbanklinks mit den Erweiterungen oracle_fdw und postgres_fdw, einer Auto Scaling-Gruppe und einem Network Load Balancer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer EC2 Startvorl age.	1. Erstellen Sie ein AMI der EC2-Instance, das die `oracle_fdw` PostgreSQ L-Erweiterung enthält. 2. Verwenden Sie das AMI, um eine EC2-Startvorlage zu erstellen.	Cloud-Administrator, DBA
Richten Sie eine Zielgruppe, einen Network Load Balancer und eine Auto Scaling-Gruppe ein.	1. Um eine Zielgruppe zu erstellen, wählen Sie Instances als Zieltyp aus. Wählen Sie für Protokoll die Option TCP und für Port die Option 5432 aus. Wählen Sie dann die VPC aus, in der Sie die Zielgrupp e haben möchten, und wählen Sie die entsprech ende Zustandsprüfung aus. 2. Erstellen Sie einen internen Network Load Balancer in der VPC. Konfigurieren Sie den Load Balancer so, dass er protocol:port TCP:5432 überwacht. Legen Sie die Standardaktion auf	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weiterleiten an fest und wählen Sie die Zielgruppe aus, die Sie erstellt haben. 3. Richten Sie eine Auto Scaling-Gruppe mithilfe der von Ihnen erstellten Startvorlage ein. 4. Konfigurieren Sie die Auto Scaling-Gruppe mit der entsprechenden VPC und den entsprech enden Subnetzen, die zum Starten der EC2-Instances verwendet werden. 5. Wählen Sie für die Option Load Balancing die Option An einen vorhandenen Load Balancer anhängen und wählen Sie die Zielgruppe aus, die Sie erstellt haben. Wählen Sie für Zustandsprüfungen die Option ELB aus. 6. Legen Sie unter Skalierun gsrichtlinien die gewünscht e und minimale Kapazität auf 2 und die maximale Kapazität auf eine höhere Zahl fest, wie es zur Unterstützung der Last mit HA erforderlich ist. 7. Um Warnungen an das Betriebsteam zu senden, fügen Sie Benachric	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	htigungen für Ereignisse wie Starten oder Beenden hinzu. 8. Überprüfen Sie die Konfiguration und wählen Sie Auto Scaling-Gruppe erstellen aus. Nach Abschluss startet die Auto Scaling-Gruppe die gewünschte Anzahl von EC2-Instances, die die `oracle_fdw` PostgreSQL-Erweiterung enthalten, die eine Verbindung mit Oracle Database herstellt. Hinweis: Wenn Sie auf eine neue Oracle-Tabelle zugreifen oder die Struktur einer Oracle-Tabelle ändern müssen, müssen diese Änderungen in der PostgreSQL-Fremdta belle wiedergegeben werden. Nachdem Sie die Änderungen implementiert haben, müssen Sie ein neues AMI der EC2-Instance erstellen und es zum Konfigurieren der Startvorlage verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die postgres_fdw-Erweiterung in der Aurora-PostgreSQL-kompatiblen Instance.	Konfigurieren Sie `postgres_fdw` in der mit Aurora PostgreSQL kompatiblen Instance. Dadurch wird über einen Network Load Balancer eine Verbindung zur PostgreSQL-Datenbank in EC2 hergestellt. Die PostgreSQL-Instance auf EC2 fungiert als Zwischenknoten zwischen der mit Aurora PostgreSQL kompatiblen Instance und Oracle Database.
	
	Stellen Sie eine Verbindung mit der mit Aurora PostgreSQL kompatiblen Instance her und führen Sie die folgenden Befehle aus.
	
	`create extension postgres_fdw;`
	`CREATE SERVER pgoradb FOREIGN DATA WRAPPER postgres_fdw OPTIONS (dbname 'postgres', host 'DNS name of Network Load Balancer', port '5432');`
	
	`CREATE USER MAPPING for postgres SERVER pgoradb OPTIONS (user 'pguser', password '<password>');`
		Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>CREATE FOREIGN TABLE
	data_mart.name_data(
	name_type CHARACTER
	VARYING(15) NOT NULL,
	name CHARACTER
	VARYING(45) NOT NULL
	) SERVER pgoradb OPTIONS
	(schema_name 'public',
	table_name 'name_dat
	a');
	
	select count(*) from
	data_mart.name_data;</pre>	

	Damit ist die Einrichtung des Datenbanklinks von Aurora PostgreSQL – kompatibel mit Oracle Database abgeschlossen.	
	Wenn EC2, das die PostgreSQL-Datenbank hostet, ausfällt, identifiziert der Network Load Balancer den Fehler und stoppt den Datenverkehr zu einer ausgefallenen EC2-Instance. Die Auto Scaling-Gruppe startet eine neue EC2-Instance und registriert sie beim Load Balancer. Dadurch wird sichergestellt, dass die fremden Tabellen in der Aurora PostgreSQL-kompatiblen Instance nach einem Ausfall der ursprünglichen EC2-Instance ohne manuellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Eingriff auf die Oracle-Ta bellen zugreifen können.	

Option 3: Einrichten eines Datenbanklinks mit der Erweiterung oracle_fdw in einer mit Aurora PostgreSQL kompatiblen Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Erweiterung oracle_fdw in der mit Aurora PostgreSQL kompatiblen Instance.	Für Aurora-PostgreSQL-kompatible Datenbank version 12.7 und höher ist die `oracle_fdw` Erweiteru ng nativ verfügbar. Dadurch entfällt die Notwendigkeit, die PostgreSQL-Zwische ndatenbank auf einer EC2-Instance zu erstellen. Die mit Aurora PostgreSQL kompatible Instance kann direkt eine Verbindung zu Oracle Database herstellen. 1. Um die `oracle_fdw` Erweiterung zu erstellen , melden Sie sich bei der mit Aurora PostgreSQ L kompatiblen Instance an und führen Sie den folgenden Befehl aus. `create extension oracle_fdw;` 2. Erstellen Sie den Fremddaten-Wrapper.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ersetzen Sie die folgenden Werte durch Ihre Oracle Database-Serverdetails: • `<Oracle DB Server IP>` • `<Oracle DB Port>` • `<Oracle_SID>` `create server oradb foreign data wrapper oracle_fdw options (dbserver '//<Oracle DB Server IP>:<Oracle DB Port>/<Oracle_SID>');` 3. Führen Sie den folgenden Befehl aus, um die Benutzerzuordnung und eine Fremdtabelle zu erstellen, die der Oracle-Tabelle zugeordnet ist. Beachten Sie, dass im Beispielcode als Oracle-Schema verwendet `DMS_SAMPLE` wird, das die `NAME_DATA` Tabelle enthält, und sein Passwort `dms_sample` ist. Ersetzen Sie sie nach Bedarf. Außerdem muss eine Fremdtabelle in der mit Aurora PostgreSQL kompatiblen Instance erstellt werden, um auf	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	jede andere Oracle-Tabelle zugreifen zu können.
	
	`create user mapping for postgres server oradb options (user 'DMS_SAMPLE', password 'dms_sample');`
	
	`CREATE FOREIGN TABLE name_data( name_type character varying(15) OPTIONS (key 'true') NOT NULL, name character varying(45) OPTIONS (key 'true') NOT NULL )SERVER oradb OPTIONS (schema 'DMS_SAMPLE', table 'NAME_DATA');`
	
	Für jede Oracle-Tabelle, die Zugriff von der PostgreSQL-Instance benötigt, muss eine ähnliche Fremdtabelle erstellt werden.	

Oracle Database Gateways für die Konnektivität von einer lokalen Oracle-Datenbank zu Aurora PostgreSQL einrichten – kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie das Gateway auf dem lokalen Oracle Database-Server.	1. Installieren Sie als Root-Benutzer den neuesten unixODBC-Treibermanager.
	`sudo yum install unixODBC*`
	2. Installieren Sie den PostgreSQL-ODBC-Treiber (`psql0DBC`).
	`sudo wget https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm`
	`sudo yum install pgdg-redhat-repo-latest.noarch.rpm`
	`sudo yum install postgresql12-odbc`
	3. Erstellen Sie einen ODBC-Datenquellennamen (DSN) für den Treiber.
	Der unixODBC-Treibermanager stellt die `isql` Befehlszeilen-Dienstprogramme `odbcinst`, und bereit`odbc_config` , die zum Konfigurieren und Testen des Treibers
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	verwendet werden. Mit den `odbc_config` Dienstpro grammen `odbcinst` oder können Sie die unixODBC-Treibermanagerdate ien finden, um Treiberin formationen an die Erstellun g des DSN zu übergeben.
	
	`odbcinst -j`
	
	Der folgende Code zeigt eine Beispielausgabe.
	
	`unixODBC 2.3.1`
	`DRIVERS.....`
	`.......: /etc/odbc`
	`inst.ini`
	`SYSTEM DATA`
	` SOURCES: /etc/odbc`
	`.ini`
	`FILE DATA SOURCES..`
	`: /etc/ODBCDataSourc`
	`es`
	`USER DATA SOURCES..`
	`: /root/.odbc.ini`
	`SQLULEN Size.......:`
	` 8`
	`SQLLEN Size........:`
	` 8`
	`SQLSETPOSIROW Size.:`
	` 8`
	
	`odbc_config --odbcini`
	` --odbcinstini`
	`/etc/odbc.ini`
	`/etc/odbcinst.ini`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	In der Beispielausgabe sehen Sie die `odbc.ini` Dateien `odbcinst.ini` und . Im Grunde `odbcinst.ini` ist eine Registrierungs- und Konfigurationsdatei für ODBC-Treiber in einer Umgebung, während eine Registrierungs- und Konfigurationsdatei für ODBC-DSNs `odbc.ini` ist. Um die Treiber zu aktiviere n, müssen Sie diese beiden Dateien ändern.
	4. Konfigurieren Sie die `psqlODBC` Treiberbi bliotheken in der ODBC-Treiberdatei `/etc/odbcinst.ini` und fügen Sie die folgenden Zeilen am Ende der Datei hinzu. Diese Zeilen machen einen Eintrag für den Treiber.
	`[PostgreSQL]`
	`Description = ODBC for PostgreSQL`
	`Driver = /usr/lib/psqlodbcw.so`
	`Setup = /usr/lib/libodbcpsqlS.so`
	`Driver64 = /usr/lib64/psqlodbcw.so`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Setup64 = /usr/lib64/libodbcpsqlS.so`
	`FileUsage = 1`
	
	5. Erstellen Sie einen DSN in der Datei `/etc/odbc.ini` . Der Treiberma nager liest diese Datei, um zu bestimmen, wie eine Verbindung mit der Datenbank unter Verwendung der in angegebenen Treiberde tails hergestellt werden sollodbcinst.ini . Ersetzen Sie die folgenden Parameter durch tatsächli che Werte:
	• `<PostgreSQL Port>`
	• `<PostgreSQL Database Name>`
	• `<Aurora PostgreSQL Endpoint>`
	• `<PostgreSQL username>`
	• `<PostgreSQL password>`
	
	`[pgdsn]`
	`Driver=/usr/pgsql-12/lib/psqlodbc.so`
	`Description=PostgreSQL ODBC Driver`
	`Database=<PostgreSQL Database Name>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>Servername=< Aurora PostgreSQL Endpoint> Username=<Postgre SQL username> Password=<PostgreSQL password> Port=<PostgreSQL Port> UseDeclareFetch=1 CommLog=/tmp/ pgodbclink.log Debug=1 LowerCaseIde ntifier=1</pre>	
	6. Testen Sie mit dem `isql` Dienstprogramm die ODBC-Verbindung (`psql0DBC`) mit dem PostgreSQL-Datenbank-DSN, den Sie erstellt haben. <pre>isql -v pgdsn</pre>Der folgende Code zeigt eine Beispielausgabe. <pre>+----------------- ----------------- ----+ | Connected! | | | | sql-statement | | help [tablename] |</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>| quit
	|
	|
	+----------
	---------- 	
	------+
	quit</pre>	

	7. Erstellen Sie mithilfe des DSN das Gateway für den ODBC-Service-Handler (HS).
	
	Erstellen Sie als `oracle` Benutzer eine Datei `initDSN.ora` am Speicherort `$ORACLE_HOME/hs/admin` . In diesem Fall `pgdsn` ist der DSN, daher müssen Sie eine Datei mit dem Namen erstellen`initpgdsn.ora` .
	
	<pre>more initpgdsn.ora</pre>
	Der folgende Code zeigt eine Beispielausgabe.
	
	<pre># This is a sample
	agent init file
	that contains the HS
	parameters that are
	# needed for the
	Database Gateway for
	ODBC
	#
	# HS init parameters</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>#
	
	HS_FDS_CONNEC
	T_INFO=pgdsn
	HS_FDS_TRACE_L
	EVEL=OFF
	HS_FDS_TRACE_FILE_
	NAME=/tmp/ora_hs_t
	race.log
	HS_FDS_SHAREABLE_N
	AME=/usr/lib64/lib
	odbc.so
	HS_NLS_NCHAR=UCS2
	HS_LANGUAGE=AMERICA
	N_AMERICA.AL32UTF8
	
	#
	# ODBC specific
	 environment
	 variables
	#
	
	set ODBCINI=/etc/
	odbc.ini</pre>	

	8. Passen Sie den Listener (`$ORACLE_HOME/network/admin/listener.ora`) an, indem Sie den DSN-Eintrag in `SID_LIST_LISTENER` hinzufügen.
	
	<pre>more $ORACLE_HOME/
	network/admin/
	listener.ora</pre>
	Der folgende Code zeigt eine Beispielausgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>SID_LIST_LISTENER =
	  (SID_LIST =
	   (SID_DESC=
	    (SID_NAME = pgdsn)
	    (ORACLE_HOME = /
	u01/app/oracle/pr
	oduct/12.2.0.1/db_
	1)
	    (ENVS="LD
	_LIBRARY_PATH=/lib
	64:/usr/lib:/usr/l
	ib64:/u01/app/orac
	le/product/12.2.0.
	1/db_1")
	    (PROGRAM=dg4odbc)
	   )
	)</pre> 9. Passen Sie die `tnsname` (`$ORACLE_HOME/network/admin/tnsnames.ora`) an, indem Sie den DSN-Eintrag hinzufügen.
	<pre>more $ORACLE_HOME/
	network/admin/
	tnsnames.ora</pre> Der folgende Code zeigt eine Beispielausgabe.
	<pre>pgdsn=(DESCRIPTION
	=(ADDRESS=(PROTOCO
	L=tcp)(HOST=localh
	ost)(PORT=1521))(C
	ONNECT_DATA=(SID=p
	gdsn))(HS=OK))</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	10. Starten Sie den Oracle-Listener neu, damit die DSN-bezogenen Einträge für die Netzwerkdateien wirksam werden können, und ändern Sie sich `<Listener Name>` mit dem entsprechenden Oracle-Listenernamen.
	`lsnrctl stop <Listener Name>`
	`lsnrctl start <Listener Name>`
	Nach dem Neustart des Oracle-Listeners wird ein Oracle HS-Handler mit einem DSN-Namen () erstelltpgdsn.
	11. Verwenden Sie den DSN, um einen Oracle-Datenbanklink zu erstellen, um auf die PostgreSQL-Datenbank zuzugreifen, indem Sie sich bei Oracle Database anmelden.
	`create public database link pgdb connect to "postgres" identified by "postgres" using 'pgdsn';`
	12. Greifen Sie über den erstellten Oracle-Da	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tenbanklink auf die PostgreSQL-Daten zu. `select count(*) from "pg_tables"@pgdb;`	

Zugehörige Ressourcen

- Amazon Aurora PostgreSQL
- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Identity and Access Management (IAM)
- Starten einer Instance über eine Startvorlage
- Auto Scaling-Gruppen
- Amazon Route 53
- Amazon Simple Notification Service (SNS)
- AWS Network Load Balancer
- Oracle Database Gateways

Zusätzliche Informationen

Obwohl die `oracle_fdw` Erweiterung mit Aurora PostgreSQL -kompatible Version 12.7 und höher verfügbar ist, enthält dieses Muster Lösungen für frühere Versionen von Aurora PostgreSQL -kompatiblen Datenbanken, da viele Kunden ältere Versionen von Aurora PostgreSQL -kompatiblen Datenbanken unterstützen und das Upgrade einer Datenbank mehrere Anwendungs- und Leistungstests beinhaltet. Außerdem wird das Datenbank-Link-Feature umfassend verwendet und die Bereitstellung von Optionen für alle Versionen von Aurora PostgreSQL – kompatibel ist das Ziel dieses Artikels.

Exportieren einer Microsoft SQL Server-Datenbank nach Amazon S3 mithilfe von AWS DMS

Erstellt von Sweta Krishna (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Microsoft SQL Server	Ziel: Amazon S3
R-Typ: Plattformwechsel	Workload: Microsoft	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; Amazon S3		

Übersicht

Organisationen müssen Datenbanken häufig für Datenbankmigration, Sicherung und Wiederherstellung, Datenarchivierung und Datenanalysen in Amazon Simple Storage Service (Amazon S3) kopieren. Dieses Muster beschreibt, wie Sie eine Microsoft SQL Server-Datenbank nach Amazon S3 exportieren können. Die Quelldatenbank kann On-Premises oder auf Amazon Elastic Compute Cloud (Amazon EC2) oder Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server in der Amazon Web Services (AWS) Cloud gehostet werden.

Die Daten werden mit AWS Database Migration Service (AWS DMS) exportiert. Standardmäßig schreibt AWS DMS Volllast- und Change Data Capture (CDC)-Daten im CSV-Format (durch Kommas getrennte Werte). Für eine kompaktere Speicherung und schnellere Abfrageoptionen verwendet dieses Muster die Apache Parquet (.parquet)-Formatoption.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM)-Rolle für das Konto mit Schreib-, Lösch- und Tag-Zugriff auf den S3-Ziel-Bucket und AWS DMS (`dms.amazonaws.com`), die dieser IAM-Rolle als vertrauenswürdige Entität hinzugefügt wurde

- Eine lokale Microsoft SQL Server-Datenbank (oder Microsoft SQL Server auf einer EC2-Instance oder einer Amazon RDS for SQL Server-Datenbank)
- Netzwerkkonnektivität zwischen der Virtual Private Cloud (VPC) in AWS und dem On-Premises-Netzwerk, das von AWS Direct Connect oder einem Virtual Private Network (VPN) bereitgestellt wird

Einschränkungen

- Ein VPC-fähiger S3-Bucket (Gateway-VPC) wird derzeit in AWS DMS-Versionen vor 3.4.7 nicht unterstützt.
- Änderungen an der Quelltabellenstruktur während des vollständigen Ladevorgangs werden nicht unterstützt.
- Der Modus „Volles großes Binärobjekt (LOB)“ von AWS DMS wird nicht unterstützt.

Produktversionen

- Microsoft SQL Server-Versionen 2005 oder höher für die Editionen Enterprise, Standard, Arbeitsgruppe und Entwickler.
- Unterstützung für Microsoft SQL Server Version 2019 als Quelle ist in AWS DMS-Versionen 3.3.2 und höher verfügbar.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank (oder Microsoft SQL Server auf einer EC2-Instance oder einer Amazon RDS for SQL Server-Datenbank)

Zieltechnologie-Stack

- AWS Direct Connect
- AWS DMS
- Amazon S3

Zielarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Polen

Vorbereiten der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Datenbankversion.	Validieren Sie die Quelldatenbankversion und stellen Sie sicher, dass sie von AWS DMS unterstützt wird. Informationen zu unterstützten SQL Server-Datenbankversionen finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS.	DBA
Erstellen Sie eine VPC und eine Sicherheitsgruppe.	Erstellen Sie in Ihrem AWS-Konto eine VPC und eine Sicherheitsgruppe. Weitere Informationen finden Sie in der Amazon-VPC-Dokumentation.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzer für die AWS DMS-Aufgabe.	Erstellen Sie einen AWS DMS-Benutzer in der Quelldatenbank und erteilen Sie ihm READ-Berechtigunge n. Dieser Benutzer wird von AWS DMS verwendet.	DBA
Testen Sie die DB-Konnek tivität.	Testen Sie die Konnektivität zur SQL Server-DB-Instance vom AWS DMS-Benutzer aus.	DBA
Erstellen Sie einen S3-Bucket.	Erstellen Sie den S3-Ziel-B ucket. Dieser Bucket enthält die migrierten Tabellendaten.	Systemadministrator
Erstellen Sie eine IAM-Richt linie und -Rolle.	1. Um eine IAM-Richtlinie mit Bucket-Berechtigungen zu erstellen, verwenden Sie den Code im Abschnitt Zusätzliche Informationen. 2. Erstellen Sie die Rolle für AWS DMS und fügen Sie die Richtlinie an die Rolle an.	Systemadministrator

Migrieren von Daten mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS DMS-Konsole. Wählen Sie im Navigationsbereich Replikati ons-Instances, Replikati	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ons-Instance erstellen aus. Anweisungen finden Sie in Schritt 1 der AWS DMS-Dokumentation.	
Erstellen Sie Quell- und Zielendpunkte.	Erstellen Sie Quell- und Zielendpunkte. Testen Sie die Verbindung von der Replikati ons-Instance zu Quell- und Zielendpunkten. Anweisung en finden Sie in Schritt 2 der AWS DMS-Dokumentation.	DBA
Erstellen Sie eine Replikati onsaufgabe.	Erstellen Sie eine Replikati onsaufgabe und wählen Sie Volllast oder Volllast mit Change Data Capture (CDC) aus, um Daten vom SQL Server in den S3-Bucket zu migrieren. Anweisungen finden Sie in Schritt 3 der AWS DMS-Dokumentation.	DBA
Starten Sie die Datenrepl ikation.	Starten Sie die Replikati onsaufgabe und überwachen Sie die Protokolle auf Fehler.	DBA

Validieren der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die migrierten Daten.	Navigieren Sie in der -Konsole zu Ihrem S3-Ziel-Bucket. Öffnen Sie den Unterordner mit demselben Namen wie die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quelldatenbank. Vergewissern Sie sich, dass der Ordner alle Tabellen enthält, die aus der Quelldatenbank migriert wurden.	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter und löschen Sie sie.	Fahren Sie temporäre AWS-Ressourcen herunter, die Sie für die Datenmigration erstellt haben, z. B. die AWS DMS-Replikations-Instance, und löschen Sie sie, nachdem Sie den Export validiert haben.	DBA

Zugehörige Ressourcen

- AWS Database Migration Service-Benutzerhandbuch
- Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS
- Verwenden von Amazon S3 als Ziel für AWS Database Migration Service
- Verwenden eines S3-Buckets als AWS DMS-Ziel (AWS re:Post)

Zusätzliche Informationen

Verwenden Sie den folgenden Code, um eine IAM-Richtlinie mit S3-Bucket-Berechtigungen für die AWS DMS-Rolle hinzuzufügen. Ersetzen Sie `bucketname` durch den Namen von Ihrem Bucket.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        }
    ]
}
```

Migrieren von ML Build, Training und Bereitstellung von Workloads zu Amazon SageMaker mithilfe von AWS-Entwicklertools

Erstellt von Scot Marvin (AWS)

R-Typ: Plattformwechsel	Quelle: Machine Learning	Ziel: Amazon SageMaker
Erstellt von: AWS	Umgebung: PoC oder Pilotprojekt	Technologien: Machine Learning und KI DevOps; Migration
AWS-Services: Amazon SageMaker		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer On-Premises-Anwendung für Machine Learning (ML), die auf Unix- oder Linux-Servern ausgeführt wird, um auf AWS mit Amazon zu trainieren und bereitzustellen SageMaker. Diese Bereitstellung verwendet eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD). Das Migrationsmuster wird mithilfe eines AWS- CloudFormation Stacks bereitgestellt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto, das AWS Landing Zone verwendet
- AWS-Befehlszeilenschnittstelle (AWS CLI), die auf Ihrem Unix- oder Linux-Server installiert und konfiguriert ist
- Ein ML-Quellcode-Repository in CodeCommit, GitHubAWS oder Amazon Simple Storage Service (Amazon S3)

Einschränkungen

- In einer AWS-Region können nur 300 einzelne Pipelines bereitgestellt werden.
- Dieses Muster ist für überwachte ML-Workloads mit train-and-deploy Code in Python vorgesehen.

Produktversionen

- Docker-Version 19.03.5, Build 633a0ea, mit Python 3.6x

Architektur

Quelltechnologie-Stack

- On-Premises-Linux-Compute-Instance mit Daten entweder im lokalen Dateisystem oder in einer relationalen Datenbank

Quellarchitektur

Zieltechnologie-Stack

- AWS CodePipeline bereitgestellt mit Amazon S3 für die Datenspeicherung und Amazon DynamoDB als Metadatenspeicher für die Nachverfolgung oder Protokollierung von Pipeline-Ausführungen

Zielarchitektur

Architektur der Anwendungsmigration

- Natives Python-Paket und AWS- CodeCommit Repository (und ein SQL-Client für On-Premises-Datensätze auf der Datenbank-Instance)

Tools

- Python
- Git
- AWS CLI – Die AWS CLI stellt den AWS- CloudFormation Stack bereit und verschiebt Daten in den S3-Bucket. Der S3-Bucket wiederum führt zum Ziel.

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Quellcode und Datensätze.		Data Scientist
Identifizieren Sie die Instance-Typen und -Größen für die Erstellung, Schulung und Bereitstellung des Ziels.		Dateningenieur, Datenwissenschaftler
Erstellen Sie eine Funktionsliste und Kapazitätsanforderungen.		
Identifizieren Sie die Netzwerkanforderungen.		DBA, Systemadministrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerk- oder Hostzugriff für die Quell- und Zielanwendungen.		Dateningenieur, ML-Techniker, Systemadministrator
Bestimmen Sie die Backup-Strategie.		ML-Techniker, Systemadministrator
Bestimmen Sie die Verfügbarkeitsanforderungen.		ML-Techniker, Systemadministrator
Identifizieren Sie die Migrations- oder Umstellungsstrategie der Anwendung.		Datenwissenschaftler, ML-Techniker

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		ML-Techniker, Systemadministrator
Erstellen Sie Sicherheitsgruppen.		ML-Techniker, Systemadministrator
Richten Sie einen Amazon S3-Bucket und AWS-CodeCommit Repository-Verzweigungen für ML-Code ein.		ML-Techniker

Hochladen der Daten und des Codes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbietern, um Trainings-, Validierungs- und Testdatensätze in den bereitgestellten S3-Bucket zu migrieren.	Dies ist für die AWS-CloudFormation Stack-Bereitstellung erforderlich.	Dateningenieur, ML-Ingenieur
Verpacken Sie den ML-Trainings- und Hosting-Code als Python-Pakete und pushen Sie in das bereitgestellte Repository in AWS CodeCommit oder GitHub.	Sie benötigen den Verzweigungsnamen des Repositorys, um die AWS- CloudFormation Vorlage für die Migration bereitzustellen.	Datenwissenschaftler, ML-Techniker

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ML-Workload-Migrationsstrategie.		Anwendungsbesitzer, ML-Techniker
Stellen Sie den AWS-CloudFormation Stack bereit.	Verwenden Sie die AWS CLI, um den Stack zu erstellen, der in der YAML-Vorlage deklariert ist, die mit dieser Lösung bereitgestellt wird.	Datenwissenschaftler, ML-Techniker

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendungsclients auf die neue Infrastruktur um.		Anwendungseigentümer, Datenwissenschaftler, ML-Techniker

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.	Fahren Sie alle benutzerdefinierten Ressourcen aus der AWS- CloudFormation Vorlage herunter (z. B. alle AWS Lambda-Funktionen, die nicht verwendet werden).	Datenwissenschaftler, ML-Techniker
Überprüfen und validieren Sie die Projektdokumente.		Anwendungsbesitzer, Datenwissenschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Ergebnisse und die Metriken zur ML-Modellbewertung mit Operatoren.	Stellen Sie sicher, dass die Modellleistung den Erwartungen der Anwendungsbenutzer entspricht und mit dem On-Premises-Status vergleichbar ist.	Anwendungsbesitzer, Datenwissenschaftler
Schließen Sie das Projekt ab und geben Sie Feedback.		Anwendungsbesitzer, ML-Techniker

Zugehörige Ressourcen

- AWSCodePipeline
- AWSCodeBuild
- AmazonSageMaker
- Amazon S3
- Amazon DynamoDB
- AWS Lambda

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie OpenText TeamSite Workloads in die AWS-Cloud

Erstellt von Battulga Purevragchaa (AWS), Michael Stewart und Carlos Marruenda Molina

Umwelt: Produktion	Quelle: Vor Ort	Ziel: AWS
R-Typ: Replatform	Arbeitslast: Alle anderen Workloads	Technologien: Migration; Web- und mobile Apps
AWS-Dienste: Amazon EC2; Amazon RDS		

Übersicht

> Warnung: Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Die Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Viele OpenText Experience Platform-Instanzen werden vor Ort oder auf herkömmlichen Hosting-Lösungen mit fester Kapazität und älteren Kostenmodellen gehostet. Die Migration Ihrer OpenText Experience Platform-Workloads in die Amazon Web Services (AWS) Cloud bietet zusätzliche Funktionen und Mehrwert, indem Sie Ihre Geschäftsflexibilität und Integrationsmöglichkeiten erhöhen und gleichzeitig Ihre Gesamtbetriebskosten senken.

Dieses Muster enthält Schritte und eine Vorlage für die Migration von OpenText TeamSiteWorkloads in die AWS-Cloud. Das Muster hilft Ihnen, den Umfang und die Budgetierung Ihrer Migrationsprojekte zu verstehen, indem es einen detaillierten Abschnitt zu Epics enthält, der Sie durch den OpenText TeamSite Migrationsprozess führt.

Dieses Muster wurde von AWS und TBSCG, einem AWS-Partner, entwickelt und liegt dem Leitfaden Migration OpenText TeamSite und Medienmanagement von Workloads in die AWS-Cloud auf der AWS Prescriptive Guidance-Website bei.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Mindestens ein aktives AWS-Konto
- Ein OpenText Workload, der in einem lokalen Rechenzentrum oder bei einem anderen Cloud-Anbieter gehostet wird
- Aktive Lizenzen OpenText

Der Migrationsprozess erfordert auch die Rollen und Verantwortlichkeiten, die in der folgenden Tabelle beschrieben sind.

Rolle	Verantwortlichkeiten
Sponsor	Internes Sponsoring
Liefermanager	Lieferung der Migration
Architekt für Lösungen	Definieren Sie die aktuelle und neue Architektur
DevOps Ingenieur	DevOps Aktivitäten
Ein Tester	Testen auf Systemebene
Eigentümer des Produkts	Priorisierung von Aufgaben auf der Grundlage von Geschäftsanforderungen
TeamSite Autoren	Benutzerakzeptanztests für Migration (UAT)
TeamSite Administrator	UAT-Migration
OpenText führen	OpenText Produktspezialist
OpenText Entwickler	OpenText Produktspezialist
Spezialist für Preisgestaltung	AWS und OpenText Lizenzierung
IT-Sicherheit	Grundzüge der IT-Sicherheit
Integrationsentwickler eines Drittanbieters	Überarbeiten Sie bestehende Integrationen

Frontend-Entwickler	Nehmen Sie Änderungen am migrierten Frontend-Code vor
Datenbankadministrator	Konfiguration der Datenbank

Einschränkungen

- Stellen Sie die Kompatibilität mit Ihren Zielbetriebssystemen (OS) sicher. Sie können die Kompatibilitätsmatrix aus den Versionshinweisen der OpenText Produktversion verwenden, die Sie migrieren.

Architektur

Quelltechnologie-Stack

- OpenText Kundenerlebnislösungen, die vor Ort oder bei einem anderen Cloud-Anbieter gehostet werden:
  - OpenText TeamSite
  - OpenText LiveSite
  - OpenText Medienmanagement
  - OpenText MediaBin

Zieltechnologie-Stack

- Eine OpenText Customer Experience-Plattform, die in der AWS-Cloud gehostet wird und die folgenden AWS-Services verwendet:
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Elastic Container Service (Amazon ECS)
  - OpenSearch Amazon-Dienst
  - Elastic Load Balancing
  - AWS Lambda
  - Amazon API Gateway
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon Elastic Block Store (Amazon EBS)

- Amazon-Simple-Storage-Service (Amazon-S3)

Zielarchitektur

Tools

- AWS Database Migration Service (AWS DMS) ist ein Cloud-Service, der die Migration von relationalen Datenbanken, Data Warehouses, NoSQL-Datenbanken und anderen Arten von Datenspeichern vereinfacht.
- AWS Application Migration Service automatisiert die Konvertierung Ihrer Quellserver zur nativen Ausführung auf AWS. Er vereinfacht außerdem die Modernisierung von Anwendungen mit integrierten und benutzerdefinierten Optimierungsoptionen.

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie Workshops zu Entdeckungsanforderungen ab.	Halten Sie Workshops mit Geschäfts- und Technikteams ab, um die aktuelle Situation zu ermitteln, Anforderungen zu sammeln und die Migration sstrategie zu validieren. Je nach Komplexität und Umfang Ihrer Migration benötigt Ihr Unternehmen möglicherweise mehrere Workshops. Dauer: Zwei Wochen	Sponsor (optional), Delivery Manager, Lösungsarchitekt, OpenText Leiter, Product Owner
Analysieren Sie die Lösungs- und Migrationsanforderungen.	Analysieren und dokumenti eren Sie die geschäftlichen, funktionalen und technisch en Anforderungen, die das	Lösungsarchitekt, OpenText Leiter, Produkteigentümer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Design der geplanten Lösung und den Migrationsprozess beeinflussen. Dauer: Eine Woche	
Dokumentieren Sie Ihre bestehende OpenText Architektur.	Dokumentieren Sie Ihre bestehende OpenText Architektur, einschließlich der Kernkomponenten und aller zugehörigen Anwendungen und Dienste. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer
Definieren Sie die geplante AWS-Architektur.	Definieren Sie Ihre geplante AWS-Architektur auf der Grundlage der identifizierten Komponenten und Anforderungen und mithilfe der OpenText Kompatibilitätsmatrix. Die OpenText Kompatibilitätsmatrix finden Sie in den Versionshinweisen Ihrer OpenText TeamSite Version. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produktverantwortlicher, IT-Sicherheit
Beurteilen Sie die Größe Ihrer geplanten AWS-Architektur.	Die Größenanforderungen variieren je nach Arbeitslast und anderen nicht funktionalen Anforderungen für verschiedene Architekturkomponenten. Dauer: Zwei Tage	Lösungsarchitekt, OpenText Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Berechnen Sie die Gesamtbetriebskosten.	Berechnen Sie die Gesamtbetriebskosten (TCO) für Ihre vorgeschlagene Lösung. Dauer: Zwei Tage	Lösungsarchitekt, Preisspezialist
Definieren Sie die Migrationsstrategie für jede Komponente.	Definieren und dokumentieren Sie, welche der sieben gängigen Migrationsstrategien (7 Rs) für jeden Kern oder jede zusätzliche Komponente, die in die AWS-Cloud migriert werden muss, verwendet werden soll. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer
Definieren Sie den Migrationsprozess für die Komponenten.	Definieren Sie den detaillierten Migrationsprozess für jede Komponente Ihres Workloads. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produktverantwortlicher, IT-Sicherheit
Definieren Sie den globalen Migrationsprozess und die Abhängigkeiten.	Erstellen Sie einen globalen Migrationsprozess und einen Kalender, der die Migrationsdetails für Komponenten, Abhängigkeiten und Geschäftskontinuität enthält. Dauer: Drei Tage	Lösungsarchitekt, OpenText Leiter, Produktverantwortlicher, IT-Sicherheit

Sicherheits- und Compliance-Aktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherheitsrichtlinien.	Konfigurieren Sie die vom Kunden verwalteten Sicherheitsrichtlinien in Ihren AWS-Konten. Diese sollten die Komplexität und Rotation von Passwörtern sowie die automatische Deaktivierung ungenutzter Konten beinhalten. Weitere Informationen zu vom Kunden verwalteten Richtlinien finden Sie unter Vom Kunden verwaltete Richtlinien in der Dokumentation zu AWS Identity and Access Management (IAM).	Lösungsarchitekt
Erstellen Sie IAM-Benutzer.	Erstellen Sie die IAM-Benutzer, die Zugriff auf die AWS-Managementkonsole, die AWS-Befehlszeilenschnittstelle (AWS CLI) und das AWS-SDK benötigen. Weitere Informationen zum Erstellen von IAM-Benutzern finden Sie in der IAM-Dokumentation unter Erstellen eines IAM-Benutzers in Ihrem AWS-Konto.	Lösungsarchitekt
Erstellen Sie IAM-Gruppen.	Erstellen Sie die erforderlichen IAM-Benutzergruppe	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n (z. B. Administrator- oder Entwicklergruppen) und fügen Sie diesen Gruppen IAM-Benutzer hinzu. Weitere Informationen zu IAM-Benutzergruppen finden Sie unter IAM-Benutzergruppen in der IAM-Dokumentation.	
Fügen Sie Sicherheitsrichtli nien hinzu.	Fügen Sie den IAM-Gruppen oder -Rollen Sicherheitsrichtli nien hinzu. Weitere Informationen dazu finden Sie in der IAM-Dokum entation unter Eine Richtlinie an eine IAM-Benutzergruppe anhängen.	Lösungsarchitekt
Aktivieren Sie die detaillierte Abrechnung.	Weitere Informationen zur Abrechnung finden Sie unter Überwachung Ihrer Nutzung und Kosten in der Dokumenta tion zu AWS Billing and Cost Management.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Kontaktdaten Ihrer Konten.	Stellen Sie sicher, dass die Kontaktdaten für Ihre Konten aktuell sind und mehr als einer Person in Ihrer Organisation zugeordnet sind. Weitere Informationen finden Sie unter Verwaltung eines AWS-Kontos in der Dokumentation zu AWS Billing and Cost Management.	Lösungsarchitekt, Produkteigentümer
Kontaktinformationen für Sicherheitsfragen hinzufügen.	Konfigurieren Sie Ihre Kontaktinformationen mit Ihren Sicherheitskontaktinformationen. Weitere Informationen dazu finden Sie unter Verwaltung eines AWS-Kontos in der Dokumentation zu AWS Billing and Cost Management.	Lösungsarchitekt, IT-Sicherheit
Richten Sie IAM-Rollen für EC2-Instances ein.	Konfigurieren Sie die IAM-Rollen für die EC2-Instances. Weitere Informationen dazu finden Sie unter IAM-Rollen für Amazon EC2 in der Amazon EC2 EC2-Dokumentation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Zugriff auf den AWS-Support.	Fügen Sie eine IAM-Richtlinie für IAM-Benutzer hinzu, die Zugriff auf das AWS Support for Support Center benötigen , und um Supportfälle zu erstellen. Weitere Informationen dazu finden Sie unter Zugriffsb erechtigungen für AWS Support in der AWS-Support-Dokumentation.	Lösungsarchitekt
Aktivieren CloudTrail.	Aktivieren Sie AWS automatis ch CloudTrail in all Ihren AWS-Regionen. Weitere Informationen dazu finden Sie `create-trail` in der CloudTrail AWS-Dokum entation unter Verwenden.	Lösungsarchitekt
Aktivieren CloudTrail Sie die Überprüfung der Protokoll datei.	Aktivieren Sie die Validieru ng von CloudTrail Protokoll dateien. Weitere Informationen dazu finden Sie CloudTrail in der CloudTrail AWS-Dokum entation unter Aktivieren der Protokolldatei-Integritätsp rüfung für.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beschränken Sie den Zugriff auf alle S3-Buckets, die CloudTrail Protokolle enthalten .	Wenden Sie eine Bucket-Richtlinie an, die den Zugriff auf S3-Buckets einschränkt, die Protokolldateien enthalten CloudTrail . Weitere Informationen dazu finden Sie unter Amazon S3 S3-Bucket-Richtlinie für CloudTrail in der CloudTrail AWS-Dokumentation.	Lösungsarchitekt
Integrieren Sie CloudTrail mit CloudWatch Protokollen	Integrieren Sie CloudTrail mit Amazon CloudWatch Logs generierte Trails. Weitere Informationen dazu finden Sie in der CloudTrail AWS-Dokumentation unter Ereignisse an CloudWatch Logs senden	Lösungsarchitekt
Aktivieren Sie AWS Config in allen erforderlichen Regionen.	Aktivieren Sie AWS Config automatisch in allen erforderlichen Regionen. Sie können AWS Config mithilfe der AWS-CLI einrichten. Weitere Informationen finden Sie unter Einrichten von AWS Config mit der AWS-CLI in der AWS Config-Dokumentation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Protokollierung des S3-Bucket-Zugriffs.	Automatisieren Sie die Protokollierung des S3-Bucket-Zugriffs mit CloudTrail. Weitere Informationen dazu finden Sie in der Amazon S3-Dokumentation unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und -Objekte.	Lösungsarchitekt
Konfigurieren Sie die AWS KMS KMS-Schlüsselrichtlinien für CloudTrail.	Automatisieren Sie die Konfiguration der wichtigsten Richtlinien des AWS Key Management Service (AWS KMS) für CloudTrail. Weitere Informationen dazu finden Sie CloudTrail in der CloudTrail AWS-Dokumentation unter Configure AWS KMS key policies for.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschlüsseln Sie CloudTrail Protokolle im Ruhezustand.	Konfigurieren Sie die serversei tige Verschlüsselung von CloudTrail Protokollen mithilfe von kundenverwalteten Schlüsseln, die in AWS KMS gespeichert sind. Weitere Informationen dazu finden Sie in der AWS-Dokum entation unter Verschlüs seln von CloudTrail Protokoll dateien mit verwalteten AWS-Schlüsseln (SSE-KMS). CloudTrail	Lösungsarchitekt
Automatische Rotation der KMS-Schlüssel.	Konfigurieren Sie die Rotation von AWS-KMS-Schlüsseln. Weitere Informationen dazu finden Sie in der AWS KMS KMS-Dokumentation unter So aktivieren und deaktivieren Sie die automatische Schlüssel rotation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
CloudWatch Alarme konfiguri eren.	Konfigurieren Sie die CloudWatch Amazon-Al arme, die durch bestimmte Ereignisse ausgelöst werden. Zum Beispiel unautorisierte Anfragen an APIs oder die Verwendung des Root-Kont os. Weitere Informationen dazu finden Sie im AWS-Siche rheitsblog unter So erhalten Sie Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS-Kontos verwendet werden.	Lösungsarchitekt
Konfigurieren Sie Sicherhei tsgruppen.	Konfigurieren Sie Sicherhei tsgruppen, um sicherzus tellen, dass uneingeschränkter eingehender Datenverkehr auf den Ports 22 und 3389 nicht zulässig ist.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die VPC-Flow-Protokollierung.	Erfassen Sie abgelehnt en IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer Virtual Private Cloud (VPC) und konfigurieren Sie ihn so CloudWatch , dass er erfasst wird. Weitere Informationen dazu finden Sie unter Erstellen eines Flow-Protokolls in der Amazon VPC-Dokumentation.	Lösungsarchitekt
Ändern Sie die Standards icherheitsgruppe, um den gesamten Datenverkehr einzuschränken.	Ändern Sie die Standards icherheitsgruppe jeder VPC so, dass der Datenverkehr standardmäßig verweigert wird und der Zugriff explizit über Ihre Sicherheitsgruppen gewährt wird. Weitere Informationen dazu finden Sie unter Sicherhei tsgruppen für Ihre VPC in der Amazon VPC-Dokumentation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Routing-T abellen zwischen den VPCs.	Konfigurieren Sie die Routingtabellen für VPC-Peering mit dem geringsten erforderlichen Zugriff. Weitere Informationen dazu finden Sie unter Aktualisieren Ihrer Routing-Tabellen für eine VPC-Peering-Verbindung in der Amazon VPC-Dokum entation.	Lösungsarchitekt

Einrichtungsaktivitäten für die neue AWS-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-Infra struktur bereit.	Erstellen Sie die AWS-Konten und Ressourcen. Dauer: Zwei Wochen	DevOps Ingenieur, Lösungsar chitekt
Richten Sie DevOps Tools und Prozesse ein.	Richten Sie DevOps Tools und Verfahren ein, z. B. CI/CD-Pip elines (Continuous Integrati on and Continuous Delivery) und automatisierte Test-Fram eworks.	DevOps Ingenieur, Lösungsar chitekt
Automatisieren Sie die Migration von Kernkompo nenten.	Verwenden Sie vorhanden e Vorlagen oder Skripts, um die Installation und Konfigura tion von OpenText Produkten wie TeamSite LiveSite, OpenDeploy und zu automatis ieren MediaBin.	DevOps Ingenieur, Lösungsar chitekt, OpenText Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dauer: Eine Woche	
Automatisieren Sie die Migration zusätzlicher Komponenten.	Analysieren und automatisieren Sie die Migration zusätzlicher Anwendungen, die in OpenText Kernkomponenten integriert sind (z. B. zusätzliche Datenbanken, Kommunikations-, Überwachungs- oder Cache-Komponenten). Dauer: Zwei Wochen	DevOps Ingenieur, Lösungsarchitekt, OpenText Leiter
Passen Sie die Kernkomponenten an.	Nehmen Sie alle erforderlichen Änderungen an den Anpassungen der OpenText Kernkomponenten vor (z. B. Integrationen).	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler, Integrationsentwickler eines Drittanbieters, Frontend-Entwickler
Implementieren und konfigurieren Sie zusätzliche Dienste.	Stellen Sie alle neuen AWS-Services wie AWS Lambda-Funktionen oder Amazon API Gateway bereit, konfigurieren und implementieren.	DevOps Ingenieur, Lösungsarchitekt, Integrationsentwickler eines Drittanbieters, Frontend-Entwickler
Migrieren oder überarbeiten Sie andere Komponenten.	Migrieren Sie zusätzliche Komponenten, einschließlich aller erforderlichen Umgestaltungen. Dazu gehören externe Anwendungen wie maßgeschneiderte Berichtsportale oder bestehende API-Integrationsebenen.	DevOps Ingenieur, Lösungsarchitekt, Integrationsentwickler eines Drittanbieters, Frontend-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Migration in der Entwicklungsumgebung durch.	Automatisierte Migration saktivitäten für die Entwicklungsumgebung, einschließlich Systembereitstellung, Datenmigration, Anwendungsmigration, Installation und Konfiguration.	DevOps Ingenieur
Führen Sie die Migration in der Produktionsumgebung durch.	Automatisierte Migration saktivitäten für die Produktionsumgebung, einschließlich Systembereitstellung, Datenmigration, Anwendungsmigration, Installation und Konfiguration.	DevOps Ingenieur

Netzwerkaktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie CIDR-Blöcke für jede VPC.	Definieren Sie den CIDR-Block (Classless Inter-Domain Routing) (IP-Bereich und Maske) für jede nicht standardmäßige VPC. Dauer: Weniger als eine Woche	DevOps Ingenieur, Lösungsarchitekt
Definieren Sie Subnetze und Availability Zones.	Definieren Sie die Subnetze und Availability Zones, die in jeder nicht standardmäßigen VPC verwendet werden.	DevOps Ingenieur, Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dauer: Weniger als eine Woche	
Definieren Sie Sicherheitsgruppen.	Definieren Sie Sicherheitsgruppen und Sicherheitsgruppenregeln für die Steuerung der Sicherheit auf AWS-Ressourcen. Dauer: Weniger als eine Woche	DevOps Ingenieur, Lösungsarchitekt
Definieren Sie Netzwerk-ACLs.	Definieren Sie die Network Access Control Lists (ACLs), um die Sicherheit an den Subnetzgrenzen zu kontrollieren. Dauer: Weniger als eine Woche	DevOps Ingenieur, Lösungsarchitekt

Datenbanken migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbanken vor.	Verwenden Sie AWS DMS, um jede Quelldatenbank für die laufende Replikation in die AWS-Cloud vorzubereiten.	DevOps Ingenieur, Lösungsarchitekt
Erstellen Sie die Datenbanken für die OpenText Kernkomponenten.	Erstellen Sie die Datenbanken, die für die Opentext-TeamSite LiveSite, und MediaBin -Komponenten erforderlich sind. Stellen Sie sicher, dass Benutzer und	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zugriffsrechte gemäß der OpenText Installationsdokumentation korrekt konfiguriert sind.	
Kopieren Sie Daten von Quelldatenbankservern.	Automatisieren Sie den Vorgang des Kopierens von Daten für OpenText Kernkomponenten vom Quelldatenbankserver auf den Zieldatenbankserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Synchronisieren Sie Daten von den Datenbankservern.	Automatisieren Sie den Prozess der regelmäßigen Datensynchronisierung von den Quelldatenbanken zu den Zieldatenbanken.	OpenText Entwickler

Aktivitäten zur Migration von Inhalten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die OpenText TeamSite Inhaltsspeicher.	Automatisieren Sie den Vorgang des Kopierens der Inhaltsspeicher vom OpenText TeamSite Quellserver auf den OpenText TeamSite Zielserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Ordnen Sie Benutzer und Gruppen zu.	Interne Zuordnung von internen OpenText TeamSite Benutzer-IDs zu Zielsystem-IDs.	OpenText führen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synchronisieren Sie die OpenText TeamSite Inhaltsspeicher.	Automatisieren Sie den Prozess der regelmäßigen Synchronisierung von Quell- und Zielinhaltsspeichern. Dies wird im Rahmen des Migrations- und Qualitätssicherungsprozesses implementiert.	OpenText Entwickler
Daten von Webservern kopieren.	Automatisieren Sie den Vorgang des Kopierens von Daten von den Quell-Webservern auf die Ziel-Webserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Synchronisieren Sie die Webserver-Daten.	Automatisieren Sie den Prozess der regelmäßigen Synchronisierung von Quell- und Ziel-Webserverdaten.	OpenText Entwickler
Daten aus dem Dateisystem des Webservers kopieren.	Automatisieren Sie den Vorgang des Kopierens von Inhalten und anderen Web-Assets aus dem Dateisystem des Quell-Webservers auf die Ziel-Webserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Synchronisieren Sie die Dateisysteme des Webservers.	Automatisieren Sie den Prozess der regelmäßigen Synchronisierung von Inhalten und anderen Web-Assets vom Dateisystem des Quell-Webservers mit den Ziel-Webservern.	OpenText Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie Feeds und Indizes.	Automatisieren Sie die Ausführung aller Prozesse, die Feeds oder andere Indizes generieren (z. B. Websuche) , die unsere OpenText TeamSite Webserver-Inhalte als Datenquelle verwenden.	Lösungsarchitekt, OpenText Leiter, Entwickler OpenText
Synchronisieren Sie die Generierung von Feeds und Indizes.	Automatisieren Sie den Prozess der regelmäßigen Neuerstellung von Feeds und Indizes nach Datensync hronisationen.	OpenText Entwickler

Test- und QA-Aktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Migrations-QA durch.	Testen Sie die AWS-Zielu mgebung, -anwendungen und -Services, um sicherzus tellen, dass die automatis ierten Migrationsprozesse korrekt erstellt und konfiguriert sind.	DevOps Ingenieur, OpenText Leiter, QA-Tester
Führen Sie Leistungstests durch.	Testen Sie die Leistung im Hinblick auf Reaktions fähigkeit und Stabilität unter einer bestimmten Arbeitsla st. Untersuchen, messen, validieren oder verifizieren Sie andere Qualitätsmerkmale des Zielsystems, wie Skalierbarkeit und Zuverlässigkeit.	DevOps Ingenieur, OpenText Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Damit dieser Test nützlich ist, müssen Sie über eine Testumgebung verfügen, die dieselbe Größe wie Ihre Produktionsumgebung hat. Dauer: Zwischen einer und zwei Wochen	
Sicherheitstests.	Scannen von Sicherhei tslücken und Penetrationstests zur Aufdeckung potenziel ler Schwachstellen in den Sicherheitsmechanismen einer Anwendung, die Daten schützt und die Funktionalität nach Bedarf aufrechterhält. Damit dieser Test nützlich ist, müssen Sie über eine Testumgebung verfügen, die in Bezug auf Netzwerk und Sicherheit Ihrer Produktio nsumgebung entspricht. Dauer: Zwischen einer und zwei Wochen	DevOps Ingenieur, OpenText Leiter

Aktivitäten zur betrieblichen Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Betriebsb ereitschaft.	Erfahren Sie, wie Sie derzeit IT-Operationen durchführen und wie Sie in der AWS-Cloud arbeiten werden. Sie können	DevOps Ingenieur, OpenText Leiter, Leiter der Servicebe reitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieses Geschäftsergebnis erzielen, indem Sie ein Cloud-Betriebsmodell definieren. Dauer: Eine Woche	
Investieren Sie in die Betriebsautomatisierung.	Investieren Sie in Automatisierung, um ein AWS-Betriebsmodell bereitzustellen.	DevOps Ingenieur, OpenText Leiter, Leiter der Servicebereitstellung
Integrieren Sie den Betrieb.	Verwenden Sie weiterhin aktuelle IT-Tools und erweitern Sie sie durch die Integration in die AWS-Cloud.	DevOps Ingenieur, OpenText Leiter, Leiter der Servicebereitstellung

Umstellungsaktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
DNS wechseln.	Wechseln Sie das Domain Name System (DNS) manuell von vorhandenen Hosts auf Hosts in der AWS-Cloud. Dauer: Eine Stunde	DevOps Ingenieur, OpenText Leiter
Testen Sie die Notfallwiederherstellung.	Testen Sie Disaster Recovery, Backup und Wiederherstellung und führen Sie Ihre automatisierten Tests durch. Dauer: Ein Tag	DevOps Ingenieur, OpenText Leiter, QA-Tester
Validieren Sie Überwachung und Analyse.	Stellen Sie sicher, dass die Überwachung und Analyse funktionieren.	DevOps Ingenieur, OpenText Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dauer: Zwei Stunden	
Schalten Sie die alte Umgebung aus und fordern Sie das Herunterfahren des Servers an.	Dauer: Drei Tage	DevOps Ingenieur, OpenText Leiter

Zugehörige Ressourcen

- Kundenverwaltete Richtlinien
- Einen IAM-Benutzer in Ihrem AWS-Konto erstellen
- IAM-Benutzergruppen
- Einer IAM-Benutzergruppe eine Richtlinie zuordnen
- Überwachung Ihrer Nutzung und Kosten
- Verwaltung eines AWS-Kontos
- IAM-Rollen für Amazon EC2
- Zugriffsberechtigungen für den AWS-Support
- Verwenden von Create-Trail
- Aktivierung der Integritätsprüfung der Protokolldatei für CloudTrail
- Amazon S3 S3-Bucket-Richtlinie für CloudTrail
- Ereignisse an CloudWatch Logs senden
- AWS Config mit der AWS-CLI einrichten
- Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und -Objekte
- Konfiguration von AWS KMS KMS-Schlüsselrichtlinien für CloudTrail
- Verschlüsselung von CloudTrail Protokolldateien mit verwalteten AWS KMS KMS-Schlüsseln (SSE-KMS)
- Wie aktiviere und deaktiviere ich die automatische Schlüsselrotation
- So erhalten Sie Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS-Kontos verwendet werden
- Ein Flow-Protokoll erstellen
- Sicherheitsgruppen für Ihre VPC

- Aktualisierung Ihrer Routentabellen für eine VPC-Peering-Verbindung

Migrieren von Oracle CLOB-Werten zu einzelnen Zeilen in PostgreSQL in AWS

Erstellt von Sai Krishna Namburu (AWS) und Sindhusha Paturu (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: Aurora PostgreSQL – kompatibel oder Amazon RDS für PostgreSQL
R-Typ: Plattformwechsel	Workload: Oracle; Open-Source	Technologien: Migration; Speicher und Backup; Datenbanken
AWS-Services: Amazon Aurora; AWS DMS; Amazon S3; Amazon RDS		

Übersicht

Dieses Muster beschreibt, wie Sie Oracle-Werte für Zeichengrößenobjekte (CLOB) in einzelne Zeilen in Amazon Aurora PostgreSQL -kompatible Edition und Amazon Relational Database Service (Amazon RDS) für PostgreSQL aufteilen. PostgreSQL unterstützt den Datentyp CLOB nicht.

Tabellen mit Intervallpartitionen werden in der Oracle-Quelldatenbank identifiziert, und der Tabellenname, der Partitionstyp, das Intervall der Partition und andere Metadaten werden erfasst und in die Zieldatenbank geladen. Sie können CLOB-Daten mit einer Größe von weniger als 1 GB als Text in Zieltabellen laden, indem Sie AWS Database Migration Service (AWS DMS) verwenden, oder Sie können die Daten im CSV-Format exportieren, in einen Amazon Simple Storage Service (Amazon S3)-Bucket laden und in Ihre PostgreSQL-Zieldatenbank migrieren.

Nach der Migration können Sie den benutzerdefinierten PostgreSQL-Code verwenden, der mit diesem Muster bereitgestellt wird, um die CLOB-Daten basierend auf der neuen Zeilenzeichen-ID (`CHR(10)`) in einzelne Zeilen aufzuteilen und die Zieltabelle zu füllen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Datenbanktabelle mit Intervallpartitionen und Datensätzen mit einem CLOB-Datentyp.
- Eine Datenbank von Aurora PostgreSQL -kompatibel oder Amazon RDS für PostgreSQL mit einer Tabellenstruktur, die der Quelltabelle ähnelt (die gleichen Spalten und Datentypen).

Einschränkungen

- Der CLOB-Wert darf 1 GB nicht überschreiten.
- Jede Zeile in der Zieltabelle muss eine neue Zeilenzeichen-ID haben.

Produktversionen

- Oracle 12c
- Aurora Postgres 11.6

Architektur

Das folgende Diagramm zeigt eine Oracle-Quelltabelle mit CLOB-Daten und die entsprechende PostgreSQL-Tabelle in Aurora PostgreSQL – kompatible Version 11.6.

Tools

AWS-Services

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

Sie können die folgenden Client-Tools verwenden, um eine Verbindung zu Ihren Datenbanken von Aurora PostgreSQL – kompatibel und Amazon RDS für PostgreSQL herzustellen, darauf zuzugreifen und diese zu verwalten. (Diese Tools werden in diesem Muster nicht verwendet.)

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.
- DBeaver ist ein Open-Source-Datenbank-Tool für Entwickler und Datenbankadministratoren. Sie können das Tool verwenden, um Ihre Daten zu bearbeiten, zu überwachen, zu analysieren, zu verwalten und zu migrieren.

Bewährte Methoden

Bewährte Methoden für die Migration Ihrer Datenbank von Oracle zu PostgreSQL finden Sie im AWS-Blogbeitrag Bewährte Methoden für die Migration einer Oracle-Datenbank zu Amazon RDS PostgreSQL oder Amazon Aurora PostgreSQL: Überlegungen zum Migrationsprozess und zur Infrastruktur.

Bewährte Methoden für die Konfiguration der AWS DMS-Aufgabe für die Migration großer binärer Objekte finden Sie unter Migrieren großer binärer Objekte (LOBs) in der AWS DMS-Dokumentation.

Polen

Identifizieren der CLOB-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die CLOB-Daten.	Analysieren Sie in der Oracle-Quelldatenbank die CLOB-Daten, um festzustellen, ob sie Spaltenüberschriften enthalten , sodass Sie die Methode zum Laden der Daten in die Zieltabelle ermitteln können. Verwenden Sie die folgende Abfrage, um die Eingabedaten zu analysieren.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SELECT * FROM clobdata_or;`	
Laden Sie die CLOB-Daten in die Zieldatenbank.	Migrieren Sie die Tabelle mit CLOB-Daten in eine Zwischentabelle (Staging) in der Aurora- oder Amazon RDS-Zieldatenbank. Sie können AWS DMS verwenden oder die Daten als CSV-Datei in einen Amazon S3-Bucket hochladen. Informationen zur Verwendung von AWS DMS für diese Aufgabe finden Sie unter Verwenden einer Oracle-Datenbank als Quelle und Verwenden einer PostgreSQL-Datenbank als Ziel in der AWS DMS-Dokumentation. Informationen zur Verwendung von Amazon S3 für diese Aufgabe finden Sie unter Verwenden von Amazon S3 als Ziel in der AWS DMS-Dokumentation.	Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Validieren Sie die PostgreSQL-Zieltabelle.	Validieren Sie die Zieldaten, einschließlich der Header, anhand der Quelldaten, indem Sie die folgenden Abfragen in der Zieldatenbank verwenden.
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
	Vergleichen Sie die Ergebnisse mit den Abfrageergebnissen aus der Quelldatenbank (aus dem ersten Schritt).
		Developer

Teilen Sie die CLOB-Daten in separate Zeilen auf.	Führen Sie den benutzerdefinierten PostgreSQL-Code aus, der im Abschnitt Zusätzliche Informationen bereitgestellt wird, um die CLOB-Daten aufzuteilen und in separate Zeilen in der PostgreSQL-Zieltabelle einzufügen.	Developer

Validieren Sie die Daten.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten in der Zieltabelle.	Validieren Sie die in die Zieltabelle eingefügten Daten mithilfe der folgenden Abfragen.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SELECT * FROM clobdata_pg;` `SELECT * FROM clobdatatarget;`	

Zugehörige Ressourcen

- CLOB-Datentyp (Oracle-Dokumentation)
- Datentypen (PostgreSQL-Dokumentation)

Zusätzliche Informationen

PostgreSQL-Funktion zum Aufteilen von CLOB-Daten

```
do
$$
declare
totalstr varchar;
str1 varchar;
str2 varchar;
pos1 integer := 1;
pos2 integer ;
len integer;


begin
        select rawdata||chr(10) into totalstr from clobdata_pg;
        len :=  length(totalstr) ;
        raise notice 'Total length : %',len;
        raise notice 'totalstr : %',totalstr;
        raise notice 'Before while loop';


        while pos1 < len  loop


                select position (chr(10) in totalstr) into pos2;
```

```
                 raise notice '1st position of new line : %',pos2;


                str1 := substring (totalstr,pos1,pos2-1);
                raise notice 'str1 : %',str1;


                   insert into clobdatatarget(data) values (str1);
                   totalstr := substring(totalstr,pos2+1,len);
                   raise notice 'new totalstr :%',totalstr;
                len :=  length(totalstr) ;


        end loop;
end
$$
LANGUAGE 'plpgsql' ;
```

Ein- und Ausgabebeispiele

Sie können die folgenden Beispiele verwenden, um den PostgreSQL-Code auszuprobieren, bevor Sie Ihre Daten migrieren.

Erstellen Sie eine Oracle-Datenbank mit drei Eingabezeilen.

```
CREATE TABLE clobdata_or (
id INTEGER GENERATED ALWAYS AS IDENTITY,
rawdata clob  );


insert into clobdata_or(rawdata) values (to_clob('test line 1') || chr(10) ||
 to_clob('test line 2') || chr(10) || to_clob('test line 3') || chr(10));
COMMIT;


SELECT * FROM clobdata_or;
```

Dadurch wird die folgende Ausgabe angezeigt.

id	Rohdaten
1	Testlinie 1 Testlinie 2 Testlinie 3

Laden Sie die Quelldaten `clobdata_pg`zur Verarbeitung in eine PostgreSQL-Staging-Tabelle ().

```
SELECT * FROM clobdata_pg;

CREATE TEMP TABLE clobdatatarget (id1 SERIAL,data VARCHAR );

<Run the code in the additional information section.>

SELECT * FROM clobdatatarget;
```

Dadurch wird die folgende Ausgabe angezeigt.

id1	data
1	Testlinie 1
2	Testlinie 2
3	Testlinie 3

Migrieren einer On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle mithilfe des direkten Oracle Data Pump Imports über einen Datenbanklink

Erstellt von Rizwan Wangde (AWS)

Umgebung: Produktion	Quelle: On-Premises-Oracle-Datenbank	Ziel: Amazon RDS für Oracle
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; AWS Direct Connect; Amazon RDS		

Übersicht

Zahlreiche Muster umfassen die Migration von lokalen Oracle-Datenbanken zu Amazon RDS für Oracle mithilfe von Oracle Data Pump, einem nativen Oracle-Dienstprogramm, das die bevorzugte Methode für die Migration großer Oracle-Workloads darstellt. Zu diesen Mustern gehören in der Regel das Exportieren von Anwendungsschemata oder Tabellen in Dumpdateien, das Übertragen der Dumpdateien in ein Datenbankverzeichnis auf Amazon RDS für Oracle und das anschließende Importieren der Anwendungsschemata und Daten aus den Dumpdateien.

Bei diesem Ansatz kann eine Migration je nach Größe der Daten und benötigter Zeit für die Übertragung der Dump-Dateien auf die Amazon-RDS-Instance länger dauern. Darüber hinaus befinden sich die Dump-Dateien auf dem Amazon Elastic Block Store (Amazon EBS)-Volume der Amazon-RDS-Instance, das für die Datenbank und die Dump-Dateien groß genug sein muss. Wenn die Dump-Dateien nach dem Import gelöscht werden, kann der leere Speicherplatz nicht abgerufen werden, sodass Sie weiterhin für ungenutzten Speicherplatz bezahlen.

Dieses Muster behebt diese Probleme, indem es einen direkten Import auf der Amazon-RDS-Instance durchführt, indem die Oracle Data Pump API (`DBMS_DATAPUMP`) über einen Datenbanklink verwendet wird. Das Muster initiiert eine gleichzeitige Export- und Importpipeline zwischen der Quell- und der Zieldatenbank. Dieses Muster erfordert keine Größenanpassung eines EBS-Volumes für die Dump-Dateien, da keine Dump-Dateien auf dem Volume erstellt oder gespeichert werden. Dieser Ansatz spart die monatlichen Kosten für ungenutzten Speicherplatz.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto.
- Eine Virtual Private Cloud (VPC), die mit privaten Subnetzen in mindestens zwei Availability Zones konfiguriert ist, um die Netzwerkinfrastruktur für die Amazon-RDS-Instance bereitzustellen.
- Eine Oracle-Datenbank in einem On-Premises-Rechenzentrum.
- Eine vorhandene Amazon RDS Oracle-Instance in einer einzigen Availability Zone. Die Verwendung einer einzigen Availability Zone verbessert die Schreibleistung während der Migration. Eine Multi-AZ-Bereitstellung kann 24–48 Stunden vor dem Cutover aktiviert werden.
- AWS Direct Connect (empfohlen für große Datenbanken).
- Netzwerkkonnektivität und Firewallregeln On-Premises, die so konfiguriert sind, dass eine eingehende Verbindung von der Amazon-RDS-Instance zur On-Premises-Oracle-Datenbank zugelassen wird.

Einschränkungen

- Die Datenbankgrößenbeschränkung auf Amazon RDS für Oracle beträgt 64 TiB (ab Dezember 2022).

Produktversionen

- Quelldatenbank: Oracle Database Version 10g Release 1 und höher.
- Zieldatenbank: Die neueste Liste der unterstützten Versionen und Editionen in Amazon RDS finden Sie unter Amazon RDS for Oracle in der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Selbstverwaltete Oracle-Datenbank On-Premises oder in der Cloud

Zieltechnologie-Stack

- Amazon RDS für Oracle

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für die Migration von einer On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle in einer Single-AZ-Umgebung. Die Pfeilrichtungen zeigen den Datenfluss in der Architektur. Das Diagramm zeigt nicht, welche Komponente die Verbindung initiiert.

1. Die Amazon RDS for Oracle-Instance stellt eine Verbindung zur lokalen Oracle-Quelldatenbank her, um eine Volllastmigration über den Datenbanklink durchzuführen.
2. AWS DMS stellt eine Verbindung mit der lokalen Oracle-Quelldatenbank her, um mithilfe von Change Data Capture (CDC) eine fortlaufende Replikation durchzuführen.
3. CDC-Änderungen werden auf die Datenbank von Amazon RDS für Oracle angewendet.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen. Dieses Muster verwendet CDC und die Einstellung Nur Datenänderungen replizieren.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein standardmäßiges Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.

Andere Tools

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hohen Geschwindigkeiten von einer Datenbank in eine andere verschieben.
- Client-Tools wie Oracle Instant Client oder SQL Developer werden verwendet, um SQL-Abfragen in der Datenbank zu verbinden und auszuführen.

Bewährte Methoden

Obwohl AWS Direct Connect dedizierte, private Netzwerkverbindungen zwischen dem On-Premises-Netzwerk und AWS verwendet, sollten Sie die folgenden Optionen für zusätzliche Sicherheit und Datenverschlüsselung für Daten während der Übertragung berücksichtigen:

- Ein Virtual Private Network (VPN) mit Amazon Site-to-Site VPN oder einer IPsec VPN-Verbindung vom On-Premises-Netzwerk zum AWS-Netzwerk
- Oracle Database Native Network Encryption, konfiguriert in der lokalen Oracle-Datenbank
- Verschlüsselung mit TLS

Sekunden

Vorbereiten der lokalen Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Netzwerkk onnektivität von der Zieldaten bank zur Quelldatenbank ein.	Konfigurieren Sie das On-Premises-Netzwerk und die Firewall, um eingehend e Verbindungen von der Amazon RDS-Ziel-Instance zur lokalen Oracle-Qu elldatenbank zuzulassen.	Netzwerkadministrator, Sicherheitsingenieur

Erstellen Sie einen Datenbank benutzer mit den entsprech enden Berechtigungen.	Erstellen Sie einen Datenbank benutzer in der lokalen Oracle-Quelldatenbank mit Berechtig ungen zum Migrieren von Daten zwischen Quelle und Ziel mithilfe von Oracle Data Pump.
	`GRANT CONNECT to <migration_user>;`
	`GRANT DATAPUMP_EXP_FULL_DATABASE to <migration_user>;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`GRANT SELECT ANY TABLE to <migration_user>;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereiten Sie die On-Premises-Quelldatenbank für die AWS DMS-CDC-Migration vor.	(Optional) Bereiten Sie die lokale Oracle-Quelldatenbank nach Abschluss von Oracle Data Pump Full Load für die AWS DMS-CDC-Migration vor:
	1. Konfigurieren Sie die zusätzlichen Berechtigungen, die für die Verwaltung von FLASHBACK während der Oracle Data Pump-Migration erforderlich sind.
	`GRANT FLASHBACK ANY TABLE to <migration_user>;`
	`GRANT FLASHBACK ARCHIVE ADMINISTER to <migration_user>;`
	2. Informationen zum Konfigurieren der erforderlichen Benutzerkontoberechtigungen für eine selbstverwaltete Oracle-Quelle für AWS DMS finden Sie in der AWS DMS-Dokumentation.
	3. Informationen zur Vorbereitung einer selbstverwalteten Oracle-Quelldatenbank für CDC mit AWS DMS finden Sie in der AWS DMS-Dokumentation.
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie SQL Developer.	Installieren und konfigurieren Sie SQL Developer, um SQL-Abfragen in den Quell- und Zieldatenbanken zu verbinden und auszuführen.	DBA, Migrationsingenieur
Generieren Sie ein Skript, um die Tabellenbereiche zu erstellen.	Verwenden Sie die folgende Beispiel-SQL-Abfrage, um das Skript in der Quelldatenbank zu generieren. `SELECT 'CREATE TABLESPACE ' tablespace_name ' DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE UNLIMITED;' from dba_tablespaces where tablespace_name not in ('SYSTEM', 'SYSAUX','TEMP','UNDOTBS1') order by 1;` Das Skript wird auf die Zieldatenbank angewendet.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie ein Skript, um Benutzer, Profile, Rollen und Berechtigungen zu erstellen.	Um ein Skript zum Erstellen der Datenbankbenutzer, Profile, Rollen und Berechtigungen zu generieren, verwenden Sie die Skripts aus dem Oracle Support-Dokument So extrahieren Sie DDL für Benutzer einschließlich Berechtigungen und Rollen mit dbms_metadata.get_ddl (Dokument-ID 2739952.1) (Oracle-Konto erforderlich). Das Skript wird auf die Zieldatenbank angewendet.	DBA

Vorbereiten der Ziel-Instance von Amazon RDS für Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Datenbanklink zur Quelldatenbank und überprüfen Sie die Konnektivität.	Um einen Datenbanklink zur On-Premises-Quelldatenbank zu erstellen, können Sie den folgenden Beispielbefehl verwenden. `CREATE DATABASE LINK link2src CONNECT TO <migration_user_account> IDENTIFIED BY <password> USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	or ip address of remote db>) (PORT=<listener port>))(CONNECT_DATA=(SID=<remote SID>)))'; Führen Sie den folgenden SQL-Befehl aus, um die Konnektivität zu überprüfen. select * from dual@link2src; Die Konnektivität ist erfolgreich, wenn die Antwort lautetX.	
Führen Sie die Skripts aus, um die Ziel-Instance vorzubereiten.	Führen Sie die zuvor generierten Skripts aus, um die Ziel-Instance von Amazon RDS für Oracle vorzubereiten: 1. Tablespaces 2. Profile 3. Rollen Dadurch wird sichergestellt, dass die Oracle Data Pump-Migration die Schemata und ihre Objekte erstellen kann.	DBA, Migrationsingenieur

Durchführen einer Volllastmigration mithilfe von Oracle Data Pump Import über einen Datenbanklink

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die erforderl ichen Schemata.	Um die erforderlichen Schemata von der On-Premis es-Quelldatenbank zur Amazon-RDS-Ziel-Instance zu migrieren, verwenden Sie den Code im Abschnitt Zusätzliche Informationen: • Um ein einzelnes Schema zu migrieren, führen Sie Code 1 im Abschnitt Zusätzliche Informationen aus. • Um mehrere Schemata zu migrieren, führen Sie Code 2 im Abschnitt Zusätzliche Informationen aus. Um die Leistung der Migration zu optimieren, können Sie die Anzahl der parallelen Prozesse anpassen, indem Sie den folgenden Befehl ausführen. `DBMS_DATAPUMP.SET_ PARALLEL (handle => v_hdnl, degree => 4);`	DBA
Erfassen Sie Schemasta tistiken, um die Leistung zu verbessern.	Der Befehl Gather Schema Statistics gibt die für Datenbankobjekte gesammelt en Statistiken des Oracle-	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abfrageoptimierers zurück. Mithilfe dieser Informationen kann der Optimierer den besten Ausführungsplan für jede Abfrage für diese Objekte auswählen. `EXECUTE DBMS_STAT S.GATHER_SCHEMA_ST ATS(ownname => '<schema_name>');`	

Durchführen einer Volllastmigration und CDC-Replikation mithilfe von Oracle Data Pump und AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie die SCN in der lokalen Oracle-Quelldatenbank.	Erfassen Sie die Systemänderungsnummer (SCN) in der lokalen Oracle-Quelldatenbank. Sie verwenden die SCN für den Volllastimport und als Ausgangspunkt für die CDC-Replikation. Um die aktuelle SCN in der Quelldatenbank zu generieren, führen Sie die folgende SQL-Anweisung aus. `SELECT current_scn FROM V$DATABASE;`	DBA
Führen Sie die Volllastmigration der Schemata durch.	Gehen Sie wie folgt vor, um die erforderlichen Schemata	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(FULL LOAD) von der On-Premises-Quelldatenbank zur Amazon-RDS-Ziel-Instance zu migrieren: • Um ein einzelnes Schema zu migrieren, führen Sie Code 3 im Abschnitt Zusätzliche Informationen aus. • Um mehrere Schemata zu migrieren, führen Sie Code 4 im Abschnitt Zusätzliche Informationen aus. Ersetzen Sie im Code durch <CURRENT_SCN_VALUE _IN_SOURCE_DATABAS E> die SCN, die Sie aus der Quelldatenbank erfasst haben. `DBMS_DATAPUMP.SET_ PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value => <CURRENT_SCN_VALUE _IN_SOURCE_DATABAS E>);` Um die Leistung der Migration zu optimieren, können Sie die Anzahl der parallelen Prozesse anpassen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	
Deaktivieren Sie die Auslöser unter den migrierten Schemata.	Bevor Sie mit der reinen AWS DMS-CDC-Aufgabe beginnen, deaktivieren Sie `TRIGGERS` unter den migrierten Schemata.	DBA
Erfassen Sie Schemastatistiken, um die Leistung zu verbessern.	Der Befehl Gather Schema Statistics gibt die für Datenbankobjekte gesammelten Statistiken des Oracle-Abfrageoptimierers zurück. Mithilfe dieser Informationen kann der Optimierer den besten Ausführungsplan für jede Abfrage für diese Objekte auswählen. `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS DMS, um eine fortlaufende Replikation von der Quelle zum Ziel durchzuführen.	Verwenden Sie AWS DMS, um eine fortlaufende Replikation von der Oracle-Quelldatenbank zur Amazon RDS for Oracle-Ziel-Instance durchzuführen. Weitere Informationen finden Sie unter Erstellen von Aufgaben für die laufende Replikation mit AWS DMS und im Blogbeitrag So arbeiten Sie mit nativer CDC-Unterstützung in AWS DMS.	DBA, Migrationsingenieur

Umstellung auf Amazon RDS für Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Multi-AZ auf der Instance 48 Stunden vor dem Cutover.	Wenn es sich um eine Produktions-Instance handelt, empfehlen wir, die Multi-AZ-Bereitstellung auf der Amazon-RDS-Instance zu aktivieren, um die Vorteile von Hochverfügbarkeit (HA) und Notfallwiederherstellung (DR) zu nutzen.	DBA, Migrationsingenieur
Stoppen Sie die reine AWS DMS-CDC-Aufgabe (wenn CDC aktiviert war).	1. Stellen Sie sicher, dass die Quelllatenz und die Ziellatenz für die Amazon-CloudWatch Metriken der AWS DMS-Aufgabe 0 Sekunden anzeigen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Stoppen Sie die reine AWS DMS-CDC-Aufgabe.	
Aktivieren Sie die Auslöser.	Aktivieren Sie die TRIGOREN, die Sie deaktiviert haben, bevor die CDC-Aufgabe erstellt wurde.	DBA

Zugehörige Ressourcen

AWS

- Vorbereiten einer selbstverwalteten Oracle-Quelldatenbank für CDC mit AWS DMS
- Erstellen von Aufgaben für die fortlaufende Replikation mit AWS DMS
- Multi-AZ-Bereitstellungen für hohe Verfügbarkeit
- So arbeiten Sie mit nativer CDC-Unterstützung in AWS DMS (Blogbeitrag)

Oracle-Dokumentation

- DBMS_DATAPUMP

Zusätzliche Informationen

Code 1: nur Volllastmigration, Einzelanwendungsschema

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')'); --
 To prevent gathering Statistics during the import
```

```
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Code 2: nur Volllastmigration, mehrere Anwendungsschemata

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Code 3: Volllastmigration vor reine CDC-Aufgabe, Einzelanwendungsschema

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
```

```
END;
/
```

Code 4: Volllastmigration vor reine CDC-Aufgabe, mehrere Anwendungsschemata

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN (operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE (handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Szenario, in dem ein gemischter Migrationsansatz besser funktionieren kann

In seltenen Szenarien, in denen die Quelldatenbank Tabellen mit Millionen von Zeilen und sehr großen LOBSEGMENT-Spalten enthält, verlangsamt dieses Muster die Migration. Oracle migriert LOBSEGMENTs nacheinander über die Netzwerkverbindung. Es extrahiert eine einzelne Zeile (zusammen mit den LOB-Spaltendaten) aus der Quelltabelle und fügt die Zeile in die Zieltabelle ein, wobei der Vorgang wiederholt wird, bis alle Zeilen migriert sind. Oracle Data Pump über die Datenbankverbindung unterstützt keine Massenlade- oder Direktpfadlademechanismen für LOBSEGMENTs.

In diesem Fall empfehlen wir Folgendes:

- Überspringen Sie die identifizierten Tabellen während der Oracle Data Pump-Migration, indem Sie den folgenden Metadatenfilter hinzufügen.

```
dbms_datapump.metadata_filter(handle =>h1, name=>'NAME_EXPR', value => 'NOT IN
 (''TABLE_1'',''TABLE_2'')');
```

- Verwenden Sie eine AWS DMS-Aufgabe (Migration mit vollständigem Ladevorgang, bei Bedarf mit CDC-Replikation), um die identifizierten Tabellen zu migrieren. AWS DMS extrahiert mehrere Zeilen aus der Oracle-Quelldatenbank und fügt sie in einem Stapel in die Amazon RDS-Ziel-Instance ein, was die Leistung verbessert.

Migrieren der Oracle E-Business Suite zu Amazon RDS Custom

Erstellt von Cunningham (AWS), Jaydeep Nandy (AWS), Nitin Saxena (AWS) und Vishnu Vinnakota (AWS)

Umgebung: Produktion	Quelle: Amazon EC2 oder On-Premises	Ziel: Amazon RDS Custom
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken; Infrastruktur
AWS-Services: Amazon EFS; Amazon RDS; AWS Secrets Manager		

Übersicht

Oracle E-Business Suite ist eine Enterprise Resource Planning (ERP)-Lösung zur Automatisierung unternehmensweiter Prozesse wie Finanzen, Personalwesen, Lieferketten und Fertigung. Es verfügt über eine dreistufige Architektur: Client, Anwendung und Datenbank. Zuvor mussten Sie Ihre Oracle E-Business Suite-Datenbank auf einer selbstverwalteten Amazon Elastic Compute Cloud (Amazon EC2)-Instance ausführen, aber Sie können jetzt von Amazon Relational Database Service (Amazon RDS) Custom profitieren.

Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Es automatisiert Aufgaben und Vorgänge der Datenbankverwaltung und ermöglicht Ihnen als Datenbankadministrator den Zugriff auf Ihre Datenbankumgebung und Ihr Betriebssystem. Wenn Sie Ihre Oracle-Datenbank zu Amazon RDS Custom migrieren, kümmert sich Amazon Web Services (AWS) um die Hauptarbeit, wie z. B. Backup-Aufgaben und die Sicherstellung einer hohen Verfügbarkeit, während Sie sich auf die Wartung Ihrer Oracle-E-Business-Suite-Anwendung und -Funktionalität konzentrieren können. Die wichtigsten Faktoren, die bei einer Migration zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster konzentriert sich auf die Schritte zur Migration einer eigenständigen Oracle-Datenbank auf Amazon EC2 zu Amazon RDS Custom mithilfe eines Oracle Recovery Manager (RMAN)-

Backups und eines gemeinsam genutzten Dateisystems von Amazon Elastic File System (Amazon EFS) zwischen der EC2-Instance und Amazon RDS Custom. Das Muster verwendet ein vollständiges RMAN-Backup (manchmal auch als Level-0-Backup bezeichnet). Der Einfachheit halber wird ein Cold-Backup verwendet, bei dem die Anwendung heruntergefahren wird und die Datenbank gemountet und nicht geöffnet wird. (Sie können auch Oracle Data Guard oder RMAN-Duplikation für Backups verwenden. Dieses Muster deckt diese Optionen jedoch nicht ab.)

Informationen zum Entwerfen von Oracle E-Business Suite in AWS für Hochverfügbarkeit und Notfallwiederherstellung finden Sie im Muster Einrichten einer HA/DR-Architektur für Oracle E-Business Suite in Amazon RDS Custom mit einer aktiven Standby-Datenbank.

Hinweis: Dieses Muster enthält Links zu Oracle-Supporthinweisen. Sie benötigen ein Oracle Support-Konto, um auf diese Dokumente zugreifen zu können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Quelldatenbank der Version 12.1.0.2 oder 19c (mindestens 19.3), die auf Amazon EC2 mit Oracle Linux 7 oder Red Hat Enterprise Linux (RHEL) Version 7.x ausgeführt wird. Bei diesem Muster wird davon ausgegangen, dass der Name der Quelldatenbank lautet `VIS` und dass der zusätzliche Name der Containerdatenbank für Oracle 19c lautet`VISCDB`. Sie können jedoch auch andere Namen verwenden.

  Hinweis: Sie können dieses Muster auch mit lokalen Oracle-Quelldatenbanken verwenden, sofern Sie über die entsprechende Netzwerkkonnektivität zwischen dem On-Premises-Netzwerk und Amazon Virtual Private Cloud (Amazon VPC) verfügen.
- Eine Oracle E-Business Suite Version 12.2.x-Anwendung (vision-Instance). Dieses Verfahren wurde mit Version 12.2.11 getestet.
- Eine einzelne Oracle E-Business Suite-Anwendungsebene. Sie können dieses Muster jedoch so anpassen, dass es mit mehreren Anwendungsebenen funktioniert.
- Für Oracle 12.1.0.2 ist Amazon RDS Custom mit mindestens 16 GB Auslagerungsbereich konfiguriert. Andernfalls zeigt die CD „12c Examples“ eine Warnung an. (Oracle 19c benötigt die Beispiel-CD nicht, wie später in diesem Dokument erwähnt.)

Führen Sie die folgenden Schritte aus, bevor Sie mit der Migration beginnen:

1. Erstellen Sie in der Amazon-RDS-Konsole eine DB-Instance von Amazon RDS Custom für Oracle mit dem Datenbanknamen `VIS` (oder Ihrem Quelldatenbanknamen). Anweisungen finden Sie unter Arbeiten mit Amazon RDS Custom in der AWS-Dokumentation und im Blogbeitrag Amazon RDS Custom for Oracle – Neue Kontrollfunktionen in der Datenbankumgebung. Dadurch wird sichergestellt, dass der Datenbankname auf denselben Namen wie die Quelldatenbank festgelegt ist. (Wenn das Feld leer gelassen wird, werden die EC2-Instance und der Datenbankname auf gesetzt`ORCL`.) Stellen Sie sicher, dass Sie Ihre benutzerdefinierte Engine-Version (CEV) mit den Patches erstellen, die mindestens auf die Quelle angewendet wurden. Weitere Informationen finden Sie unter Vorbereiten der Erstellung einer CEV in der Amazon-RDS-Dokumentation.

   Hinweis für Oracle 19c: Derzeit kann für Oracle 19c der Name der Amazon-RDS-Containerdatenbank angepasst werden. Der Standardwert ist `RDSCDB`. Stellen Sie sicher, dass Sie die RDS Custom Oracle-Instance mit derselben System-ID (SID) wie auf der EC2-Quell-Instance erstellen. In diesem Muster wird beispielsweise davon ausgegangen, dass sich die Oracle 19c SID `VISCDB` auf der Quell-Instance befindet. Daher sollte die Ziel-Oracle-19c-SID auf Amazon RDS Custom ebenfalls lauten`VISCDB`.
2. Konfigurieren Sie die Amazon-RDS-Custom-DB-Instance mit genügend Speicher, vCPU und Arbeitsspeicher, um mit der Amazon EC2Quelldatenbank übereinzustimmen. Dazu können Sie die Amazon EC2-Instance-Typen basierend auf vCPU und Arbeitsspeicher abgleichen.
3. Erstellen Sie ein Amazon-EFS-Dateisystem und mounten Sie es auf den Amazon EC2- und Amazon-RDS-Custom-Instances. Anweisungen finden Sie im Blogbeitrag Integrate Amazon RDS Custom for Oracle with Amazon EFS. Bei diesem Muster wird davon ausgegangen, dass Sie das Amazon-EFS-Volume sowohl auf den Amazon EC2-Quell- als auch `/RMAN` auf den Amazon-RDS-Custom-DB-Instances gemountet haben und dass Netzwerkkonnektivität zwischen Quelle und Ziel möglich ist. Sie können dieselbe Methode auch verwenden, indem Sie Amazon FSx oder ein beliebiges freigegebenes Laufwerk verwenden.

Annahmen

Bei diesem Muster wird davon ausgegangen, dass Ihre Anwendung und Datenbank logische Hostnamen verwenden, wodurch die Anzahl der Migrationsschritte reduziert wird. Sie können diese Schritte anpassen, um physische Hostnamen zu verwenden, aber logische Hostnamen reduzieren die Komplexität des Migrationsprozesses. Informationen zu den Vorteilen der Verwendung logischer Hostnamen finden Sie in den folgenden Supporthinweisen:

- Für 12c Oracle Support Note 2246690.1
- Für 19c Oracle Support Note 2617788.1

Dieses Muster deckt das Upgrade-Szenario von Oracle 12c auf 19c nicht ab und konzentriert sich auf die Migration derselben Version der Oracle-Datenbank, die auf Amazon EC2 ausgeführt wird, zu Amazon RDS Custom für Oracle.

Amazon RDS Custom für Oracle unterstützt Oracle Home-Anpassungen. (Oracle Home speichert die Oracle-Binärdateien.) Sie können den Standardpfad von `/rdsdbbin/oracle` zu einem von Ihnen angegebenen Pfad ändern, z. B. `/d01/oracle/VIS/19c`. Der Einfachheit halber wird bei den Anweisungen in diesem Muster der Standardpfad verwendet`/rdsdbbin/oracle`.

Einschränkungen

Dieses Muster unterstützt die folgenden Funktionen und Konfigurationen nicht:

- Festlegen des `ARCHIVE_LAG_TARGET` Datenbankparameters auf einen Wert außerhalb des Bereichs von 60–7200
- Deaktivieren des DB-Instance-Protokollmodus (`NOARCHIVELOG`)
- Deaktivieren des `EBS-optimized` Attributs der EC2-Instance
- Ändern der ursprünglichen Amazon Elastic Block Store (Amazon EBS)-Volumes, die an die EC2-Instance angefügt sind
- Hinzufügen neuer EBS-Volumes oder Ändern des Volume-Typs von `gp2` zu`gp3`
- Unterstützung für das TNS-ifile
- Ändern des `control_file` Speicherorts und des Namens (es muss sein`/rdsdbdata/db/VISCDB_A/controlfile/control-01.ctl`, wobei der CDB-Name `VISCDB` ist)

Weitere Informationen zu diesen und anderen nicht unterstützten Konfigurationen finden Sie unter Behebung nicht unterstützter Konfigurationen in der Amazon-RDS-Dokumentation.

Produktversionen

Informationen zu Oracle-Database-Versionen und Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Verfügbarkeit und Anforderungen für Amazon RDS Custom für Oracle.

Architektur

Das folgende Architekturdiagramm stellt ein Oracle E-Business Suite-System dar, das in einer einzigen Availability Zone auf AWS ausgeführt wird. Auf die Anwendungsebene wird über einen

Application Load Balancer zugegriffen, sowohl die Anwendung als auch die Datenbanken befinden sich in privaten Subnetzen, und die Datenbankebene von Amazon RDS Custom und Amazon EC2 verwendet ein gemeinsam genutztes Amazon-EFS-Dateisystem, um die RMAN-Sicherungsdateien zu speichern und darauf zuzugreifen.

Tools

AWS-Services

- Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und gepackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Es automatisiert Aufgaben und Vorgänge der Datenbankverwaltung und ermöglicht Ihnen als Datenbankadministrator den Zugriff auf Ihre Datenbankumgebung und Ihr Betriebssystem.
- Amazon Elastic File System (Amazon EFS)ist ein einfaches, Serverless-Elastic-Dateisystem zum Hinzufügen und Entfernen von Dateien, ohne dass eine Verwaltung oder Bereitstellung erforderlich ist. Dieses Muster verwendet ein gemeinsam genutztes Amazon-EFS-Dateisystem, um die RMAN-Sicherungsdateien zu speichern und darauf zuzugreifen.
- AWS Secrets Manager ist ein von AWS verwalteter Service, mit dem Sie Datenbankanmeldeinformationen, API-Schlüssel und andere geheime Informationen einfach rotieren, verwalten und abrufen können. Amazon RDS Custom speichert das Schlüsselpaar und die Anmeldeinformationen des Datenbankbenutzers bei der Datenbankerstellung in Secrets Manager. In diesem Muster rufen Sie die Datenbankbenutzerpasswörter von Secrets Manager ab, um die - `RDSADMIN` und -`ADMIN`Benutzer zu erstellen und die Syss- und Systempasswörter zu ändern.

Andere Tools

- RMAN ist ein Tool, das Backup- und Wiederherstellungsunterstützung für Oracle-Datenbanken bietet. Dieses Muster verwendet RMAN, um ein Cold-Backup der Oracle-Quelldatenbank auf Amazon EC2 durchzuführen, das auf Amazon RDS Custom wiederhergestellt wird.

Bewährte Methoden

- Verwenden Sie logische Hostnamen. Dadurch wird die Anzahl der Skripte nach dem Klon erheblich reduziert, die Sie ausführen müssen. Weitere Informationen finden Sie unter Oracle Support Note 2246690.1.
- Amazon RDS Custom verwendet standardmäßig Oracle Automatic Memory Management (AMM). Wenn Sie den Hugem-Kernel verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass stattdessen die automatische gemeinsame Speicherverwaltung (ASMM) verwendet wird.
- Lassen Sie den `memory_max_target` Parameter standardmäßig aktiviert. Das Framework verwendet diesen Parameter im Hintergrund, um Lesereplikate zu erstellen.
- Aktivieren Sie Oracle Flashback Database. Diese Funktion ist in Testszenarien für Failover (keine Umstellung) nützlich, um die Standby-Instance wiederherzustellen.
- Passen Sie für Datenbankinitialisierungsparameter das standardmäßige PFILE an, das von der Amazon RDS Custom DB-Instance für Oracle E-Business Suite bereitgestellt wird, anstatt das SPFILE aus der Oracle-Quelldatenbank zu verwenden. Dies liegt daran, dass Leerzeichen und Kommentare Probleme beim Erstellen von Lesereplikaten in Amazon RDS Custom verursachen. Weitere Informationen zu Datenbankinitialisierungsparametern finden Sie unter Oracle Support Note 396009.1.

Im folgenden Abschnitt „Epics“ haben wir separate Anweisungen für Oracle 12.1.0.2 und 19c bereitgestellt, wobei sich die Details unterscheiden.

Polen

Herunterfahren der Quellanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fahren Sie die Anwendung herunter.	Verwenden Sie die folgenden Befehle, um die Quellanwendung herunterzufahren:
	`$ su - applmgr`
	`$ cd $INST_TOP/admin/scripts`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ ./adstpall.sh`	
Erstellen Sie die ZIP-Datei.	Erstellen Sie die `appsutil.zip` Datei auf der Ebene der Quellanwendung. Sie verwenden diese Datei später, um den Amazon RDS Custom-Datenbankknoten zu konfigurieren. `$ perl $AD_TOP/bin/admkappsutil.pl`	DBA
Kopieren Sie die ZIP-Datei in Amazon EFS .	Kopieren Sie `appsutil.zip` von `$INST_TOP/admin/out` auf Ihr freigegebenes Amazon-EFS-Volume (`/RMAN/appsutil`). Sie können die Datei manuell übertragen, indem Sie Secure Copy (SCP) oder einen anderen Übertragungsmechanismus verwenden.	DBA

Klonen Sie die Quelldatenbank vorab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie die Datenbankebene auf Amazon EC2 vorab.	Melden Sie sich als Oracle-Benutzer an und führen Sie Folgendes aus: `$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ perl adpreclone.pl dbTier` Überprüfen Sie die generierte Protokolldatei, um zu bestätigen, dass der Vorgang erfolgreich abgeschlossen wurde.	

Kopieren Sie appsutil.zip in das freigegebene Amazon-EFS-Dateisystem.	Erstellen Sie ein tar-Backup und kopieren Sie `$ORACLE_HOME/appsutil` es in das gemeinsam genutzte Amazon EFS-Dateisystem (z. B. `/RMAN/appsutil`):
	
	`$ cd $ORACLE_HOME`
	`$ tar cvf sourceappsutil.tar appsutil`
	`$ cp sourceappsutil.tar /RMAN/appsutil`
		DBA

Führen Sie ein Cold-RMAN-Voll-Backup der Amazon EC2Quelldatenbank durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Backup-Skript.	Führen Sie eine vollständige RMAN-Sicherung der Quelldatenbank auf dem freigegebenen Amazon-EFS-Dateisystem durch. Der Einfachheit halber führt dieses Muster ein Cold-RMAN-Backup durch. Sie können diese Schritte jedoch ändern,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	um ein Hot-RMAN-Backup mit Oracle Data Guard durchzufü hren, um Ausfallzeiten zu reduzieren.
	
	1. Starten Sie die Amazon EC2-Quelldatenbank im Mounting-Modus:
	
	`$ sqlplus / as sysdba`
	`$ SQL> shutdown immediate`
	`$ SQL> startup mount`
	
	2. Erstellen Sie ein RMAN-Sicherungsskript (verwende n Sie eines der folgenden Beispiele, je nach Version von Oracle, oder führen Sie eines Ihrer vorhandenen RMAN-Skri pte aus), um die Datenbank auf dem Amazon-EFS-Dateisy stem zu sichern, das Sie gemountet haben (`/RMAN` in diesem Beispiel).
	
	Für Oracle 12.1.0.2:
	
	`$ vi FullRMANColdBackup.sh`
	`#!/bin/bash`
	`. /home/oracle/.bash_profile`
	
	`export ORACLE_SID=VIS`
	`export ORACLE_HOME=/d01/oracle/VIS/12.1.0`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	export DATE=$(date +
	%y-%m-%d_%H%M%S)
	
	rman target / log=/RMAN
	/VISDB_${DATE}.log <<
	EOF
	run
	{
	allocate channel ch1
	device type disk format
	'/RMAN/visdb_full_
	bkp_%u';
	allocate channel ch2
	device type disk format
	'/RMAN/visdb_full_
	bkp_%u';
	crosscheck backup;
	delete noprompt
	obsolete;
	BACKUP AS COMPRESSED
	BACKUPSET DATABASE PLUS
	ARCHIVELOG;
	backup archivelog all;
	release channel ch1;
	release channel ch2;
	}
	EOF
	
	Für Oracle 19c:
	
	$ vi FullRMANColdBackup
	.sh
	#!/bin/bash
	. /home/oracle/.bash
	_profile
	
	export ORACLE_SI
	D=VISCDB
	export ORACLE_HOME=/
	d01/oracle/VIS/19c	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`export DATE=$(date +%y-%m-%d_%H%M%S)`
	
	`rman target / log=/RMAN/VISDB_${DATE}.log <<`
	` EOF`
	`run`
	`{`
	`allocate channel ch1`
	` device type disk format`
	` '/RMAN/visdb_full_bkp_%u';`
	`allocate channel ch2`
	` device type disk format`
	` '/RMAN/visdb_full_bkp_%u';`
	`crosscheck backup;`
	`delete noprompt`
	` obsolete;`
	`BACKUP AS COMPRESSED`
	` BACKUPSET DATABASE PLUS`
	` ARCHIVELOG;`
	`backup archivelog all;`
	`backup current`
	` controlfile format '/RMAN/cntrl.bak';`
	`release channel ch1;`
	`release channel ch2;`
	`}`
	`EOF`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie das Backup-Skript aus.	Ändern Sie die Berechtigungen, melden Sie sich als Oracle-Benutzer an und führen Sie das Skript aus:
	`$  chmod 755 FullRMANColdBackup.sh`
	`$ ./FullRMANColdBackup.sh`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie auf Fehler und notieren Sie sich den Namen der Sicherungsdatei.	Überprüfen Sie die RMAN-Protokolldatei auf Fehler. Wenn alles in Ordnung aussieht, listen Sie die Sicherung der Kontrolldatei auf. Notieren Sie sich den Namen der Ausgabedatei. Für Oracle 12.1.0.2: `RMAN> connect target /` `RMAN> list backup of controlfile;` `BS Key Type LV Size Device Type Elapsed Time Completion Time ------- ---- -- ---------- --------- -- ------------ --------------- 9 Full 1.11M DISK 00:00:04 23-APR-22 BP Key: 9 Status: AVAILABLE Compressed: YES Tag: TAG20220423T121011 Piece Name: /RMAN/visdb_full_bkp_100rlsbt Control File Included: Ckp SCN: 122045953 96727 Ckp time: 23-APR-22`  Sie verwenden die Sicherungsdatei `/RMAN/vis`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`db_full_bkp_100rlsbt` später, wenn Sie die Datenbank in Amazon RDS Custom wiederherstellen.
	
	Für Oracle 19c:
	
	``
	RMAN> connect target /
	
	RMAN> list backup of controlfile;
	
	BS Key Type LV Size Device Type Elapsed Time Completion Time
	------- ---- -- ---------- ----------- ------------ ---------------
	38 Full 17.92M DISK 00:00:01 25-NOV-22
	        BP Key: 38 Status: AVAILABLE Compressed: NO Tag: TAG20221125T095014
	        Piece Name: /RMAN/cntrl.bak
	  Control File Included: Ckp SCN: 12204620188873 Ckp time: 23-NOV-22
	``
	
	Sie verwenden die Sicherungsdatei/`RMAN/cntrl.bak` später, wenn Sie die Datenbank in Amazon RDS Custom wiederherstellen.	

Konfigurieren der Amazon-RDS-Custom-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Hostdatei und legen Sie den Hostnamen fest.	Hinweis: Die Befehle in diesem Abschnitt müssen als Root-Benutzer ausgeführt werden.
	
	1. Bearbeiten Sie die `/etc/hosts` Datei auf der Amazon RDS Custom DB-Instance. Eine einfache Möglichkeit hierfür besteht darin, die Datenbank- und Anwendungshosteinträge aus der Quelldatei der Amazon EC2-Datenbankhosts zu kopieren.
	
	`<IP-address> OEBS-app01.localdomain OEBS-app01 OEBS-app01log.localdomain OEBS-app01log`
	`<IP-address> OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log`
	
	wobei die IP-Adresse des Datenbankknotens `<IP-address>` ist, die Sie durch die benutzerdefinierte IP-Adresse von Amazon RDS ersetzen sollten. Den logischen Hostnamen wird angehängt`*log`.
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Ändern Sie den Datenbank-Hostnamen, indem Sie den `hostnamectl` Befehl ausführen:
	`$ sudo hostnamectl set-hostname --static persistent-hostname`
	Beispielsweise:
	`$ sudo hostnamectl set-hostname --static OEBS-db01log`
	Weitere Informationen finden Sie im Knowledge-Center-Artikel zum Zuweisen statischer Hostnamen.
	3. Starten Sie die Amazon RDS Custom DB-Instance neu. Machen Sie sich keine Gedanken über das Herunterfahren der Datenbank, da Sie sie in einem späteren Schritt löschen werden.
	`$ reboot`
	4. Wenn die Amazon RDS Custom DB-Instance wieder gestartet wird, melden Sie sich an und überprüfen Sie, ob sich der Hostname geändert hat:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ hostname` `oebs-db01`	

Installieren Sie die Oracle E-Business Suite-Software.	Installieren Sie die von Oracle E-Business Suite empfohlenen RPMs am Oracle-Heimatspeicherort auf der Amazon RDS Custom DB-Instance. Weitere Informationen finden Sie unter Oracle Support Note #1330701.1. Im Folgenden finden Sie eine Teilliste. Die RPM-Liste ändert sich für jede Version. Überprüfen Sie daher, ob alle erforderlichen RPMs installiert sind.
	
	Führen Sie als Root-Benutzer Folgendes aus:
	
	`$ sudo yum -y update`
	`$ sudo yum install -y elfutils-libelf-devel*`
	`$ sudo yum install -y libXp-1.0.2-2.1*.i686`
	`$ sudo yum install -y libXp-1.0.2-2.1*`
	`$ sudo yum install -y compat-libstdc++-*`
	
	Stellen Sie sicher, dass alle erforderlichen Patches installiert sind, bevor Sie mit dem nächsten Schritt fortfahren.
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie den VNC-Server.	Hinweis: Sie können diesen Schritt für Oracle 19c weglassen, da die Beispiel-CD nicht mehr erforderlich ist. Weitere Informationen finden Sie unter Oracle Support Note 2782085.1.
	
	Für Oracle 12.1.0.2:
	
	Installieren Sie den VNC-Server und seine abhängigen Desktop-Pakete. Dies ist eine Voraussetzung für die Installation der CD mit 12c-Beispielen im nächsten Schritt.
	
	1. Führen Sie als Root-Benutzer Folgendes aus:
	
	`$ sudo yum install -y tigervnc-server`
	`$ sudo yum install -y *kde*`
	`$ sudo yum install -y *xorg*`
	
	2. Starten Sie den VNC-Server für den `rdsdb` Benutzer und legen Sie das Passwort für VNC fest:
	
	`$ su - rdsdb`
	`$ vncserver :1`
	`$ vncpassword`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die CD 12c Examples.	Hinweis: Sie können diesen Schritt für Oracle 19c weglassen, da die Beispiel-CD nicht mehr erforderlich ist. Weitere Informationen finden Sie unter Oracle Support Note 2782085.1.
	
	Für Oracle 12.1.0.2:
	
	1. Laden Sie die Installat ionsdateien von https://edelivery.oracle.com/ herunter. Suchen Sie für Oracle E-Business Suite 12.2.11 – Oracle Database 12c Release 1 (12.1.0.2) nach Beispielen für Linux x86-64 V100102-01.zip .
	
	2. Erstellen Sie ein Verzeichn is zum Speichern der Beispiel-CD:
	
	`$ mkdir /RMAN/12c examples`
	
	3. Kopieren Sie die CD-ZIP-Be ispieldatei in dieses Verzeichn is, indem Sie den Übertragu ngsmechanismus Ihrer Wahl verwenden (z. B. SCP):
	
	`V100102-01.zip`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Ändern Sie den Besitz in `rdsdb`:
	`$ chown -R rdsdb:rdsdb /RMAN/12cexamples`
	5. Entpacken Sie als `rdsdb` Benutzer die Datei:
	`$ unzip V10010201.zip`
	6. Stellen Sie eine Verbindung von einem Client her, der Zugriff auf den VNC-Client und Amazon RDS Custom hat. Stellen Sie sicher, dass Sie die erforderlichen Netzwerkkonnektivitäts- und Firewall-Ports geöffnet haben, um den Zugriff für VNC zu ermöglichen. Beispielsweise muss ein VNC-Server, der auf ausgeführt `display :1` wird, Port 5901 auf der Sicherheitsgruppe öffnen, die dem Host von Amazon RDS Custom EC2 zugeordnet ist.
	7. Wechseln Sie in das Verzeichnis, in das Sie die Beispiel-CD kopiert haben:
	`$ cd /RMAN/12cexamples/examples`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	8. Führen Sie das Installat ionsprogramm aus. Stellen Sie sicher, dass Sie den Speicherort der `oraInst.l oc` Datei überprüfen.
	`./runInstaller - invPtrLoc /rdsdbbin /oracle.12.1.custo m.r1.EE.1/oraInst.loc`
	9. Verwenden Sie bei der Installation der Beispiel-CD die folgenden Parameter:
	`Skip Software Update Downloads`
	`Select Oracle Home 12.1.0.2`
	`(Oracle Base = / rdsdbbin)`
	`(Software Location = /rdsdbbin/oracle/1 2.1.custom.r1.EE.1)`
	10. Das Installationsprogr amm umfasst fünf Schritte mit Eingabeaufforderungen. Führen Sie die Schritte aus, bis die Installation abgeschlo ssen ist.	

Löschen Sie die Starter-Datenbank und erstellen Sie die Verzeichnisse zum Speichern der Datenbankdateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Der Automatisierungsmodus wird angehalten.	Sie müssen den Automatisierungsmodus auf Ihrer Amazon RDS Custom DB-Instance anhalten, bevor Sie mit den nächsten Schritten fortfahren, um sicherzustellen, dass die Automatisierung die RMAN-Aktivität nicht beeinträchtigt. Halten Sie die Automatisierung mit dem folgenden AWS Command Line Interface (AWS CLI)-Befehl an. (Stellen Sie sicher, dass Sie zuerst die AWS CLI konfiguriert haben.) `aws rds modify-db-instance \ --db-instance-id entifier VIS \ --automation-mode all-paused \ --resume-full-automation-mode-minute 360 \ --region eu-west-1` Wenn Sie die Dauer der Pause angeben, stellen Sie sicher, dass Sie genügend Zeit für die RMAN-Wiederherstellung lassen. Dies	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hängt von der Größe der Quelldatenbank ab. Ändern Sie daher den 360-Wert entsprechend.	

Löschen Sie die Starter-Datenbank.	Löschen Sie die vorhandene Amazon-RDS-Custom-Datenbank.
	
	Führen Sie als Oracle-Basisbenutzer die folgenden Befehle aus. (Der Standarddbenutzer ist `rdsdb`, es sei denn, Sie haben ihn angepasst.)
	
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate;`
	`SQL> startup nomount restrict;`
	`SQL> alter database mount;`
	`SQL> drop database;`
	`SQL> exit`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Verzeichnisse zum Speichern der Datenbank dateien.	Für Oracle 12.1.0.2:
	
	Erstellen Sie Verzeichnisse für die Datenbank, die Kontrolld atei, Datendateien und das Online-Protokoll. Verwenden Sie das übergeordnete Verzeichnis des `control_f iles` Parameters im vorherigen Befehl (in diesem Fall `VIS_A`). Führen Sie die folgenden Befehle als Oracle-Basisbenutzer aus (standard mäßig `rdsdb`).
	
	`$ mkdir -p /rdsdbdata/ db/VIS_A/controlfile`
	`$ mkdir -p /rdsdbdata/ db/VIS_A/datafile`
	`$ mkdir -p /rdsdbdata/ db/VIS_A/onlinelog`
	
	Für Oracle 19c:
	
	Erstellen Sie Verzeichnisse für die Datenbank, die Kontrolld atei, Datendateien und das Online-Protokoll. Verwenden Sie das übergeordnete Verzeichnis des `control_f iles` Parameters im vorherigen Befehl (in diesem Fall `VISCDB_A`). Führen Sie die folgenden Befehle als Oracle-Basisbenutzer aus (standardmäßig `rdsdb`).
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/controlfile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/datafile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog/arch`
	`$ mkdir /rdsdbdata/db/pdb/VISCDB_A`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und ändern Sie die Parameterdatei für Oracle E-Business Suite.	In diesem Schritt kopieren Sie die Serverparameterdatei (SPFILE) nicht aus der Quelldatenbank. Stattdessen verwenden Sie die Standardparameterdatei (PFILE), die mit der Amazon RDS Custom DB-Instance erstellt wurde, und fügen die Parameter hinzu, die Sie für Oracle E-Business Suite benötigen. Wenn Sie die Datenbank löschen, erstellt die Amazon-RDS-Automatisierung eine Sicherung der `init.ora` Datei, die der Amazon-RDS-Custom-Datenbank zugeordnet ist. Diese Datei heißt `oracle_pfile` und befindet sich in `/rdsdbdata/config` . Für Oracle 12.1.0.2: 1. Kopieren Sie `/rdsdbdata/config/oracle_pfile` in `$ORACLE_HOME` . `$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVIS.ora` 2. Bearbeiten Sie die `initVIS.ora` Datei auf der Amazon RDS Custom	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	DB-Instance. Validieren Sie alle Parameter in der Quelle und fügen Sie nach Bedarf Parameter hinzu. Weitere Informationen finden Sie unter Oracle Support Note 396009.1.
	
	Wichtig: Stellen Sie sicher, dass die von Ihnen hinzugefügten Parameter keine Kommentare enthalten. Kommentare verursachen Probleme mit der Automatisierung, z. B. das Erstellen von Lesereplikaten und das Ausgeben von point-in-time Wiederherstellungen (PITRs).
	
	3. Fügen Sie der `initVIS.ora` Datei basierend auf Ihren Anforderungen Parameter hinzu, die den folgenden ähneln:
	
	`*.workarea_size_policy='AUTO'`
	`*.plsql_code_type='INTERPRETED'`
	`*.cursor_sharing='EXACT'`
	`*._b_tree_bitmap_plans=FALSE`
	`*.session_cached_cursors=500`
	`*.optimizer_adaptive_features=false`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	*.optimizer_secur e_view_merging=false *.SQL92_SECURITY=TRUE *.temp_undo_enabled= true _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_charact ers = "." nls_comp = binary nls_sort = binary nls_date_format = DD- MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enable d = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL sec_case_sensitive_l ogon = FALSE compatible = 12.1.0 o7_dictionary_access ibility = FALSE	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`utl_file_dir =/tmp`
	
	4. Ändern Sie Folgendes. Die Werte hängen von Ihrem Quellsystem ab. Überprüfen Sie sie daher basierend auf Ihrer aktuellen Einrichtung.
	
	`*.open_cursors=500`
	`*.undo_tablespace`
	`='APPS_UNDOTS1`
	
	5. Entfernen Sie die SPFILE-Referenz.
	
	`*.spfile='/rdsdbbi`
	`n/oracle/dbs/spfil`
	`eVIS.ora'`
	
	Hinweise:
	
	• Ändern Sie nicht die Werte, die von Amazon RDS Custom PFILE für `control_files` und bereitgestellt werden`db_unique_name` . Amazon RDS erwartet diese Werte. Wenn Sie versuchen , in Zukunft ein Leserepli kat zu erstellen, kann es zu Problemen kommen, wenn Sie davon abweichen.
	• Amazon RDS Custom verwendet standardm äßig Automatic Memory	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Management (AMM). Wenn Sie Hugem verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass Automatic Shared Memory Management (ASMM) verwendet wird.
	• Lassen Sie den `memory_max_target` Parameter standardmäßig aktiviert. Das Amazon-RDS-Framework verwendet dies im Hintergrund, um Leserepli kate zu erstellen.
	
	6. Vergewissern Sie sich, dass es keine Probleme mit der `initVIS.ora` Datei gibt, indem Sie den `startup nomount` Befehl ausführen:
	`SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVIS.ora;`
	`SQL> create spfile='/rdsdbdata/admin/VIS/pfile/spfileVIS.ora' from pfile;`
	`SQL> exit`
	
	7. Erstellen Sie einen symbolischen Link für SPFILE.
	`$ ln -s /rdsdbdata/admin/VIS/pfile/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`spfileVIS.ora $ORACLE_HOME/dbs/`
	
	Für Oracle 19c:
	
	1. Kopieren Sie `/rdsdbdata/config/oracle_pfile` in `$ORACLE_HOME` .
	
	`$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVISCDB.ora`
	
	2. Bearbeiten Sie die `initVISCDB.ora` Datei auf der Amazon RDS Custom DB-Instance. Validieren Sie alle Parameter in der Quelle und fügen Sie nach Bedarf Parameter hinzu. Weitere Informationen finden Sie unter Oracle Support Note 396009.1.
	
	Wichtig: Stellen Sie sicher, dass die von Ihnen hinzugefügten Parameter keine Kommentare enthalten. Wenn Kommentare vorliegen, verursachen sie Probleme mit der Automatisierung, z. B. das Erstellen von Lesereplikaten und das Ausgeben von point-in-time Wiederherstellungen (PITRs).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Fügen Sie der `initVISCDB.ora` Datei basierend auf Ihren Anforderungen Parameter hinzu, die den folgenden ähneln.
	
	`*.instance_name=VISCDB`
	`*.sec_case_sensitive_logon= FALSE`
	`*.result_cache_max_size = 600M`
	`*.optimizer_adaptive_plans =TRUE`
	`*.optimizer_adaptive_statistics = FALSE`
	`*.pga_aggregate_limit = 0`
	`*.temp_undo_enabled = FALSE`
	`*._pdb_name_case_sensitive = TRUE`
	`*.event='10946 trace name context forever, level 8454144'`
	`*.workarea_size_policy='AUTO'`
	`*.plsql_code_type='INTERPRETED'`
	`*.cursor_sharing='EXACT'`
	`*._b_tree_bitmap_plans=FALSE`
	`*.session_cached_cursors=500`
	`*.optimizer_secure_view_merging=false`
	`*.SQL92_SECURITY=TRUE`
	`_system_trig_enabled = TRUE`
	`nls_language = american`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nls_territory = america nls_numeric_characters = ".," nls_comp = binary nls_sort = binary nls_date_format = DD-MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enabled = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL 4. Ändern Sie Folgendes. Die Werte hängen von Ihrem Quellsystem ab. Überprüfen Sie sie daher basierend auf Ihrem aktuellen Setup. *.open_cursors=500 *.undo_tablespace ='UNDOTBS1'	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Entfernen Sie die SPFILE-Referenz: `*.spfile='/rdsdbbin/oracle/dbs/spfileVISCDB.ora'` Hinweise: • Ändern Sie nicht die Werte, die von Amazon RDS Custom PFILE für `control_files` und bereitgestellt werden`db_unique_name` . Amazon RDS erwartet diese Werte. Wenn Sie versuchen , in Zukunft ein Leserepli kat zu erstellen, kann es zu Problemen kommen, wenn Sie davon abweichen. • Amazon RDS Custom verwendet standardm äßig Automatic Memory Management (AMM). Wenn Sie Hugem verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass Automatic Shared Memory Management (ASMM) verwendet wird. • Lassen Sie den `memory_max_target` Parameter standardmäßig aktiviert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Das Amazon-RDS-Framework verwendet dies im Hintergrund, um Leserepli kate zu erstellen.
	
	6. Vergewissern Sie sich, dass es keine Probleme mit der `initVISCDB.ora` Datei gibt, indem Sie den `startup nomount` Befehl ausführen:
	
	`SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVISCDB.ora;`
	`SQL> create spfile='/rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora' from pfile;`
	`SQL> exit`
	
	7. Erstellen Sie einen symbolischen Link für SPFILE.
	
	`$ ln -s /rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora $ORACLE_HOME/dbs/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Amazon-RDS-Custom-Datenbank aus dem Backup wieder her.	Für Oracle 12.1.0.2:
	
	1. Stellen Sie die Kontrolldatei mithilfe der Sicherungsdatei wieder her, die Sie zuvor in der Quelle erfasst haben:
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFILE FROM '/RMAN/visdb_full_bkp_100rlsbt';`
	
	`Starting restore at 10-APR-22`
	`using target database control file instead of recovery catalog`
	`allocated channel: ORA_DISK_1`
	`channel ORA_DISK_1: SID=201 device type=DISK`
	
	`channel ORA_DISK_1: restoring control file`
	`channel ORA_DISK_1: restore complete, elapsed time: 00:00:01`
	`output file name=/rdsdbdata/db/VIS_A/controlfile/control-01.ctl`
	`Finished restore at 10-APR-22`
	
	2. Katalogisieren Sie die Backup-Teile, damit Sie
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	eine ausgeben könnenRMAN `restore`:
	
	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	
	3. Erstellen Sie ein Skript, um die Datenbank wiederher zustellen:
	
	`$ vi restore.sh`
	`rman target / log=/home /rdsdb/rman.log << EOF`
	`run`
	`{`
	`set newname for database to '/rdsdbdata/db/VIS _A/datafile/%b';`
	`restore database;`
	`switch datafile all;`
	`switch tempfile all;`
	`}`
	`EOF`
	
	4. Stellen Sie die Quelle in der Amazon-RDS-Custom-Zieldatenbank wieder her. Sie müssen die Berechtigungen des Skripts ändern, damit es ausgeführt werden kann, und dann das `restore.s h` Skript ausführen, um die Datenbank wiederherzustellen .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`
	
	Für Oracle 19c:
	
	1. Stellen Sie die Kontrolldatei mithilfe der Sicherungsdatei wieder her, die Sie zuvor in der Quelle erfasst haben:
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFI LE FROM '/RMAN/cn trl.bak';`
	`Starting restore at 07- JUN-23`
	`using target database control file instead of recovery catalog`
	`allocated channel: ORA_DISK_1`
	`channel ORA_DISK_ 1: SID=201 device type=DISK`
	`channel ORA_DISK_1: restoring control file`
	`channel ORA_DISK_ 1: restore complete, elapsed time: 00:00:01`
	`output file name=/rds dbdata/db/cdb/VISC DB_A/controlfile/c ontrol-01.ctl`
	`Finished restore at 07- JUN-23`
	
	2. Katalogisieren Sie die Backup-Teile, damit Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	eine ausgeben könnenRMAN `restore`:
	
	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	
	Wenn Sie Probleme mit dem `start with` Befehl haben, können Sie die Backup-Teile einzeln hinzufügen, z. B.:
	
	`RMAN> catalog backuppiece '/RMAN/visdb_full_bkp_1d1e507m';`
	
	und wiederholen Sie dann den Befehl für jeden Backup-Teil.
	
	3. Erstellen Sie ein Skript, um die Datenbank wiederherzustellen. Ändern Sie den steckbaren Datenbanknamen entsprechend Ihren Anforderungen. Weisen Sie parallele Kanäle basierend auf der Anzahl der verfügbaren vCPUs zu, um den Wiederherstellungsprozess zu beschleunigen.
	
	`$ vi restore.sh`
	`rman target / log=/home/rdsdb/rmancdb.log <<`
	`EOF`
	`run {`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>allocate channel c1
	 type disk;
	allocate channel c2
	 type disk;
	....
	allocate channel c<N>
	 type disk;
	set newname for database
	 to '/rdsdbdata/db/cdb
	/VISCDB_A/datafile/
	%b';
	set newname for database
	 root to '/rdsdbda
	ta/db/cdb/VISCDB_A/
	datafile/%f_%b';
	set newname for
	 database "PDB$SEED" to
	 '/rdsdbdata/db/cdb/
	pdbseed/%f_%b';
	set newname for
	 pluggable database VIS
	 to '/rdsdbdata/db/pdb
	/VISCDB_A/%f_%b';
	restore database;
	switch datafile all;
	switch tempfile all;
	release channel c1;
	release channel c2;
	release channel c3;
	....
	release channel c<N>;
	}
	EOF</pre>
	4. Stellen Sie die Quelle in der Amazon-RDS-Custom-Zieldatenbank wieder her. Sie müssen die Berechtigungen des Skripts ändern, damit es ausgeführt werden kann,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	und dann das `restore.sh` Skript ausführen, um die Datenbank wiederherzustellen.
	
	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Protokoll dateien auf Probleme.	Für Oracle 12.1.0.2:
	
	1. Vergewissern Sie sich, dass es keine Probleme gibt, indem Sie die `rman.log` Datei überprüfen:
	
	`$ cat /home/rdsdb/ rman.log`
	
	2. Bestätigen Sie den Pfad der in der Kontrolldatei registrie rten Protokolldateien:
	
	`SQL> select member from v$logfile; MEMBER ---------- ---------- ---------- ---------- -------- /d01/oracle/VIS/data/ log1.dbf /d01/oracle/VIS/data/ log2.dbf /d01/oracle/VIS/data/ log3.dbf`
	
	3. Benennen Sie die Protokoll dateien so um, dass sie dem Dateipfad des Ziels entsprech en. Ersetzen Sie den Pfad so, dass er der Ausgabe aus dem vorherigen Schritt entspricht:
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log1.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log1.dbf';`
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log2.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log2.dbf';`
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log3.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log3.dbf';`
	
	Für Oracle 19c:
	
	1. Vergewissern Sie sich, dass es keine Probleme gibt, indem Sie die `rmancdb.log` Datei überprüfen:
	
	`$ cat /home/rdsdb/rmancdb.log`
	
	2. Bestätigen Sie den Pfad der in der Kontrolldatei registrierten Protokolldateien:
	
	`SQL> select member from v$logfile;`
	`MEMBER`
	`----------`
	`----------`
	`----------`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ------------------ -------- /d01/oracle/VIS/or adata/VISCDB/redo0 3.log /d01/oracle/VIS/orada ta/VISCDB/redo02.log /d01/oracle/VIS/ oradata/VISCDB/re do01.log ```	
	3. Benennen Sie die Protokoll dateien so um, dass sie dem Dateipfad des Ziels entsprech en. Ersetzen Sie den Pfad so, dass er der Ausgabe aus dem vorherigen Schritt entspricht: ``` SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo01.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log1.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo02.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log2.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo03.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log3.dbf'; ```	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Bestätigen Sie den Pfad, den Status der Protokoll dateien und die Gruppennu mmer, die in der Kontrolldatei registriert ist:
	
	`SQL> column REDOLOG_F ILE_NAME format a50 SQL> SELECT a.GROUP#, a.status, b.MEMBER AS REDOLOG_FILE_NAME, (a.BYTES/1024/1024) AS SIZE_MB FROM v$log a JOIN v$logfile b ON a.Group#=b.Group# ORDER BY a.GROUP#;`
	
	`GROUP# STATUS REDOLOG_F ILE_NAME SIZE_MB 1 CURRENT /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log1.dbf 512 2 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log2.dbf 512 3 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log3.dbf 512`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass Sie die Amazon-RDS-Custom-Datenbank öffnen und OMF-Protokolldateien erstellen können.	Amazon RDS Custom für Oracle verwendet Oracle Managed Files (OMF), um den Betrieb zu vereinfachen. Sie können Lesereplikate zu eigenständigen Instances hochstufen, müssen jedoch zuerst die Protokolldateien mithilfe von OMF erstellen . Dadurch wird sichergestellt, dass beim Hochstufen der Instance der richtige Pfad verwendet wird. Weitere Informationen zum Hochstufen von Lesereplikaten finden Sie in der Amazon-RDS-Dokumentation. Wenn Sie OMF-Dateien nicht verwenden, kann dies möglicherweise zu Problemen führen, wenn Sie versuchen, Lesereplikate hochzustufen. 1. Öffnen Sie die Datenbank mit `resetlogs` : `SQL> alter database open resetlogs;` Hinweis: Wenn Sie die Fehlermeldung ORA-00392 : Protokoll xx von Thread 1 wird gelöscht, die Operation ist nicht zulässig, befolgen Sie die Schritte im Abschnitt	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Fehlerbehebung für ORA-00392.
	
	2. Vergewissern Sie sich, dass die Datenbank geöffnet ist:
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`READ WRITE`
	
	3. Erstellen Sie die OMF-Protokolldateien. Ändern Sie die Gruppennummern, die Anzahl der Gruppen und die Größe je nach Ihren Anforderungen, indem Sie die Ausgabe der vorherigen Protokolldateiabfrage verwenden. Das folgende Beispiel beginnt bei Gruppe 4 und fügt der Einfachheit halber drei Gruppen hinzu.
	
	`SQL> alter database add logfile group 4 size 512M;`
	`Database altered.`
	`SQL> alter database add logfile group 5 size 512M;`
	`Database altered.`
	`SQL> alter database add logfile group 6 size 512M;`
	`Database altered.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Löschen Sie die vorherigen Nicht-OMF-Dateien. Hier ist ein Beispiel, das Sie basierend auf Ihren Anforderungen und der Ausgabe der Abfrage in früheren Schritten anpassen können:
	`SQL> alter database drop logfile group 1;`
	`System altered.`
	`SQL> alter database drop logfile group 2;`
	`System altered.`
	`SQL> alter database drop logfile group 3;`
	`System altered.`
	Hinweis: Wenn Sie beim Versuch, die Protokolldateien zu löschen, einen ORA-01624-Fehler erhalten, lesen Sie den Abschnitt Fehlerbehebung.
	5. Vergewissern Sie sich, dass Sie die erstellten OMF-Dateien sehen können. (Der Verzeichnispfad variiert für Oracle 12.1.0.2 und 19c, aber das Konzept ist dasselbe.)
	`SQL> select member from v$logfile;`
	`MEMBER`
	`----------`
	`----------`
	`----------`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_4_ksrbslny_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_5_ksrchw0k_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_6_ksrcnl9v_.log`
	6. Starten Sie die Datenbank neu und bestätigen Sie, dass SPFILE von der Instance verwendet wird:
	`SQL> shutdown immediate`
	`SQL> startup`
	`SQL> show parameter spfile`
	Für Oracle 12.1.0.2 gibt diese Abfrage Folgendes zurück:
	`spfile /rdsdbbin/oracle/dbs/spfileVIS.ora`
	Für Oracle 19c gibt die Abfrage Folgendes zurück:
	`spfile /rdsdbbin/oracle/dbs/spfileVISCDB.ora`
	7. Überprüfen Sie nur für Oracle 19c den Status der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Container-Datenbank und öffnen Sie sie bei Bedarf:
	
	`SQL> show pdbs`
	`CON_ID CON_NAME`
	`OPEN MODE`
	`RESTRICTED`
	`---------- ---------`
	`---------- ---------`
	`-`
	`2 PDB$SEED`
	`READ ONLY NO`
	`3 VIS`
	`MOUNTED NO`
	
	`SQL> alter session set`
	`container=VIS;`
	`Session altered.`
	
	`SQL> alter database`
	`open;`
	`Database altered.`
	
	`SQL> alter database save`
	`state;`
	`Database altered.`
	
	`SQL> show pdbs`
	`CON_ID CON_NAME`
	`OPEN MODE`
	`RESTRICTED`
	`---------- ---------`
	`----------`
	`---------- -----`
	`3 VIS`
	`READ`
	`WRITE NO`
	
	`SQL> exit`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	8. Löschen Sie die `init.ora` Datei aus `$ORACLE_HOME/dbs`, da Sie PFILE nicht verwenden:
	`$ cd $ORACLE_HOME/dbs`
	Verwenden Sie für Oracle 12.1.0.2 den Befehl :
	`$ pwd`
	`/rdsdbbin/oracle/dbs`
	`$ rm initVIS.ora`
	Verwenden Sie für Oracle 19c den Befehl :
	`$ pwd`
	`/rdsdbbin/oracle/dbs`
	`$ rm initVISCDB.ora`	

Abrufen von Passwörtern aus Secrets Manager, Erstellen von Benutzern und Ändern von Passwörtern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie Passwörter aus Secrets Manager ab.	Sie können diese Schritte in der -Konsole oder mithilfe der AWS CLI ausführen. Die folgenden Schritte enthalten Anweisungen für die -Konsole. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	RDS-Konsole unter https://console.aws.amazon.com/rds/. 2. Wählen Sie im Navigationsbereich Datenbanken und dann die Amazon-RDS-Datenbank aus. 3. Wählen Sie Konfiguration und notieren Sie sich die Ressourcen-ID für die Instance (sie wird im Format vorliegen: `db-WZ4WLCK6AOQ6TJGZKMGRCDCI3Y`). 4. Öffnen Sie die AWS Secrets Manager-Konsole unter https://console.aws.amazon.com/secretsmanager/. 5. Wählen Sie das Secret aus, das denselben Namen wie hat`do-not-delete-custom-<resource_id>` , wobei sich auf die ID für die Instance `resource-id` bezieht, die Sie in Schritt 3 notiert haben. 6. Wählen Sie Retrieve secret value (Secret-Wert abrufen) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den RDSADMIN-Benutzer.	`RDSADMIN` ist ein Benutzer der Überwachungs- und Orchestrator-Datenbank in der Amazon RDS Custom DB-Instance. Da die Starter-Datenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie diesen Benutzer nach dem Wiederherstellungsvorgang neu erstellen, um sicherzustellen, dass die Überwachung von Amazon RDS Custom wie erwartet funktioniert. Sie müssen auch ein separates Profil und einen separaten Tabellenraum für den `RDSADMIN` Benutzer erstellen. Die Anweisungen unterscheiden sich für Oracle 12.1.0.2 und 19c geringfügig.
	
	Für Oracle 12.1.0.2:
	
	1. Geben Sie die folgenden Befehle an einer SQL-Eingabeaufforderung ein:
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	
	`SQL> ALTER PROFILE DEFAULT LIMIT`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL; 2. Erstellen Sie das Profil RDSADMIN: SQL> create profile RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`PASSWORD_GRACE_TIME 604800/86400;`
	
	3. Legen Sie die `DBSNMP` Benutzerprofile `SYS` `SYSTEM`, und auf fest`RDSADMIN`:
	
	`SQL> set echo on feedback on serverout on`
	`SQL> alter user SYS profile RDSADMIN;`
	`SQL> alter user SYSTEM profile RDSADMIN;`
	`SQL> alter user DBSNMP profile RDSADMIN;`
	
	4. Erstellen Sie den `RDSADMIN`Tabellenraum:
	
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent managemen t local autoallocate default nocompress segment space managemen t auto;`
	
	5. Erstellen Sie den `RDSADMIN` Benutzer. Ersetzen Sie das `RDSADMIN` Passwort durch das Passwort, das Sie zuvor von Secrets Manager erhalten haben:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> create user rdsadmin identified by xxxxxxxxxx Default tablespace rdsadmin Temporary tablespace temp profile rdsadmin ;`
	
	6. Erteilen Sie Berechtigungen für `RDSADMIN`:
	
	`SQL> grant select on sys.v_$instance to rdsadmin; SQL> grant select on sys.v_$archived_log to rdsadmin; SQL> grant select on sys.v_$database to rdsadmin; SQL> grant select on sys.v_$database_in carnation to rdsadmin; SQL> grant select on dba_users to rdsadmin; SQL> grant alter system to rdsadmin; SQL> grant alter database to rdsadmin; SQL> grant connect to rdsadmin with admin option; SQL> grant resource to rdsadmin with admin option; SQL> alter user rdsadmin account unlock identified by xxxxxxxxxxx;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> @?/rdbms/admin/use rlock.sql SQL> @?/rdbms/admin/utl rp.sql Für Oracle 19c: 1. Geben Sie die folgenden Befehle an einer SQL-Einga beaufforderung ein: SQL> set echo on feedback on serverout on SQL> @?/rdbms/admin/utl pwdmg.sql SQL> alter profile default LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL; 2. Erstellen Sie das Profil RDSADMIN. Hinweis: RDSADMIN hat das Präfix C## in Oracle 19c. Dies liegt daran, dass der Datenbankparameter auf gesetzt common_us er_prefix istC##. RDSADMIN hat kein Präfix in Oracle 12.1.0.2.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQL> create profile C##RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400;`  3. Legen Sie die DBSNMP Benutzerprofile SYSSYSTEM, und auf festRDSADMIN:  `SQL> alter user SYS profile C##RDSADMIN; SQL> alter user SYSTEM profile C##RDSADMIN;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> alter user DBSNMP profile C##RDSADMIN;`
	
	4. Erstellen Sie den `RDSADMIN`Tabellenraum:
	
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent managemen t local autoallocate default nocompress segment space managemen t auto;`
	
	5. Erstellen Sie den `RDSADMIN` Benutzer. Ersetzen Sie das `RDSADMIN` Passwort durch das Passwort, das Sie zuvor von Secrets Manager erhalten haben.
	
	`SQL> create user C##rdsadmin identifie d by xxxxxxxxxx profile C##rdsadmin container=all;`
	
	6. Erteilen Sie Berechtigungen für `RDSADMIN`:
	
	`SQL> grant select on sys.v_$instance to c##rdsadmin;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> grant select on sys.v_$archived_log to c##rdsadmin; SQL> grant select on sys.v_$database to c##rdsadmin; SQL> grant select on sys.v_$database_incarnation to c##rdsadmin; SQL> grant select on dba_users to c##rdsadmin; SQL> grant alter system to C##rdsadmin; SQL> grant alter database to C##rdsadmin; SQL> grant connect to C##rdsadmin with admin option; SQL> grant resource to C##rdsadmin with admin option; SQL> alter user C##rdsadmin account unlock identified by xxxxxxxxxxx; SQL> @?/rdbms/admin/userlock.sql SQL> @?/rdbms/admin/utlrp.sql	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Hauptbenutzer.	Da die Starter-Datenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie den Hauptbenutzer neu erstellen. In diesem Beispiel lautet der Hauptbenutzername `admin`.
	
	Für Oracle 12.1.0.2:
	
	`SQL> create user admin identified by <password>; SQL> grant dba to admin`
	
	Für Oracle 19c:
	
	`SQL> alter session set container=VIS;`
	
	`Session altered.`
	
	`SQL> create user admin identified by <password>;`
	
	`User created.`
	
	`SQL> grant dba to admin;`
	
	`Grant succeeded.`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Superuser-Passwörter.	1. Ändern Sie die Systempas swörter mithilfe des Passworts , das Sie von Secrets Manager abgerufen haben.
	
	Für Oracle 12.1.0.2:
	
	`SQL> alter user sys identified by xxxxxxxxxx; SQL> alter user system identified by xxxxxxxxxx;`
	
	Für Oracle 19c:
	
	`SQL> alter user sys identified by xxxxxxxxxx container =all; SQL> alter user system identified by xxxxxxxxxx container =all;`
	
	1. Ändern Sie die EBS_SYSTE M Passwörter.
	
	Für Oracle 12.1.0.2:
	
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	Für Oracle 19c:
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Für diese Version müssen Sie auch eine Verbindung zur Container-Datenbank herstelle n, um das `EBS_SYSTEM` Passwort dort zu aktualisieren.
	
	`SQL> alter session set container=vis;`
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	`SQL> exit;`
	
	Wenn Sie diese Passwörter nicht ändern, zeigt Amazon RDS Custom die Fehlermel dung an: Der Datenbank überwachungsbenutzer oder die Benutzeranmeldeinf ormationen haben sich geändert.	

Verzeichnisse für Oracle E-Business Suite erstellen, ETCC installieren und Autoconfig ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die für Oracle E-Business Suite erforderlichen Verzeichnisse.	1. Führen Sie in der Amazon RDS Custom Oracle-Da tenbank das folgende Skript als Oracle-Basisbenutzer aus, um das `9idata` Verzeichn is in zu erstellen`$ORACLE_H OME/nls/data/9idat a` . Dieses Verzeichnis ist	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	für Oracle E-Business Suite erforderlich.
	
	`perl $ORACLE_HOME/nls/data/old/cr9idata.pl`
	
	Ignorieren Sie die `ORA_NLS10` Nachricht, da Sie die kontextfähige Umgebung in späteren Schritten erstellen.
	
	2. Kopieren Sie die `appsutil.tar` Datei, die Sie zuvor aus dem freigegebenen Amazon-EFS-Dateisystem erstellt haben, und heben Sie die Markierung im Amazon-RDS-Custom-Oracle-Stammverzeichnis auf. Dadurch wird das `appsutil` Verzeichnis im `$ORACLE_HOME` Verzeichnis erstellt.
	
	`$ cd /RMAN/appsutil`
	`$ cp sourceappsutil.tar $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	`$ tar xvf sourceappsutil.tar appsutil`
	
	3. Kopieren Sie die `appsutil.zip` Datei, die Sie zuvor im freigegebenen Amazon-EFS-Dateisystem gespeichert haben. Dies war die Datei, die Sie auf der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Anwendungsebene erstellt haben.
	
	Als `rdsdb` Benutzer auf der Amazon RDS Custom DB-Instance:
	
	`$ cp /RMAN/appsutil/appsutil.zip $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	
	4. Entpacken Sie die `appsutil.zip` Datei, um das `appsutil` Verzeichnis und die Unterverzeichnisse im Oracle-Stammverzeichnis zu erstellen:
	
	`$ unzip -o appsutil.zip`
	
	Die `-o` Option bedeutet, dass einige der Dateien überschri eben werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Dateien tsanames.ora und sqlnet.ora.	Sie müssen die `tnsnames.ora` Datei konfigurieren, damit Sie mit dem Autoconfig-Tool eine Verbindung zur Datenbank herstellen können. Im folgenden Beispiel können Sie sehen, dass die `tnsnames.ora` Datei Softlinks enthält, die Datei jedoch standardmäßig leer ist.
	
	`$ cd $ORACLE_HOME/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 373 Oct 31 2013 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Feb 9 17:17 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	
	1. Erstellen Sie den `tnsnames.ora` Eintrag. Aufgrund der Art und Weise, wie die Amazon-RDS-Automatisierung die Dateien analysier
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	t, müssen Sie sicherste llen, dass der Eintrag keine Leerzeichen, Kommentar e oder zusätzliche Zeilen enthält. Andernfalls können bei der Verwendung einiger APIs wie create-db-instance -read-Replica Probleme auftreten. Verwenden Sie Folgendes als Beispiel.
	
	2. Ersetzen Sie Port, Host und SID gemäß Ihren Anforderu ngen:
	
	`$ vi tnsnames.ora`
	`VIS=(DESCRIPTION=`
	`(ADDRESS_LIST=(ADD`
	`RESS=(PROTOCOL=TCP`
	`)(PORT=1521)(HOST=`
	`xx.xx.xx.xx)))(CON`
	`NECT_DATA=(SID=VIS)`
	`(SERVER=DEDICATED)))`
	
	Hinweis: Die Datei sollte keine zusätzlichen Zeilen enthalten . Wenn Sie die Zeilen nicht entfernen, können Probleme auftreten, wenn Sie in Zukunft ein Lesereplikat erstellen. Die Erstellung eines Leserepli kats schlägt möglicherweise mit der Fehlermeldung fehl: Ausnahme „Aktivität ausgelöst “: HostManagerException: restrictReplication kann	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	auf Hosts nicht erfolgreich aufgerufen werden.
	
	3. Vergewissern Sie sich, dass die Datenbank erreicht werden kann:
	
	`$ tnsping vis`
	`OK (0 msec)`
	
	4. Aktualisieren Sie die Datei nur für Oracle 19c`sqlnet.ora` . Wenn Sie dies nicht tun, wird der Fehler ORA-01017 angezeigt: Ungültiger Benutzername/Passwort; Anmeldung verweigert, wenn Sie versuchen, eine Verbindung mit der Datenbank herzustellen. Bearbeiten Sie `sqlnet.ora` in `$ORACLE_HOME/network/admin` entsprechend den folgenden Angaben:
	
	`NAMES.DIRECTORY_PATH=(TNSNAMES, ONAMES, HOSTNAME)`
	`SQLNET.EXPIRE_TIME= 10`
	`SQLNET.INBOUND_CONNECT_TIMEOUT =60`
	`SQLNET.ALLOWED_LOGON_VERSION_SERVER=10`
	`HTTPS_SSL_VERSION=undetermined`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Testen der Konnektivität: `$ sqlplus apps/****@vis`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Datenbank.	Nachdem Sie nun die Konnektivität zur Datenbank getestet haben, können Sie die Datenbank mit dem Dienstprogramm apputil konfigurieren, um die kontextfähige Umgebung zu erstellen.
	
	Für Oracle 12.1.0.2:
	
	1. Führen Sie die folgenden Befehle aus:
	
	`$ cd $ORACLE_HOME/appsutil/bin`
	`$ perl adbldxml.pl appsuser=apps`
	`Enter Hostname of Database server: oebs-db01`
	`Enter Port of Database server: 1521`
	`Enter SID of Database server: VIS`
	`Enter Database Service Name: VIS`
	`Enter the value for Display Variable: :1`
	`The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml`
	
	2. `oraInst.loc` Aus Root-Benutzer erstellen:
	
	`$ vi /etc/oraInst.loc`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`inventory_loc=/rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInventory inst_group=database`	

	3. Klonen Sie die Kontextdatei, um den logischen Hostnamen festzulegen, indem Sie die Kontextdatei verwenden, die Sie im vorherigen Schritt erstellt haben. Führen Sie als `rdsdb` Benutzer Folgendes aus:
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	wobei sich auf den logischen Hostnamen `oebs-db01log` bezieht. Beispielsweise:
	`$ perl adclonectx.pl \`
	`contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/VIS_oebs-db01.xml \`
	`template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Target System Hostname (virtual or normal) [oebs-db01] : oebs- db01log Target System Base Directory : /rdsdbbin/ oracle Target Instance is RAC (y/n) [n] : n Target System Database SID : VIS Oracle OS User [rdsdb] : Oracle OS Group [rdsdb] : database Role separation is supported y/n [n] ? : n Target System utl_file_ dir Directory List : / tmp Number of DATA_TOP's on the Target System [1] : Target System DATA_TOP Directory 1 [/rdsdbbi n/oracle/data] : / rdsdbdata/db/VIS_A/ datafile/ Target System RDBMS ORACLE_HOME Directory [/rdsdbbin/oracle/ 12.1.0] : /rdsdbbin/ oracle Do you want to preserve the Display [:1] (y/n) : y	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Do you want the target system to have the same port values as the source system (y/n) [y] ? : y The new database context file has been created : /rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml Für Oracle 19c: 1. Führen Sie die folgenden Befehle aus: $ cd $ORACLE_HOME/appsutil/bin $ perl adbldxml.pl appsuser=apps Enter Hostname of Database server: oebs-db01 Enter Port of Database server: 1521 Enter SID of Database server: VIS Enter the database listener name:L_VISCDB_001 Enter the value for Display Variable: :1 The context file has been created at:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml`
	
	2. `oraInst.loc` Aus Root-Benutzer erstellen:
	
	`$ vi /etc/oraInst.loc`
	`inventory_loc=/rdsdbbin/oracle/oraInventory`
	`inst_group=database`
	
	3. Klonen Sie die Kontextdatei, um den logischen Hostnamen festzulegen, indem Sie die Kontextdatei verwenden, die Sie im vorherigen Schritt erstellt haben. Führen Sie als `rdsdb` Benutzer Folgendes aus:
	
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	
	wobei sich auf den logischen Hostnamen `oebs-db01log` bezieht. Beispielsweise:
	
	`$ perl adclonectx.pl \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml \ template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp Target System Hostname (virtual or normal) [oebs-db01] : oebs-db01log Target System Base Directory : /rdsdbbin/oracle Target Instance is RAC (y/n) [n] : n Target System CDB Name : VISCDB Target System PDB Name : VIS Oracle OS User [oracle] : rdsdb Oracle OS Group [dba] : database Role separation is supported y/n [n] ? : n Number of DATA_TOP's on the Target System [2] : Target System DATA_TOP Directory 1 [/d01/oracle/VISCDB] : /rdsdbdata/db/pdb/VISCDB_A Target System DATA_TOP Directory 2 [/d01/oracle/data] : /rdsdbdata/db/pdb/VISCDB_A/datafile Specify value for OSBACKUPDBA group [database] :	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Specify value for OSDGDBA group [database] : Specify value for OSKMDBA group [database] : Specify value for OSRACDBA group [database] : Target System RDBMS ORACLE_HOME Directory [/d01/oracle/19.0.0] : /rdsdbbin/oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as the source system (y/n) [y] ? : y Validating if the source port numbers are available on the target system.. Complete port information available at /rdsdbbin/oracle/appsutil/clone/bin/out/VIS_oebs-db01log/portpool.lst New context path and file name [VIS_oebs-db01log.xml] : /rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml Do you want to overwrite it (y/n) [n] ? : y Replacing /rdsdbbin/oracle/appsutil/V	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IS_oebs-db01log.xml file. The new database context file has been created : contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml Check Clone Context logfile /rdsdbbin/oracle/appsutil/clone/bin/CloneContext_0609141428.log for details.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie ETCC und führen Sie Autoconfig aus.	1. Installieren Sie den Oracle E-Business Suite Technology Codelevel Checker (ETCC).
	
	Laden Sie Patch 17537119 von My Oracle Support herunter und folgen Sie den Anweisungen unter `README.txt` . Sie erstellen ein Verzeichnis namens `etcc` im `$ORACLE_HOME` Verzeichnis , entpacken den Patch, um ein Skript namens zu erstellen, und führen dann das Skript aus`checkMTpatch.sh` , um die Patch-Versionen zu überprüfen.
	
	2. Führen Sie das Dienstprogramm Autoconfig aus und übergeben Sie die neue logische Hostnamen-Kontextdatei.
	
	Für Oracle 12.1.0.2:
	
	`cd $ORACLE_HOME/appsutil/bin`
	`$ ./adconfig.sh contextfile=/rdsdbbin/oracle.12.1.customstom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml`
	
	Für Oracle 19c:
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Autoconfig erwartet, dass der Listener-Name mit übereinst immt`CDBNAME`. Daher wird die gesicherte ursprüngliche Listener-Konfigurationsdate i `L_<CDBNAME>_001` vorübergehend verwendet.
	
	`$ lsnrctl stop L_VISCDB_ 001`
	`$ cp -rp /rdsdbdata/ config/listener.ora / rdsdbdata/config/ listener.ora_orig`
	`$ vi /rdsdbdata/ config/listener.ora :%s/L_VISCDB_001/ VISCDB/g`
	`$ lsnrctl start VISCDB`
	`$ cd /rdsdbbin/oracle/a ppsutil`
	`$ . ./txkSetCfgCDB.env dboraclehome=/rdsd bbin/oracle.19.cus tom.r1.EE-CDB.1`
	
	`Oracle Home being passed: /rdsdbbin/ oracle`
	
	`$ echo $ORACLE_HOME /rdsdbbin/orac le.19.custom.r1.EE- CDB.1`
	`$ export ORACLE_SI D=VISCDB`
	`$ cd $ORACLE_HOME/ appsutil/bin`
	`$ perl $ORACLE_H OME/appsutil/bin/t`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`xkPostPDBCreationTasks.pl -dboraclehome=$ORACLE_HOME -outdir=$ORACLE_HOME/appsutil/log -cdbsid=VISCDB -pdbsid=VIS -appsuser=apps -dbport=1521 -servicetype=onpremise`
	
	`Enter the APPS Password: <apps password>`
	
	`Enter the CDB SYSTEM Password:<password from secrets manager>`
	
	Hinweis : Wenn sich Ihre Datenbankverzeichnisse geändert haben, folgen Sie den Anweisungen in Oracle Support Note 2525754.1.	

Konfigurieren der TNS-Einträge für Amazon RDS Custom und Oracle E-Business Suite

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die TNS-Einträge für Amazon RDS Custom und Oracle E-Business Suite.	Autoconfig generiert die TNS-Isole an den Standardspeicherorten. Für Oracle 12.1.0.2 (eine Nicht-CDB) und für Oracle19c PDB ist der Standardspeicherort `$ORACLE_HOME/network/admin/$<CONTEXT_NAME>` . Die CDB für	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Oracle 19c verwendet den Standard-`$ORACLE_HOME/network/admin/` , wie `$TNS_ADMIN` in den Umgebungsdateien definiert , die generiert werden, wenn Sie in den vorherigen Schritten Autoconfig ausgeführt haben. Für Oracle 12.1.0.2 und 19c CDB verwenden Sie diese nicht, da die von Autoconfig `listener.ora` generiert en Dateien `tnsnames.ora` und nicht den Amazon-RD S-Anforderungen entsprech en, z. B. ohne Leerzeichen oder Kommentare. Stattdess en verwenden Sie die generischen Dateien, die in der Amazon-RDS-Custom-Datenbank bereitgestellt werden, um die Complianc e mit den Erwartungen des Systems sicherzustellen und die Fehlerspanne zu reduziere n. Amazon RDS Custom erwartet beispielsweise das folgende Namensformat: `L_<INSTANCE_NAME>_001` Für Oracle 12.1.0.2 wäre dies:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`L_VIS_001`
	
	Für Oracle 19c wäre dies:
	
	`L_VISCDB_001`
	
	Hier ist ein Beispiel für die `listener.ora` Datei, die Sie verwenden werden. Dies wurde generiert, als Sie die Amazon-RDS-Custom-Datenbank erstellt haben. An diesem Punkt haben Sie keine Änderungen an dieser Datei vorgenommen und sie bleibt die Standardeinstellung.
	
	Für Oracle 12.1.0.2:
	
	`$ cd $ORACLE_HOME/network/admin`
	`$ cat listener.ora`
	`ADR_BASE_L_VIS_001=/rdsdbdata/log/`
	`SID_LIST_L_VIS_001=(SID_LIST =`
	`(SID_DESC = (SID_NAME = VIS)(GLOBAL_DBNAME = VIS) (ORACLE_HOME = /rdsdbbin/oracle)))`
	`L_VIS_001=(DESCRIPTION_LIST =`
	`(DESCRIPTION =`
	`(ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION =`
	`(ADDRESS = (PROTOCOL =`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	TCP)(PORT = 1521)(HOST = 127.0.0.1))))
	SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VIS_001=OFF
	
	Für Oracle 19c: Stellen Sie die ursprüngliche `listener.ora` Datei mit dem Listener-Namen wieder her`L_<INSTANCE_NAME>_001` .
	
	$ cd $ORACLE_HOME/network/admin
	
	$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_autoconfig
	$ cp -rp /rdsdbdata/config/listener.ora_orig /rdsdbdata/config/listener.ora
	
	$ cat listener.ora
	SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VISCDB_001=OFF
	ADR_BASE_L_VISCDB_001=/rdsdbdata/log/
	USE_SID_AS_SERVICE_L_VISCDB_001=ON
	L_VISCDB_001=(DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL =	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	TCP)(PORT = 1521)(HOST = 127.0.0.1)))) SID_LIST_L_VISCDB_001= (SID_LIST = (SID_DESC = (SID_NAME = VISCDB)(GLOBAL_DBNAME = VISCDB) (ORACLE_HOME = /rdsdbbin/oracle)))	

	Starten Sie den Listener `L_<INSTANCE_NAME>_001` für standardmäßige Amazon-RDS-Operationen:
	`$ lsnrctl stop`
	`$ lsnrctl start L_VISCDB_001`	

	Für Oracle 12.1.0.2: Bearbeiten Sie die Oracle E-Business Suite-Umgebungsdatei, um den `$TNS_ADMIN` Pfad zur Verwendung der generischen TNS-Iggile von Amazon RDS Custom zu ändern. Die Umgebungsdatei wurde erstellt, als Sie Autoconfig zuvor ausgeführt haben. Bearbeiten Sie die `TNS_ADMIN` Variable, indem Sie das `<CONTEXT_NAME>` Postfix entfernen. Hinweis: Sie sollten die Umgebungsdatei nur in Oracle	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	12.1.0.2 bearbeiten, da das Standardverzeichnis für 19c ist`$ORACLE_HOME/network/admin` , was dem Standard für Amazon RDS Custom entspricht.
	
	Bearbeiten Sie beispielsweise in Oracle 12.1.0.2 die -Datei:
	
	`$ vi $ORACLE_HOME/VIS_oebs-db01log.env`
	
	Ändern Sie den Pfad von:
	
	`TNS_ADMIN=”/rdsdbbin/oracle/network/admin/VIS_oebs-db01log”`
	`export TNS_ADMIN`
	
	auf:
	
	`TNS_ADMIN=”/rdsdbbin/oracle/network/admin”`
	`export TNS_ADMIN`
	
	Hinweis: Jedes Mal, wenn Sie Autoconfig ausführen, müssen Sie diesen Schritt wiederholen, um sicherzustellen, dass die richtigen TNS-Ignile verwendet werden. (nur 12.1.0.2).
	
	Für Oracle 19c:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Ändern Sie den Wert für die Kontextvariable der Datenbankebene `s_cdb_tnsadmin` in `<ORACLE_HOME>/network/admin` anstelle von `<ORACLE_HOME>/network/admin/<CONTEXT_NAME>` .
	
	Hinweis: Aktualisieren Sie die `s_db_tnsadmin` Kontextvariable nicht. Belassen Sie es als `<ORACLE_HOME>/network/admin/<CONTEXT_NAME>` .
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ vi $CONTEXT_FILE`
	
	2. Speichern Sie die Änderungen, die Sie am Wert von vorgenommen habens`_cdb_tnsadmin` .
	
	Die Werte für `s_db_tnsadmin` und `s_cdb_tnsadmin` sollten wie folgt aussehen, wobei der PDB-Name als `VIS` und der logische Name des Datenbankknotens als lautetoebs`-db01log` .
	
	`$ grep -i tns_admin`
	`$CONTEXT_FILE`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<TNS_ADMIN oa_var="s_db_tnsadmin">/rdsdbbin/oracle/network/admin/VIS_oebs-db01log</TNS_ADMIN>
	<CDB_TNS_ADMIN oa_var="s_cdb_tnsadmin">/rdsdbbin/oracle/network/admin</CDB_TNS_ADMIN>
	3. Führen Sie Autoconfig auf der Datenbankebene aus:
	`$ . $ORACLE_HOME/VISCDB_oebs-db01log.env`
	`$ export ORACLE_PDB_SID=VIS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/appsutil/admin/adgrants.sql APPS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/rdbms/admin/utlrp.sql`
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ ./adautocfg.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Legen Sie die Umgebung für den rdsdb-Benutzer fest.	Überspringen Sie diesen Schritt für Oracle 19c.
	
	Für Oracle 12.1.0.2:
	
	Nachdem Sie die Autoconfig- und TNS-Einträge abgeschlossen haben, müssen Sie die Umgebungsdatei laden, indem Sie sie im Profil des `rdsdb`Benutzers festlegen.
	
	Aktualisieren Sie `.bash_profile` , um die `.env` Datenbankdatei der Oracle E-Business Suite aufzurufen. Sie müssen das Profil aktualisieren, um sicherzustellen, dass die Umgebung geladen ist. Diese Umgebungsdatei wurde erstellt, als Sie Autoconfig zuvor ausgeführt haben.
	
	Die folgende Beispielumgebungsdatei wird erstellt, wenn Sie Autoconfig ausführen:
	
	`. /rdsdbbin/oracle/VIS_oebs-db01log.env`
	
	Als `rdsdb` Benutzer:
	
	`cd $HOME`
	`vi .bash_profile`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`export LD_LIBRARY_PATH= ${ORACLE_HOME}/lib:$ {ORACLE_HOME}/ctx/lib export SHLIB_PATH= ${ORACLE_HOME}/lib export PATH=$PATH: ${ORACLE_HOME}/bin alias sql='rlwrap -c sqlplus / as sysdba' . ${ORACLE_HOME}/VIS _oebs-db01log.env` Hinweis: Für Oracle 19c müssen Sie die CDB-Umgebung nicht in laden `.bash_profile` . Dies liegt daran, dass der Standard auf den Standardp fad festgelegt `ORACLE_HO ME` ist `$ORACLE_HOME/ network/admin` , der das Standardverzeichnis des `rdsdb` (Oracle-Stamm)-Ben utzers ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Anwendung und die Datenbank für Amazon RDS Custom.	Führen Sie die ersten beiden Schritte für Oracle 12.1.0.2 und 19c aus. Die nachfolgenden Schritte unterscheiden sich für jede Version. 1. Bearbeiten Sie auf der Anwendungsebene die IP-Adresse für die Datenbank `/etc/hosts` und ändern Sie sie in die benutzerdefinierte IP-Adresse von Amazon RDS: `xx.xx.xx.xx OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log` Da Sie logische Hostnamen verwenden, können Sie den Datenbankknoten fast nahtlos ersetzen. 2. Fügen Sie auf der Amazon RDS Custom DB-Instance die Sicherheitsgruppe hinzu oder ändern Sie sie, die der EC2-Quell-Instance zugewiesen ist, um die Amazon RDS Custom DB-Instance widerzuspiegeln, um sicherzustellen, dass die Anwendung auf den Knoten zugreifen kann. Für Oracle 12.1.0.2:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Führen Sie Autoconfig aus. Führen Sie als Anwendungsbesitzer (z. B. `applmgr`) Folgendes aus:
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	4. Überprüfen Sie die `fnd_nodes` Einträge:
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`--------------------`
	`------------------`
	`------------------`
	`------------------`
	`------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	5. Vergewissern Sie sich, dass Sie sich anmelden und die Anwendung starten können:
	`$ ./adstrtal.sh`
	Für Oracle 19c:
	1. Überprüfen Sie, ob die PDB geöffnet ist, und öffnen Sie sie bei Bedarf:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> show pdbs`
	
	`CON_ID CON_NAME OPEN MODE RESTRICTED`
	`---------- --------- ---------- ----------`
	`2 PDB$SEED READ ONLY NO`
	`3 VIS MOUNTED`
	
	`SQL> alter session set container=vis;`
	
	`SQL> alter database open;`
	
	`SQL> alter database save state;`
	
	2. Testen Sie die Konnektivität als `apps`:
	
	`SQL> sqlplus apps/**** @vis`
	
	3. Führen Sie Autoconfig auf der Datenbankebene aus:
	
	`$ . $ORACLE_HOME/VIS_ebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`
	
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ ./adautocfg.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Führen Sie Autoconfig auf der Anwendungsebene als Anwendungsbesitzer aus (z. B. `applmgr`):
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	5. Überprüfen Sie die `fnd_nodes` Einträge:
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`----------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	6. Starten Sie die Anwendung:
	`$ ./adstrtal.sh`	

Durchführen von Schritten nach der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Setzen Sie die Automatisierung fort, um zu bestätigen, dass sie funktioniert.	Setzen Sie die Automatisierung fort, indem Sie den folgenden AWS CLI-Befehl verwenden:
	`aws rds modify-db-instance \ --db-instance-identifier vis \ --automation-mode full \`
	Die Datenbank wird jetzt von Amazon RDS Custom verwaltet. Wenn beispielsweise der Listener oder die Datenbank ausfällt, startet der Amazon-RDS-Custom-Agent sie neu. Führen Sie dazu Befehle wie die folgenden aus.
	Beispiel für das Stoppen eines Listeners:
	`-bash-4.2$ lsnrctl stop vis`
	Beispiel für das Herunterfahren der Datenbank:
	`SQL> shutdown immediate ;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Schema, Verbindungen und Wartungsaufgaben.	Um die Migration abzuschließen, müssen Sie mindestens die folgenden Aufgaben ausführen. • Führen Sie aus `FS_CLONE`, um das Patch-Dateisystem zu synchronisieren. • Erfassen Sie Schemastatistiken. • Stellen Sie sicher, dass externe Schnittstellen und Systeme eine Verbindung mit der neuen Amazon-RDS-Custom-Datenbank herstellen können. • Richten Sie Ihre Backups und Wartungspläne ein. • Stellen Sie sicher, dass AD Online Patching (ADOP) wie erwartet funktioniert, indem Sie einen Cutover zum Wechseln der Dateisysteme durchführen.	DBA

Fehlerbehebung

Problem	Lösung
Sie erhalten einen ORA-01624-Fehler, wenn Sie versuchen, die Protokolldateien zu löschen.	Wenn Sie beim Versuch, die Protokolldateien zu löschen, einen ORA-01624-Fehler erhalten, gehen Sie folgendermaßen vor.

Problem	Lösung

	Geben Sie den folgenden Befehl aus und warten Sie, bis der Status der Protokolldateien, die Sie löschen möchten, lautet`INACTIVE`. Weitere Informationen zu den Statuscodes in `V$log` finden Sie in der Oracle-Dokumentation. Hier ist ein Beispielbefehl und seine Ausgabe:
	
	`SQL> select group#, status from v$log;`
	
	`GROUP# STATUS`
	`---------- ----------------`
	`1 ACTIVE`
	`2 CURRENT`
	`3 UNUSED`
	`4 UNUSED`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`
	
	In diesem Beispiel lautet die Protokolldatei 1 , `ACTIVE` daher müssen Sie einen Wechsel der Protokolldatei dreimal erzwingen, um sicherzustellen, dass die erste neue Protokolldatei, die Sie zuvor hinzugefügt haben, den Status hat `CURRENT`:
	
	`SQL>  alter system switch logfile;`
	`System altered.`
	`SQL>  alter system switch logfile;`
	`System altered.`
	`SQL>  alter system switch logfile;`
	`System altered.`
	
	Warten Sie, bis alle Protokolldateien, die Sie löschen möchten, sind `INACTIVE`, wie im folgenden Beispiel, und führen Sie dann den `DROP LOGFILE` Befehl aus.

Problem	Lösung

	`SQL> select group#, status from v$log;`
	`GROUP# STATUS`
	`---------- ----------`
	`1 INACTIVE`
	`2 INACTIVE`
	`3 INACTIVE`
	`4 CURRENT`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`

Sie erhalten einen ORA-00392-Fehler, wenn Sie die Datenbank mit öffnen`resetlogs` .	Wenn Sie die Fehlermeldung ORA-00392 erhalten: Protokoll xx von Thread 1 wird gelöscht, die Operation ist nicht zulässig, führen Sie den folgenden Befehl aus (ersetzen Sie `xx` durch die Protokolldateinummer) und führen Sie dann den offenen `resetlogs` Befehl erneut aus:
	`SQL> alter database clear logfile group xx;`
	`SQL> alter database open resetlogs;`

Problem	Lösung

Sie haben Probleme mit der Verbindung mit der Anwendung über Sysadmin oder Anwendung sbenutzer.	Um das Problem zu bestätigen, führen Sie die folgende SQL-Abfrage aus:
	`SQL> select dbms_java.get_jdk_ version() from dual;`
	`select dbms_java.get_jdk_version()`
	` from dual`
	` ERROR at line 1:`
	`ORA-29548: Java system class reported:`
	` release of Java system classes in the database (19.0.0.0.220719 1.8) does`
	` not match that of the oracle executabl e (19.0.0.0.0 1.8)`
	Ursache: Die Quelldatenbank wurde mit mehreren Patches angewendet, aber Amazon RDS Custom `DB_HOME` ist eine neue Installat ion oder die CEV hat nicht alle Patches enthalten, da Sie beim Erstellen der CEV nicht die erforderlichen RSU-Patches wie OJVM verwendet haben. Überprüfen Sie, ob die Quellpatch-Details auf `$ORACLE_H OME/sqlpath` , `$ORACLE_HOME/.patc h_storage` und aufgeführt sind`opatch -lsinventory` .
	Referenz : datapatch -verbose Fails with Error :" Patch xxxxxx: Archiviertes Patch-Ver zeichnis ist leer“ (Dokument-ID 2235541.1)
	Behebung von : Kopieren Sie die fehlenden Patch-bezogenen Dateien aus der Quelle (`$ORACLE_HOME/sqlpatch/`) in Amazon RDS Custom (`$ORACLE_HOME/sqlpatch/`) und führen Sie dann erneut aus`./datapatch -verbose`.

Problem	Lösung

	Beispielsweise:
	`-bash-4.2$ cp -rp 18793246 20204035 20887355 22098146 22731026 $ORACLE_HOME/sqlpatch/`
	Alternativ können Sie eine Problemumgehung verwenden, indem Sie den folgenden Befehl auf der CDB und PDB ausführen:
	`@?/javavm/install/update_javavm_db.sql`
	Führen Sie dann den folgenden Befehl auf der PDB aus:
	`sql> alter session set container=vis; @?/javavm/install/update_javavm_db.sql`
	Führen Sie nun den Test erneut aus:
	`SQL> select dbms_java.get_jdk_version() from dual;`

Zugehörige Ressourcen

- Arbeiten mit Amazon RDS Custom (Amazon-RDS-Dokumentation)
- Amazon RDS Custom für Oracle – Neue Kontrollfunktionen in der Datenbankumgebung (AWS-News-Blog)
- Integrieren von Amazon RDS Custom für Oracle mit Amazon EFS (AWS-Datenbank-Blog)
- Migrieren der Oracle E-Business Suite in AWS (AWS-Whitepaper)
- Oracle E-Business Suite-Architektur in AWS (AWS-Whitepaper)

- Einrichten einer HA/DR-Architektur für Oracle E-Business Suite in Amazon RDS Custom mit einer aktiven Standby-Datenbank (AWS Prescriptive Guidance)

Zusätzliche Informationen

Wartungsvorgänge

Patchen des Oracle-E-Business-Suite-Datenbankverzeichnisses mit neuen Patches

Da das Bin-Volume (`/rdsdbbin`) ein out-of-place Upgrade ist, wird der Inhalt des Bin-Volumes während des CEV-Upgrades gelöscht. Daher müssen Sie eine Kopie des `appsutil` Verzeichnisses erstellen, bevor Sie Upgrades mithilfe von CEV durchführen.

Erstellen Sie auf der Amazon RDS Custom-Quell-Instance vor dem Upgrade der CEV eine Sicherung von `$ORACLE_HOME/appsutil`.

Hinweis: In diesem Beispiel wird ein NFS-Volume verwendet. Sie können jedoch stattdessen eine Kopie in Amazon Simple Storage Service (Amazon S3) verwenden.

1. Erstellen Sie ein Verzeichnis zum Speichern von appsutil auf der Amazon-RDS-Custom-Quell-Instance:

```
$ mkdir /RMAN/appsutil.preupgrade
```

2. Tarieren und kopieren Sie auf das Amazon-EFS-Volume:

```
$ tar cvf /RMAN/appsutil.preupgrade appsutil
```

3. Stellen Sie sicher, dass die tar-Datei vorhanden ist:

```
$ bash-4.2$ ls -l /RMAN/appsutil.preupgrade
-rw-rw-r-- 1 rdsdb rdsdb 622981120 Feb  8 20:16 appsutil.tar
```

4. Führen Sie ein Upgrade auf die neueste CEV durch (Voraussetzung, dass CEV bereits erstellt wurde), indem Sie den Anweisungen unter Upgrade einer RDS Custom DB-Instance in der Amazon RDS-Dokumentation folgen).

Sie können Patches auch direkt mit OPATCH durchführen. Weitere Informationen finden Sie im Abschnitt Anforderungen und Überlegungen für RDS Custom für Oracle Upgrades in der Amazon-RDS-Dokumentation.

Hinweis: Die IP-Adresse des Host-Computers ändert sich während des CEV-Patching-Prozesses nicht. Dieser Prozess führt ein out-of-place Upgrade durch, und beim Start wird ein neues Bin-Volume auf derselben Instance angefügt.

Migrieren von Oracle PeopleSoft zu Amazon RDS Custom

Erstellt von Gaurav Gupta (AWS)

Umgebung: Produktion	Quelle: Amazon EC2	Ziel: Amazon RDS Custom
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Infrastruktur; Datenbanken
AWS-Services: Amazon RDS; Amazon S3; AWS Secrets Manager; Amazon EFS		

Übersicht

Oracle PeopleSoft ist eine Enterprise Resource Planning (ERP)-Lösung für unternehmensweite Prozesse. PeopleSoft verfügt über eine dreistufige Architektur: Client, Anwendung und Datenbank. PeopleSoft kann auf Amazon Relational Database Service (Amazon RDS) ausgeführt werden. Jetzt können Sie auch PeopleSoft auf Amazon RDS Custom ausführen, das Zugriff auf das zugrunde liegende Betriebssystem bietet.

Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und gepackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Wenn Sie Ihre Oracle-Datenbank zu Amazon RDS Custom migrieren, kann Amazon Web Services (AWS) Sicherungsaufgaben und hohe Verfügbarkeit verwalten und sich gleichzeitig auf die Wartung Ihrer PeopleSoft Anwendung und Funktionalität konzentrieren. Die wichtigsten Faktoren, die bei einer Migration zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster konzentriert sich auf die Schritte zur Migration einer PeopleSoft Datenbank in Amazon Elastic Compute Cloud (Amazon EC2) zu Amazon RDS Custom mithilfe eines Oracle Recovery Manager (RMAN)-Backups. Es verwendet ein gemeinsam genutztes Dateisystem von Amazon Elastic File System (Amazon EFS) zwischen der EC2-Instance und Amazon RDS Custom, obwohl Sie auch Amazon FSx oder ein beliebiges gemeinsam genutztes Laufwerk verwenden können. Das Muster verwendet ein vollständiges RMAN-Backup (manchmal auch als Level-0-Backup bezeichnet).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Quelldatenbank der Version 19C, die auf Amazon EC2 mit Oracle Linux 7, Oracle Linux 8, Red Hat Enterprise Linux (RHEL) 7 oder RHEL 8 ausgeführt wird. In den Beispielen für dieses Muster lautet der Name der Quelldatenbank `FSDM092`, dies ist jedoch nicht erforderlich.

  Hinweis: Sie können dieses Muster auch mit lokalen Oracle-Quelldatenbanken verwenden. Sie müssen über die entsprechende Netzwerkkonnektivität zwischen dem On-Premises-Netzwerk und einer Virtual Private Cloud (VPC) verfügen.
- Eine PeopleSoft 9.2-Demo-Instance.
- Eine einzelne PeopleSoft Anwendungsebene. Sie können dieses Muster jedoch so anpassen, dass es mit mehreren Anwendungsebenen funktioniert.
- Amazon RDS Custom ist mit mindestens 8 GB Auslagerungsbereich konfiguriert.

Einschränkungen

Dieses Muster unterstützt die folgenden Konfigurationen nicht:

- Festlegen des `ARCHIVE_LAG_TARGET` Datenbankparameters auf einen Wert außerhalb des Bereichs von 60–7200
- Deaktivieren des DB-Instance-Protokollmodus (`NOARCHIVELOG`)
- Deaktivieren des für Amazon Elastic Block Store (Amazon EBS) optimierten Attributs der EC2-Instance
- Ändern der ursprünglichen EBS-Volumes, die an die EC2-Instance angefügt sind
- Hinzufügen neuer EBS-Volumes oder Ändern des Volume-Typs von gp2 zu gp3
- Ändern des Erweiterungsformats für den `LOG_ARCHIVE_FORMAT` Parameter (erfordert `*.arc`)
- Multiplexing oder Ändern des Speicherorts und des Namens der Kontrolldatei (es muss sein `/rdsdbdata/db/*DBNAME*/controlfile/control-01.ctl`)

Weitere Informationen zu diesen und anderen nicht unterstützten Konfigurationen finden Sie in der Amazon-RDS-Dokumentation.

Produktversionen

Informationen zu Oracle Database-Versionen und Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Anforderungen und Einschränkungen für Amazon RDS Custom für Oracle.

Architektur

Zieltechnologie-Stack

- Application Load Balancer
- Amazon EFS
- Amazon RDS Custom für Oracle
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)

Zielarchitektur

Das folgende Architekturdiagramm stellt ein PeopleSoft System dar, das in einer einzigen Availability Zone in AWS ausgeführt wird. Auf die Anwendungsebene wird über einen Application Load Balancer zugegriffen. Sowohl die Anwendung als auch die Datenbanken befinden sich in privaten Subnetzen, und die Datenbank-Instance von Amazon RDS Custom und Amazon EC2 verwenden ein gemeinsam genutztes Amazon-EFS-Dateisystem, um die RMAN-Sicherungsdateien zu speichern und darauf zuzugreifen. Amazon S3 wird zum Erstellen der benutzerdefinierten RDS-Oracle-Engine und zum Speichern der Metadaten der Redo-Protokolle verwendet.

Tools

Tools

AWS-Services

- Amazon RDS Custom für Oracle ist ein verwalteter Datenbankservice für Legacy-, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Es automatisiert Datenbankverwaltungsaufgaben wie Backups und hohe Verfügbarkeit.
- Amazon Elastic File System (Amazon EFS)hilft Ihnen beim Erstellen und Konfigurieren freigegebener Dateisysteme in der AWS Cloud. Dieses Muster verwendet ein gemeinsam

genutztes Amazon-EFS-Dateisystem, um die RMAN-Sicherungsdateien zu speichern und darauf zuzugreifen.

- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen. In diesem Muster rufen Sie die Passwörter der Datenbankbenutzer von Secrets Manager ab, um die `ADMIN` Benutzer `RDSADMIN` und zu erstellen und die `system` Passwörter `sys` und zu ändern.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Application Load Balancer .

Andere Tools

- Oracle Recovery Manager (RMAN) bietet Backup- und Wiederherstellungsunterstützung für Oracle-Datenbanken. Dieses Muster verwendet RMAN, um ein Hot-Backup der Oracle-Quelldatenbank auf Amazon EC2 durchzuführen, das auf Amazon RDS Custom wiederhergestellt wird.

Bewährte Methoden

- Passen Sie für Datenbankinitialisierungsparameter die Standarddatei an, die von der Amazon RDS Custom DB-Instance für bereitgestellt wird, PeopleSoft anstatt die spfile aus der Oracle-Quelldatenbank zu verwenden. Dies liegt daran, dass Leerzeichen und Kommentare Probleme beim Erstellen von Lesereplikaten in Amazon RDS Custom verursachen. Weitere Informationen zu Datenbankinitialisierungsparametern finden Sie unter Oracle Support Note 1100831.1 (erfordert ein Oracle Support-Konto).
- Amazon RDS Custom verwendet standardmäßig die automatische Speicherverwaltung von Oracle. Wenn Sie den Hugem-Kernel verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass stattdessen die automatische Verwaltung des gemeinsam genutzten Speichers verwendet wird.
- Lassen Sie den `memory_max_target` Parameter standardmäßig aktiviert. Das Framework verwendet dies im Hintergrund, um Lesereplikate zu erstellen.

- Aktivieren Sie Oracle Flashback Database. Diese Funktion ist nützlich, wenn die Standby-Instance in Failover-Testszenarien (nicht in Switchover-Testszenarien) erneut aktiviert wird.

Polen

Einrichten der DB-Instance und des Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die DB-Instance.	Erstellen Sie in der Amazon-RDS-Konsole eine DB-Instance von Amazon RDS Custom für Oracle mit einem DB-Namen namens FSDMO92 (oder Ihrem Quelldatenbanknamen). Anweisungen finden Sie unter Arbeiten mit Amazon RDS Custom in der AWS-Dokumentation und im Blogbeitrag Amazon RDS Custom for Oracle – Neue Kontrollfunktionen in der Datenbankumgebung. Dadurch wird sichergestellt, dass der Datenbankname auf denselben Namen wie die Quelldatenbank festgelegt ist. (Wenn das Feld leer gelassen wird, werden die EC2-Instance und der Datenbankname auf gesetzt`0RCL`.)	DBA

Durchführen einer vollständigen RMAN-Sicherung der Amazon EC2-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Backup-Skript.	Erstellen Sie ein RMAN-Sicherungsskript, um die Datenbank auf dem Amazon EFS-Dateisystem zu sichern, das Sie gemountet haben (`/efs` im folgenden Beispiel). Sie können den Beispielcode verwenden oder eines Ihrer vorhandenen RMAN-Skripte ausführen. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H%M'` `BACKUP_LOG="rman-${ORACLE_SID}-$Dt"` `export TAGDATE=`date +%Y%m%d%H%M`;` `LOGPATH=/u01/scripts/logs` `rman target / >> $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF` `SQL "ALTER SYSTEM SWITCH LOGFILE";` `SQL "ALTER SESSION SET NLS_DATE_FORMAT="DD.MM.YYYY HH24:MI:SS"";` `RUN` `{` `ALLOCATE CHANNEL ch11 TYPE DISK MAXPIECESIZE 5G;` `ALLOCATE CHANNEL ch12 TYPE DISK MAXPIECESIZE 5G;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	` BACKUP AS COMPRESSED BACKUPSET FULL DATABASE FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_FULL' ; SQL "ALTER SYSTEM ARCHIVE LOG CURRENT"; BACKUP FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_ARCHIVE' ARCHIVELOG ALL DELETE ALL INPUT ; BACKUP CURRENT CONTROLFILE FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_CONTROL';}EXIT;EOF`	

Führen Sie das Backup-Skript aus.	Um das RMAN-Sicherungsskript auszuführen, melden Sie sich als Oracle Home User an und führen Sie das Skript aus.
	`$  chmod a+x rman_backup.sh`
	`$ ./rman_backup.sh &`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie auf Fehler und notieren Sie sich den Namen der Sicherungsdatei.	Überprüfen Sie die RMAN-Protokolldatei auf Fehler. Wenn alles in Ordnung aussieht, listen Sie das Backup der Kontrolldatei auf, indem Sie den folgenden Befehl ausführen.
	`RMAN> list backup of controlfile;`
	`using target database control file instead of recovery catalog`
	Notieren Sie sich den Namen der Ausgabedatei.
	`List of Backup Sets`
	`==========`
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`12 Full 21.58M DISK 00:00:01 13-JUL-22`
	`BP Key: 12 Status: AVAILABLE Compressed: NO Tag: TAG20220713T150155`
	`Piece Name: /efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Control File Included: Ckp SCN: 165591599 85898 Ckp time: 13-JUL-22` Sie verwenden die Sicherung skontrolldatei `/efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL` , wenn Sie die Datenbank auf Amazon RDS Custom wiederherstellen.	

Herunterfahren der Ebene der Quellanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die Anwendung herunter.	Um die Ebene der Quellanwendung herunterzufahren, verwenden Sie das `psadmin` Dienstprogramm oder das `psadmin` Befehlszeilendienstprogramm. 1. Führen Sie den folgenden Befehl aus, um den Webserver herunterzufahren. `psadmin -w shutdown -d "webserver domain name"` 2. Führen Sie den folgenden Befehl aus, um den	DBA, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Anwendungsserver herunterzufahren.
	`psadmin -c shutdown -d "application server domain name"`
	3. Führen Sie den folgenden Befehl aus, um den Prozess-Scheduler herunterzufahren.
	`psadmin -p stop -d "process scheduler domain name"`	

Konfigurieren der Amazon-RDS-Custom-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das RPM-Paket nfs-utils.	Führen Sie den folgenden Befehl aus, um das `-nfs-utils rpm`Paket zu installieren. `$ yum install -y nfs-utils`	DBA
Mounten Sie den EFS-Speicher.	Rufen Sie den Amazon-EFS-Mounting-Befehl von der Amazon-EFS-Konsolenseite ab. Mounten Sie das EFS-Dateisystem auf der Amazon-RDS-Instance mithilfe eines	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Network File System (NFS)-Clients. `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-xxxxxxxxxx.efs.eu-west-1.amazonaws.com:/ /efs` `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-xxxxxxxxxx.efs.eu-west-1.amazonaws.com:/ /efs`	

Löschen Sie die Starter-Datenbank und erstellen Sie die Verzeichnisse zum Speichern der Datenbankdateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Anhalten des Automatisierungsmodus.	Sie müssen den Automatisierungsmodus auf Ihrer Amazon RDS Custom DB-Instance anhalten, bevor Sie mit den nächsten Schritten fortfahren, um sicherzustellen, dass die Automatisierung die RMAN-Wiederherstellungsaktivität nicht beeinträchtigt. Sie können die Automatisierung mithilfe der AWS-Konso	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	le oder des AWS Command Line Interface (AWS CLI)-Befehls anhalten (stellen Sie sicher, dass Sie zuerst die AWS CLI konfiguriert haben). `aws rds modify-db-instance \ --db-instance-id entifier peoplesoft-fscm-92 \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Wenn Sie die Dauer der Pause angeben, stellen Sie sicher, dass Sie genügend Zeit für die RMAN-Wied erherstellung lassen. Dies hängt von der Größe der Quelldatenbank ab. Ändern Sie daher den 360-Wert entsprechend. Stellen Sie außerdem sicher, dass sich die Gesamtzeit der angehaltenen Automatis ierung nicht mit dem Backup- oder Wartungsfenster der Datenbank überschneidet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen und Ändern der Parameterdatei für PeopleSoft	Um die pfile für zu erstellen und zu ändern PeopleSoft, verwenden Sie die Standard-pfile, die mit der Amazon RDS Custom DB-Instance erstellt wurde. Fügen Sie die Parameter hinzu, die Sie für benötigen PeopleSoft.
	1. Wechseln Sie zu , `rds user rdsdb` indem Sie den folgenden Befehl ausführen.
	`$ sudo su - rdsdb`
	2. Melden Sie sich bei SQL*Plus in der Starter-D atenbank an und erstellen Sie die pfile-Datei, indem Sie den folgenden Befehl ausführen.
	`SQL> create pfile from spfile;`
	Dadurch wird die pfile in erstellt`$ORACLE_HOME/dbs`.
	3. Erstellen Sie ein Backup dieser Datei.
	4. Bearbeiten Sie die Datei , um PeopleSoftParamete r hinzuzufügen oder zu aktualisieren.
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` *._gby_hash_aggregation_enabled=false *._unnest_subquery=false *.nls_language='AMERICAN' *.nls_length_semantics='CHAR' *.nls_territory='AMERICA' *.open_cursors=1000 *.db_files=1200 *.undo_tablespace='UNDOTBS1' ``` PeopleSoft verwandte Parameter finden Sie in Oracle Support Note 1100831.1. 5. Entfernen Sie die spfile-Referenz aus der pfile-Datei. ``` *.spfile='/rdsdbbin/oracle/dbs/spfileFSDMO92.ora' ```	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie die Starter-Datenbank.	Verwenden Sie den folgenden Code, um die vorhandene Amazon-RDS-Custom-Datenbank zu löschen.
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup mount exclusive restrict;`
	`SQL> drop database;`
	`SQL> exit`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Amazon-RDS-Custom-Datenbank aus dem Backup wieder her.	Stellen Sie die Datenbank mithilfe des folgenden Skripts wieder her. Das Skript stellt zuerst die Kontrolldatei und dann die gesamte Datenbank aus den auf dem EFS-Mount gespeicherten Sicherung steilen wieder her. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H` `%M'` `BACKUP_LOG="rman-${O` `RACLE_SID}-$Dt"` `export TAGDATE=`date +` `%Y%m%d%H%M`;` `LOGPATH=/rdsdbdata/scr` `ipts/logs` `rman target / >>` `$LOGPATH/rman-${OR` `ACLE_SID}-$Dt << EOF` `restore controlfi` `le from "/efs/rma` `n_backup/FSCM/FSDM` `O92_20220713_12_1_` `CONTROL";` `alter database mount;` `run` `{` `set newname for database` `to '/rdsdbdata/db/FSD` `MO92_A/datafile/%f_` `%b';` `SET NEWNAME FOR TEMPFILE` `1 TO '/rdsdbdata/db/` `FSDMO92_A/datafile/%f` `_%b';` `RESTORE DATABASE;` `SWITCH DATAFILE ALL;` `SWITCH TEMPFILE ALL;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	RECOVER DATABASE; } EOF sqlplus / as sysdba >> $LOGPATH/rman-${OR ACLE_SID}-$Dt<<-EOF ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 1.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo01.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 2.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo02.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 3.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo03.log'; alter database clear unarchived logfile group 1; alter database clear unarchived logfile group 2; alter database clear unarchived logfile group 3; alter database open resetlogs; EXIT EOF	

Abrufen von Passwörtern aus Secrets Manager, Erstellen von Benutzern und Ändern von Passwörtern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das Passwort von Secrets Manager ab.	Sie können diesen Schritt über die AWS-Konsole oder die AWS CLI ausführen. Die folgenden Schritte zeigen Anweisungen für die -Konsole. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole. 2. Wählen Sie im Navigationsbereich Datenbanken und dann die Amazon-RDS-Datenbank aus. 3. Wählen Sie die Registerkarte Konfiguration und notieren Sie sich die Ressourcen-ID für die Instance. Es wird das Format haben `db-<ID>` (z. B. `db-73GJNHLGDNZNDOXNWXSECUW6LE`). 4. Öffnen Sie die Secrets Manager-Konsole. 5. Wählen Sie das Secret aus, das denselben Namen wie hat`do-not-delete-custom-<resource_id>` , wobei sich auf die Ressourcen-ID	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`resource-id` bezieht, die Sie in Schritt 3 notiert haben. 6. Wählen Sie Retrieve secret value (Secret-Wert abrufen) aus. Dieses Passwort ist für die `admin` Benutzer `sys`, `systemrdsadmin`, und identisch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den RDSADMIN-Benutzer.	`RDSADMIN` ist der Datenbankbenutzer für die Überwachung und Orchestrierung der Amazon RDS Custom DB-Instance. Da die Starter-Datenbank gelöscht und die Zieldatenbank mit RMAN aus der Quelle wiederhergestellt wurde, müssen Sie diesen Benutzer nach dem Wiederherstellungsvorgang neu erstellen, um sicherzustellen, dass die Amazon RDS Custom-Überwachung wie erwartet funktioniert. Sie müssen auch ein separates Profil und einen Tabellenraum für den `RDSADMIN` Benutzer erstellen.
	
	1. Geben Sie die folgenden Befehle an einer SQL-Eingabeaufforderung ein.
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	`SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Erstellen Sie das Profil RDSADMIN.
	
	`SQL> set echo on feedback on serverout on`
	`SQL> alter session set "_oracle_script"=true;`
	`SQL> CREATE PROFILE RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER_SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_FUNCTION NULL PASSWORD_LOCK_TIME 86400/86400`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PASSWORD_GRACE_TIME 604800/86400; 3. Erstellen Sie den RDSADMIN Tabellenraum. SQL> CREATE BIGFILE TABLESPACE rdsadmin '/rdsdbdata/db/FSD MO92_A/datafile/rd sadmin.dbf' DATAFILE SIZE 7M AUTOEXTEND ON NEXT 1m LOGGING ONLINE PERMANENT BLOCKSIZE 8192 EXTENT MANAGEMEN T LOCAL AUTOALLOCATE DEFAULT NOCOMPRES S SEGMENT SPACE MANAGEMENT AUTO; 4. Erstellen Sie den RDSADMIN Benutzer. Ersetzen Sie das RDSADMIN Passwort durch das Passwort, das Sie zuvor von Secrets Manager erhalten haben. SQL> CREATE USER rdsadmin IDENTIFIED BY xxxxxxxxxx DEFAULT TABLESPACE rdsadmin TEMPORARY TABLESPACE TEMP profile rdsadmin ; 5. Erteilen Sie RDSADMIN Berechtigungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` SQL> GRANT "CONNECT" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "RESOURCE " TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "DBA" TO RDSADMIN; SQL> GRANT "SELECT_C ATALOG_ROLE" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT ALTER SYSTEM TO RDSADMIN; SQL> GRANT UNLIMITED TABLESPACE TO RDSADMIN; SQL> GRANT SELECT ANY TABLE TO RDSADMIN; SQL> GRANT ALTER DATABASE TO RDSADMIN; SQL> GRANT ADMINISTER DATABASE TRIGGER TO RDSADMIN; SQL> GRANT ANY OBJECT PRIVILEGE TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT INHERIT ANY PRIVILEGES TO RDSADMIN; SQL> ALTER USER RDSADMIN DEFAULT ROLE ALL; ``` 6. Set the SYS, SYSTEM, and DBSNMP user profiles to RDSADMIN.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> set echo on feedback on serverout on`
	`SQL> alter user SYS profile RDSADMIN;`
	`SQL> alter user SYSTEM profile RDSADMIN;`
	`SQL> alter user DBSNMP profile RDSADMIN;`	

Erstellen Sie den Hauptbenutzer.	Da die Starter-Datenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie den Hauptbenutzer neu erstellen. In diesem Beispiel lautet der Hauptbenutzername `admin`.
	`SQL> create user admin identified by <password>;`
	`SQL> grant dba to admin`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Systempas swörter.	Ändern Sie die Systempas swörter mithilfe des Passworts , das Sie von Secrets Manager abgerufen haben.
	`SQL> alter user sys identified by xxxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	Wenn Sie diese Passwörter nicht ändern, zeigt Amazon RDS Custom die Fehlermel dung „Der Benutzer oder die Benutzeranmeldeinformatione n für die Datenbanküberwachu ng haben sich geändert“ an.
		DBA

Konfigurieren der TNS-Einträge für Amazon RDS Custom und PeopleSoft

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Datei tnsnames.	Um von der Anwendung sebene aus eine Verbindun g zur Datenbank herzustel len, konfigurieren Sie die `tnsnames.ora` Datei so, dass Sie von der Anwendung sebene aus eine Verbindun g zur Datenbank herstellen können. Im folgenden Beispiel sehen Sie, dass ein Softlink zur `tnsnames.ora` Datei	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	vorhanden ist, die Datei jedoch standardmäßig leer ist.
	
	`$ cd /rdsdbbin/oracle/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 1536 Feb 14 2018 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Apr 5 13:19 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	
	1. Erstellen Sie den `tsnames.ora` Eintrag. Aufgrund der Art und Weise, wie die Amazon-RDS-Automatisierung die Dateien analysiert, müssen Sie sicherstellen, dass der Eintrag keine Leerzeichen, Kommentare oder zusätzliche Zeilen enthält. Andernfalls können bei der Verwendung einiger APIs Probleme auftreten APIs, z.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	B. create-db-instance-read-Replikat .
	2. Ersetzen Sie Port, Host und SID gemäß Ihren PeopleSoft Datenbank anforderungen. Verwenden Sie den folgenden Code als Beispiel.
	`$ vi tnsnames.ora`
	`FSDMO92=(DESCRIP TION = (ADDRESS_ LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_ DATA = (SERVER = DEDICATED) (SID = FSDMO92)))`
	3. Führen Sie den folgenden Befehl aus, um zu bestätige n, dass die PeopleSoft Datenbank erreicht werden kann.
	`$ tnsping FSDMO92`
	`TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 14-JUL-2022 10:16:45`
	`Copyright (c) 1997, 2021, Oracle. All rights reserved.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Used parameter files: /rdsdbbin/oracle/net work/admin/sqlnet. ora Used TNSNAMES adapter to resolve the alias Attempting to contact (DESCRIPT ION = (ADDRESS_ LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_ DATA = (SERVER = DEDICATED) (SID = FSDMO92))) OK (0 msec)	

Erstellen des Spfile- Softlinks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Spfile-Softlink.	1. Führen Sie den folgenden Befehl aus `/rdsdbdata/admin/FSDMO92/pfile` , um spfile am Speicherort zu erstellen. SQL> create spfile='/ rdsdbdata/admin/FS DMO92/pfile/spfile FSDMO92.ora' from pfile; 2. Navigieren Sie zu `$ORACLE_HOME/dbs` und	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellen Sie einen Softlink für die spfile. `ln -s '/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' spfileFSDMO92.ora` 3. Nachdem diese Datei erstellt wurde, können Sie die Datenbank mithilfe der spfile herunterfahren und starten.	

Durchführen von Schritten nach der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie das Schema, die Verbindungen und die Wartungsaufgaben.	Führen Sie die folgenden Schritte aus, um die Migration abzuschließen. • Erfassen Sie Schemasta tistiken. • Stellen Sie sicher, dass die PeopleSoft Anwendung sebene eine Verbindung mit der neuen Amazon-RDS-Custom-Datenbank herstelle n kann. • Richten Sie Ihre Backup- und Wartungspläne ein.	DBA

Zugehörige Ressourcen

- Arbeiten mit Amazon RDS Custom
- Amazon RDS Custom für Oracle – Neue Kontrollfunktionen in der Datenbankumgebung (Blogbeitrag)
- Integrieren von Amazon RDS Custom für Oracle mit Amazon EFS (Blogbeitrag)
- Konfigurieren von Amazon RDS als Oracle PeopleSoft -Datenbank (AWS-Whitepaper)

Migrieren der Oracle ROWID-Funktionalität zu PostgreSQL in AWS

Erstellt von Rakesh Raghav (AWS) und Ramesh Pathuri (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: PostgreSQL-Datenbank in AWS
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora; Amazon RDS; AWS SCT; AWS CLI		

Übersicht

Dieses Muster beschreibt Optionen für die Migration der `ROWID` Pseudospaltenfunktionalität in Oracle Database zu einer PostgreSQL-Datenbank in Amazon Relational Database Service (Amazon RDS) für PostgreSQL , Amazon Aurora PostgreSQL -kompatible Edition oder Amazon Elastic Compute Cloud (Amazon EC2).

In einer Oracle`ROWID`-Datenbank ist die Pseudospalte eine physische Adresse einer Zeile in einer Tabelle. Diese Pseudospalte wird verwendet, um eine Zeile eindeutig zu identifizieren, auch wenn der Primärschlüssel nicht in einer Tabelle vorhanden ist. PostgreSQL hat eine ähnliche Pseudospalte namens `ctid`, kann aber nicht als verwendet werden`ROWID`. Wie in der PostgreSQL-Dokumentation erläutert, `ctid` kann sich ändern, wenn es aktualisiert wird oder nach jedem `VACUUM` Prozess.

Es gibt drei Möglichkeiten, die `ROWID` Pseudospalten-Funktionalität in PostgreSQL zu erstellen:

- Verwenden Sie eine Primärschlüsselspalte anstelle von `ROWID`, um eine Zeile in einer Tabelle zu identifizieren.
- Verwenden Sie einen logischen Primär-/eindeutigen Schlüssel (möglicherweise einen zusammengesetzten Schlüssel) in der Tabelle.
- Fügen Sie eine Spalte mit automatisch generierten Werten hinzu und machen Sie sie zu einem primären/eindeutigen Schlüssel, um nachzuahmen`ROWID`.

Dieses Muster führt Sie durch alle drei Implementierungen und beschreibt die Vor- und Nachteile jeder Option.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Programmierkenntnisse in Procedural Language/PostgreSQL (PL/pgSQL)
- Oracle-Quelldatenbank
- Ein mit Amazon RDS for PostgreSQL oder Aurora PostgreSQL kompatibler Cluster oder eine EC2-Instance zum Hosten der PostgreSQL-Datenbank

Einschränkungen

- Dieses Muster bietet Problemumgehungen für die `ROWID` Funktionalität. PostgreSQL stellt kein Äquivalent zu `ROWID` in Oracle Database bereit.

Produktversionen

- PostgreSQL 11.9 oder höher

Architektur

Quelltechnologie-Stack

- Oracle Database

Zieltechnologie-Stack

- Aurora PostgreSQL – kompatibel, Amazon RDS für PostgreSQL oder eine EC2-Instance mit einer PostgreSQL-Datenbank

Implementierungsoptionen

Es gibt drei Möglichkeiten, die fehlende `ROWID` Unterstützung in PostgreSQL zu umgehen, je nachdem, ob Ihre Tabelle über einen Primärschlüssel oder einen eindeutigen Index, einen logischen Primärschlüssel oder ein Identitätsattribut verfügt. Ihre Wahl hängt von Ihren Projektzeitplänen, Ihrer aktuellen Migrationsphase und Abhängigkeiten vom Anwendungs- und Datenbankcode ab.

Option	Beschreibung	Vorteile	Nachteile
Primärschlüssel oder eindeutiger Index	Wenn Ihre Oracle-Tabelle über einen Primärschlüssel verfügt, können Sie die Attribute dieses Schlüssels verwenden, um eine Zeile eindeutig zu identifizieren.	• Keine Abhängigkeit von proprietären Datenbankfunktionen. • Minimale Auswirkungen auf die Leistung, da Primärschlüsselfelder indiziert sind.	• Erfordert Änderungen am Anwendungs- und Datenbankcode, die `ROWID` für den Wechsel zu Primärschlüsselfeldern benötigt.
Logischer Primär-/eindeutiger Schlüssel	Wenn Ihre Oracle-Tabelle über einen logischen Primärschlüssel verfügt, können Sie die Attribute dieses Schlüssels verwenden, um eine Zeile eindeutig zu identifizieren. Ein logischer Primärschlüssel besteht aus einem Attribut oder einer Reihe von Attributen, die eine Zeile eindeutig identifizieren können, aber er wird nicht durch eine Einschränkung	• Keine Abhängigkeit von proprietären Datenbankfunktionen.	• Erfordert Änderungen am Anwendungs- und Datenbankcode, die `ROWID` für den Wechsel zu Primärschlüsselfeldern benötigt. • Deutliche Auswirkungen auf die Leistung, wenn die Attribute des logischen Primärschlüssels nicht indiziert sind. Sie können jedoch einen eindeutigen Index hinzufüge

	in der Datenbank erzwungen.		n, um Leistungsprobleme zu vermeiden.
Identitätsattribut	Wenn Ihre Oracle-Tabelle keinen Primärschlüssel hat, können Sie ein zusätzliches Feld als erstellen `GENERATED ALWAYS AS IDENTITY`. Dieses Attribut generiert einen eindeutigen Wert, wenn Daten in die Tabelle eingefügt werden, sodass es verwendet werden kann, um eine Zeile für DML-Operationen (Data Manipulation Language) eindeutig zu identifizieren.	• Keine Abhängigkeit von proprietären Datenbankfunktionen. • Die PostgreSQL-Datenbank füllt das Attribut aus und behält seine Eindeutigkeit bei.	• Erfordert Änderungen am Anwendungs- und Datenbankcode, die für den Wechsel `ROWID` zum Identitätsattribut benötigt. • Deutliche Auswirkungen auf die Leistung, wenn das zusätzliche Feld nicht indiziert ist. Sie können jedoch einen Index hinzufügen, um Leistungsprobleme zu vermeiden.

Tools

- Amazon Relational Database Service (Amazon RDS) for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS Cloud.
- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können. In diesem Muster können Sie die AWS CLI verwenden, um SQL-Befehle über pgAdmin auszuführen.

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL . Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, warten und verwenden können.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Polen

Identifizieren der Quelltabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Oracle-Tabellen, die das -`ROWID`Attribut verwenden.	Verwenden Sie das AWS Schema Conversion Tool (AWS SCT), um Oracle-Tabellen zu identifizieren, die über `ROWID` Funktionen verfügen. Weitere Informationen finden Sie in der AWS SCT-Dokumentation. –oder– Verwenden Sie in Oracle die `DBA_TAB_COLUMNS` Ansicht , um Tabellen mit einem -`ROWID`Attribut zu identifizieren. Diese Felder können verwendet werden, um alphanumerische 10-Byte-Zeichen zu speichern. Bestimmen Sie die Nutzung und konvertieren Sie diese gegebenenfalls in ein `VARCHAR` Feld.	DBA oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Code, der auf diese Tabellen verweist.	Verwenden Sie AWS SCT, um einen Migrationsbewertungsbericht zu erstellen, der die von betroffenen Verfahren identifiziert`ROWID`. Weitere Informationen finden Sie in der AWS SCT-Dokumentation. –oder– Verwenden Sie in der Oracle-Quelldatenbank das Textfeld der `dba_source` Tabelle, um Objekte zu identifizieren, die `ROWID` Funktionen verwenden.	DBA oder Entwickler

Ermitteln der Primärschlüsselnutzung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Tabellen, die keine Primärschlüssel haben.	Verwenden Sie in der Oracle-Quelldatenbank , `DBA_CONSTRAINTS` um Tabellen zu identifizieren, die keine Primärschlüssel haben. Diese Informationen helfen Ihnen dabei, die Strategie für jede Tabelle zu bestimmen. Beispielsweise: `select dt.* from dba_tables dt where not exists (select 1`	DBA oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`from all_constraints ct where ct.owner = Dt.owner and ct.table_name = Dt.table_name and ct.constraint_type = 'P' ) and dt.owner = '{schema}'`	

Identifizieren und Anwenden der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie Änderungen für Tabellen an, die einen definierten oder logischen Primärschlüssel haben.	Nehmen Sie die Änderungen am Anwendungs- und Datenbankcode vor, die im Abschnitt Zusätzliche Informationen angezeigt werden, um einen eindeutigen Primärschlüssel oder einen logischen Primärschlüssel zur Identifizierung einer Zeile in Ihrer Tabelle zu verwenden.	DBA oder Entwickler
Fügen Sie Tabellen, die keinen definierten oder logischen Primärschlüssel haben, ein zusätzliches Feld hinzu.	Fügen Sie ein Attribut vom Typ hinzu`GENERATED ALWAYS AS IDENTITY`. Nehmen Sie die Änderungen am Anwendungs- und Datenbankcode vor, die im	DBA oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abschnitt Zusätzliche Informationen angezeigt werden.	
Fügen Sie bei Bedarf einen Index hinzu.	Fügen Sie dem zusätzlichen Feld oder dem logischen Primärschlüssel einen Index hinzu, um die SQL-Leistung zu verbessern.	DBA oder Entwickler

Zugehörige Ressourcen

- PostgreSQL CTID (PostgreSQL-Dokumentation)
- Generierte Spalten (PostgreSQL-Dokumentation)
- ROWID Pseudocolumn (Oracle-Dokumentation)

Zusätzliche Informationen

Die folgenden Abschnitte enthalten Oracle- und PostgreSQL-Codebeispiele zur Veranschaulichung der drei Ansätze.

Szenario 1: Verwenden eines primären eindeutigen Schlüssels

In den folgenden Beispielen erstellen Sie die Tabelle `testrowid_s1` mit `emp_id` als Primärschlüssel.

Oracle-Code:

```
create table testrowid_s1 (emp_id integer, name varchar2(10), CONSTRAINT testrowid_pk
 PRIMARY KEY (emp_id));
INSERT INTO testrowid_s1(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s1(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s1(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s1(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
```

```
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 empname2
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4

UPDATE testrowid_s1 SET name = 'Ramesh' WHERE rowid = 'AAAF3pAAAAAAAMOAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                   EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 Ramesh
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4
```

PostgreSQL-Code:

```
CREATE TABLE public.testrowid_s1
(
    emp_id integer,
    name character varying,
    primary key (emp_id)
);

insert into public.testrowid_s1 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s1 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
```

```
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Szenario 2: Verwenden eines logischen Primärschlüssels

In den folgenden Beispielen erstellen Sie die Tabelle`testrowid_s2` mit `emp_id` als logischem Primärschlüssel.

Oracle-Code:

```
create table testrowid_s2 (emp_id integer, name varchar2(10) );
INSERT INTO testrowid_s2(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s2(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s2(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s2(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 empname2
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4

UPDATE testrowid_s2 SET name = 'Ramesh' WHERE rowid = 'AAAF3rAAAAAAAMeAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 Ramesh
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4
```

PostgreSQL-Code:

```
CREATE TABLE public.testrowid_s2
(
    emp_id integer,
    name character varying
```

```
);

insert into public.testrowid_s2 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s2 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Szenario 3: Verwenden eines Identitätsattributs

In den folgenden Beispielen erstellen Sie die Tabelle`testrowid_s3` ohne Primärschlüssel und mithilfe eines Identitätsattributs.

Oracle-Code:

```
create table testrowid_s3 (name varchar2(10));
INSERT INTO testrowid_s3(name) values ('empname1');
INSERT INTO testrowid_s3(name) values ('empname2');
INSERT INTO testrowid_s3(name) values ('empname3');
INSERT INTO testrowid_s3(name) values ('empname4');
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB empname2
AAAF3sAAAAAAAMmAAC empname3
```

```
AAAF3sAAAAAAAMmAAD empname4

UPDATE testrowid_s3 SET name = 'Ramesh' WHERE rowid = 'AAAF3sAAAAAAAMmAAB' ;
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB Ramesh
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4
```

PostgreSQL-Code:

```
CREATE TABLE public.testrowid_s3
(
    rowid_seq bigint generated always as identity,
    name character varying
);

insert into public.testrowid_s3 (name) values
('empname1'),('empname2'),('empname3'),('empname4');

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         2 | empname2
         3 | empname3
         4 | empname4

update testrowid_s3 set name = 'Ramesh' where rowid_seq = 2 ;

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         3 | empname3
         4 | empname4
         2 | Ramesh
```

Migrieren von Oracle-Database-Fehlercodes zu einer mit Amazon Aurora PostgreSQL kompatiblen Datenbank

Erstellt von Sai Parthasaradhi (AWS) und Veeranjaney Grandhi (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle	Ziel: PostgreSQL
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora		

Übersicht

Dieses Muster zeigt, wie Fehlercodes der Oracle-Datenbank mithilfe einer vordefinierten Metadatentabelle in eine Datenbank der Amazon Aurora PostgreSQL -kompatible Edition migriert werden.

Oracle-Database-Fehlercodes haben nicht immer einen entsprechenden PostgreSQL-Fehlercode. Dieser Unterschied in den Fehlercodes kann es schwierig machen, die Verarbeitungslogik der Prozeduren oder Funktionen in der PostgreSQL-Zielarchitektur zu konfigurieren.

Sie können den Prozess vereinfachen, indem Sie die Quell- und Zieldatenbank-Fehlercodes, die für Ihr PL/pgSQL-Programm von Bedeutung sind, in einer Metadatentabelle speichern. Konfigurieren Sie dann die Tabelle so, dass gültige Oracle-Database-Fehlercodes markiert und ihren PostgreSQL-Entsprechungen zugeordnet werden, bevor Sie mit der verbleibenden Prozesslogik fortfahren. Wenn sich der Oracle Database-Fehlercode nicht in der Metadatentabelle befindet, wird der Prozess mit der Ausnahme beendet. Anschließend können Sie die Fehlerdetails manuell überprüfen und der Tabelle den neuen Fehlercode hinzufügen, wenn Ihr Programm dies erfordert.

Durch die Verwendung dieser Konfiguration kann Ihre mit Amazon Aurora PostgreSQL kompatible Datenbank Fehler genauso behandeln wie Ihre Oracle-Quelldatenbank.

Hinweis: Die Konfiguration einer PostgreSQL-Datenbank zur korrekten Verarbeitung von Oracle-Database-Fehlercodes erfordert in der Regel Änderungen an Datenbank- und Anwendungscode.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank mit Instance- und Listener-Services, die ausgeführt werden
- Ein mit Amazon Aurora PostgreSQL kompatibler Cluster, der betriebsbereit ist
- Vertrautheit mit Oracle Database
- Vertrautheit mit PostgreSQL-Datenbanken

Architektur

Das folgende Diagramm zeigt ein Beispiel für einen mit Amazon Aurora PostgreSQL kompatiblen Datenbank-Workflow für die Validierung und Behandlung von Datenfehlercodes:

Das Diagramm zeigt den folgenden Workflow:

1. Eine Tabelle enthält Oracle Database-Fehlercodes und -Klassifizierungen sowie ihre entsprechenden PostgreSQL-Fehlercodes und -Klassifizierungen. Die Tabelle enthält eine Spalte valid_error, die klassifiziert, ob bestimmte, vordefinierte Fehlercodes gültig sind oder nicht.
2. Wenn eine PL/pgSQL-Funktion (func_processdata) eine Ausnahme auslöst, ruft sie eine zweite PL/pgSQL-Funktion auf (error_validation).
3. Die error_validation-Funktion akzeptiert den Fehlercode der Oracle Database als Eingabeargument. Anschließend überprüft die Funktion den eingehenden Fehlercode anhand der Tabelle, um festzustellen, ob der Fehler in der Tabelle enthalten ist.
4. Wenn der Oracle Database-Fehlercode in der Tabelle enthalten ist, gibt die error_validation-Funktion einen TRUE-Wert zurück und die Prozesslogik wird fortgesetzt. Wenn der Fehlercode nicht in der Tabelle enthalten ist, gibt die Funktion einen FALSE-Wert zurück und die Prozesslogik wird mit einer Ausnahme beendet.
5. Wenn die Funktion einen FALSE-Wert zurückgibt, werden die Fehlerdetails manuell vom Funktionsleiter der Anwendung überprüft, um ihre Gültigkeit zu bestimmen.
6. Der neue Fehlercode wird dann entweder manuell zur Tabelle hinzugefügt oder nicht. Wenn der Fehlercode gültig ist und der Tabelle hinzugefügt wird, gibt die error_validation-Funktion bei der nächsten Ausnahme einen TRUE-Wert zurück. Wenn der Fehlercode nicht gültig ist und der

Prozess fehlschlagen muss, wenn die Ausnahme auftritt, wird der Fehlercode nicht zur Tabelle hinzugefügt.

Technologie-Stack

- Amazon Aurora PostgreSQL
- pgAdmin
- Oracle SQL Developer

Tools

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- pgAdmin ist ein Open-Source-Verwaltungs- und Entwicklungstool für PostgreSQL . Es bietet eine grafische Oberfläche, die die Erstellung, Wartung und Verwendung von Datenbankobjekten vereinfacht.
- Oracle SQL Developer ist eine kostenlose, integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle Database sowohl in herkömmlichen als auch in Cloud-Bereitstellungen vereinfacht.

Polen

Migrieren von Oracle-Database-Fehlercodes zu Ihrer Amazon-Aurora-PostgreSQL-kompatiblen Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle in der mit Amazon Aurora PostgreSQL kompatiblen Datenbank.	Führen Sie den folgenden PostgreSQL-Befehl CREATE TABLE aus: `( source_error_code numeric NOT NULL,`	PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>target_error_code character varying NOT NULL,
	
	valid_error character varying(1) NOT NULL
	
	);</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie der Tabelle PostgreSQL-Fehlercodes und die entsprechenden Oracle Database-Fehlercodes hinzu.	Führen Sie den PostgreSQL INSERT-Befehl aus, um der Tabelle error_codes die erforderlichen Fehlercodewerte hinzuzufügen.
	
	Die PostgreSQL-Fehlercodes müssen den zeichenvariierenden Datentyp (SQLSTATE-Wert) verwenden. Die Oracle-Fehlercodes müssen den numerischen Datentyp (SQLCODE-Wert) verwenden.
	
	Beispielanweisungen einfügen:
	
	`insert into error_codes values (-1817,'22007','Y');`
	`insert into error_codes values (-1816,'22007','Y');`
	`insert into error_codes values (-3114,'08006','N');`
	
	Hinweis: Wenn Sie Oracle-spezifische JDBC-Ausnahmen (Java Database Connectivity) abfangen, müssen Sie diese Ausnahmen entweder durch generische datenbankübergreifende Ausnahmen ersetzen oder zu PostgreSQ
		PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	L-spezifischen Ausnahmen wechseln.	
Erstellen Sie eine PL/pgSQL-Funktion, um Fehlercodes zu validieren.	Erstellen Sie eine PL/pgSQL-Funktion, indem Sie den PostgreSQL-Befehl CREATE FUNCTION ausführen. Stellen Sie sicher, dass die Funktion Folgendes tut: • Akzeptiert die von einem Programm ausgegebenen Oracle-Fehlercodes. • Prüft, ob Fehlercodes in der error_codes-Tabelle vorhanden sind. • Gibt den Wert TRUE oder FALSE zurück, basierend darauf, ob der Fehlercod e in der Metadatentabelle vorhanden ist oder nicht.	PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie neue Fehlercodes manuell, während sie von der PL/pgSQL-Funktion aufgezeichnet werden.	Überprüfen Sie die neuen Fehlercodes manuell. Wenn ein neuer Fehlercode für Ihren Anwendungsfall gültig ist, fügen Sie ihn der error_codes-Tabelle hinzu, indem Sie den PostgreSQL INSERT-Befehl ausführen. –oder– Wenn ein neuer Fehlercode für Ihren Anwendungsfall nicht gültig ist, fügen Sie ihn nicht zur Tabelle hinzu. Die Prozesslogik schlägt weiterhin fehl und wird mit Ausnahme beendet, wenn der Fehler auftritt.	PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Zugehörige Ressourcen

Anhang A. PostgreSQL-Fehlercodes (PostgreSQL-Dokumentation)

Datenbankfehlermeldungen (Dokumentation zu Oracle Database)

Migrieren von Redis-Workloads zu Redis Enterprise Cloud in AWS

Erstellt von Antony Prasad Thevaraj (AWS) und Sivas Pendyala (Redis)

Umgebung: Produktion	Quelle: On-Premises-Datenbank (Redis oder andere)	Ziel: Redis Enterprise Cloud in AWS
R-Typ: Plattformwechsel	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; Amazon S3		

Übersicht

In diesem Muster wird der allgemeine Prozess für die Migration von Redis-Workloads zu Redis Enterprise Cloud in Amazon Web Services (AWS) erörtert. Es beschreibt die Migrationsschritte, enthält Informationen zur Auswahl der verfügbaren Tools und erläutert die Vor- und Nachteile sowie die Schritte zur Verwendung der einzelnen Tools. Wenn Sie zusätzliche Unterstützung bei der Migration von Workloads von Redis benötigen, können Sie optional Redis Professional Services einbeziehen.

Wenn Sie Redis OSS oder Redis Enterprise Software On-Premises ausführen, sind Sie mit dem erheblichen Verwaltungsaufwand und der betrieblichen Komplexität der Wartung Ihrer Redis-Datenbanken in Ihrem Rechenzentrum vertraut. Durch die Migration Ihrer Workloads in die Cloud können Sie diesen betrieblichen Aufwand erheblich reduzieren und Redis Enterprise Cloud nutzen, ein vollständig gehostetes DBaaS-Angebot (Database as a Service) von Redis. Diese Migration trägt dazu bei, Ihre geschäftliche Agilität zu erhöhen, die Anwendungszuverlässigkeit zu verbessern und die Gesamtkosten zu senken, während Sie Zugriff auf die neuesten Features von Redis Enterprise Cloud in AWS erhalten, z. B. 99,999 % Verfügbarkeit, architektonische Einfachheit und Skalierung.

Es gibt potenzielle Anwendungen für Redis Enterprise Cloud in den Bereichen Finanzdienstleistungen, Einzelhandel, Gesundheitswesen und Spiele sowie in Anwendungsfällen, die Lösungen für Betrugserkennung, Echtzeitinventar, Bearbeitung von Ansprüchen und Sitzungsmanagement erfordern. Sie können Redis Enterprise Cloud verwenden, um eine Verbindung zu Ihren AWS-Ressourcen herzustellen, z. B. zu einem Anwendungsserver, der auf Amazon Elastic

Compute Cloud (Amazon EC2)-Instances ausgeführt wird, oder zu einem Microservice, der als AWS Lambda-Service bereitgestellt wird.

Voraussetzungen und Einschränkungen

Annahmen

- Sie betreiben derzeit ein On-Premises-Datenbanksystem, das Sie in die Cloud migrieren möchten.
- Sie haben die Migrationsanforderungen für Ihre Workloads identifiziert, darunter:
  - Anforderungen an die Datenkonsistenz
  - Anforderungen an Infrastruktur und Systemumgebung
  - Datenzuordnung und Transformationsanforderungen
  - Anforderungen an Funktionstests
  - Leistungstestanforderungen
  - Validierungsanforderungen
  - Definierte Cutover-Strategie
- Sie haben die für die Migration erforderlichen Zeitpläne und Kostenschätzungen bewertet.
- Ihre Anforderungen berücksichtigen den Umfang der Arbeit und die Systeme und Datenbanken, die Sie als Teil der Migration identifiziert haben.
- Sie haben die Stakeholder zusammen mit ihren Rollen und Verantwortlichkeiten in einer RACI-Matrix (verantwortbar, rechenschaftspflichtig, konsultiert, informiert) identifiziert.
- Sie haben die erforderliche Vereinbarung und Genehmigungen von allen Stakeholdern erhalten.

Kosten

Abhängig von den technischen Spezifikationen Ihrer vorhandenen Quelldatenbank (z. B. Speichergröße, Durchsatz und Gesamtdatengröße) kann ein Redis-Lösungsarchitekt das Zielsystem in Redis Enterprise Cloud dimensionieren. Allgemeine Preisinformationen finden Sie unter Redis-Preise auf der Redis-Website.

Personen und Fähigkeiten

Der Migrationsprozess umfasst die folgenden Rollen und Verantwortlichkeiten.

Rolle	Beschreibung	Erforderliche Fähigkeiten

Architektur der Migrationslösungen	Ein technischer Architekt, der über Fachwissen bei der Definition, Planung und Implementierung von Migrationsstrategien verfügt	Kenntnisse der Quell- und Zielsysteme auf technischer und Anwendungsebene; Erfahrung mit der Migration von Workloads in die Cloud
Datenarchitekt	Ein technischer Architekt mit umfassender Erfahrung in der Definition, Implementierung und Bereitstellung von Datenlösungen für eine Vielzahl von Datenbanken	Datenmodellierung für strukturierte und unstrukturierte Daten, fundiertes Verständnis und Erfahrung bei der Implementierung von Datenbanken für ein Unternehmen
Redis-Lösungsarchitekt	Ein technischer Architekt, der beim Entwerfen eines Redis-Clusters mit optimaler Größe für den entsprechenden Anwendungsfall helfen kann	beim Entwerfen und Bereitstellen von Redis-Lösungen für eine Vielzahl von Anwendungsfällen
Architektur für Cloud-Lösungen	Ein technischer Architekt, der ein tieferes Verständnis von Cloud-Lösungen hat, insbesondere in AWS	beim Entwerfen von Lösungen für die Cloud; Workload-Migration und Anwendungs-Modernisierungserfahrung
Unternehmensarchitekt	Ein technischer Architekt, der ein vollständiges Verständnis der technischen Landschaft in Ihrer Organisation hat, der eine gemeinsame Vision für die zukünftige Roadmap hat und der standardisierte architektonische bewährte Methoden für alle Teams in Ihrer Organisation praktiziert und einrichtet	Softwarearchitektur-Zertifizierungen wie TOGAF, grundlegende Softwareentwicklungsfähigkeiten und Lösungsarchitektur und Unternehmensarchitekturwissen

IT oder DevOps Techniker	Ein Techniker, der für die Erstellung und Wartung der Infrastruktur verantwortlich ist, einschließlich der Überwachung der Infrastruktur auf Probleme, der Durchführung von Wartungsaufgaben und der nach Bedarf erforderlichen Updates.	Starkes Verständnis verschiedener Technologien, darunter Betriebssysteme, Netzwerke und Cloud Computing; Vertrautheit mit Programmiersprachen wie Python, Bash und Ruby sowie Tools wie Docker, Kubernetes und Ansible

Architektur

Migrationsoptionen

Das folgende Diagramm zeigt Optionen für die Migration Ihrer lokalen (Redis-basierten oder anderen) Datenquellen zu AWS. Es zeigt mehrere Migrationstools, aus denen Sie wählen können, z. B. das Exportieren von Redis Database (RDB)-Dateien nach Amazon Simple Storage Service (Amazon S3), die Verwendung der Redis-Replikationsfunktion oder die Verwendung von AWS DMS.

1. On-Premises-Datenquellen: Datenbanken, die nicht auf Redis basieren, wie MySQL ,PostgreSQL, Oracle, SQL Server oder MariaDB.
2. On-Premises-Datenquellen: Protokollbasierte Redis-Datenbanken wie Redis OSS und Redis Enterprise Software.
3. Die einfachste Möglichkeit, Daten aus Redis-basierten Datenbanken zu migrieren, besteht darin, RDB-Dateien zu exportieren und sie in die Redis Enterprise Cloud in AWS zu importieren.
4. Alternativ können Sie die Daten mithilfe der Replikationsfunktion (`ReplicaOf`) in Redis von der Quelle zum Ziel migrieren.
5. Wenn Ihre Anforderungen an die Datenmigration die Datentransformation beinhalten, können Sie Redis Input/Output Tools (RIOT) verwenden, um die Daten zu migrieren.
6. Alternativ können Sie AWS Data Migration Service (AWS DMS) verwenden, um die Daten aus SQL-basierten Datenbanken zu migrieren.
7. Sie müssen Virtual Private Cloud (VPC)-Peering für AWS DMS verwenden, um die Daten erfolgreich in die Redis Enterprise Cloud in AWS zu migrieren.

Zielarchitektur

Das folgende Diagramm zeigt eine typische Bereitstellungsarchitektur für Redis Enterprise Cloud in AWS und veranschaulicht, wie es mit wichtigen AWS-Services verwendet werden kann.

1. Sie können eine Verbindung zu den Geschäftsanwendungen herstellen, die von Redis Enterprise Cloud in AWS unterstützt werden.
2. Sie können Geschäftsanwendungen in Ihrem eigenen AWS-Konto in einer VPC innerhalb dieses Kontos ausführen.
3. Sie können Datenbankendpunkte von Redis Enterprise Cloud verwenden, um eine Verbindung zu Ihren Anwendungen herzustellen. Beispiele hierfür sind ein Anwendungsserver, der auf EC2-Instances ausgeführt wird, ein Microservice, der als AWS Lambda-Service bereitgestellt wird, eine Amazon Elastic Container Service (Amazon ECS)-Anwendung oder eine Amazon Elastic Kubernetes Service (Amazon EKS)-Anwendung.
4. Geschäftsanwendungen, die in Ihrer VPC ausgeführt werden, benötigen eine VPC-Peer-Verbindung zur Redis Enterprise Cloud VPC. Auf diese Weise können sich die Geschäftsanwendungen sicher über private Endpunkte verbinden.
5. Redis Enterprise Cloud in AWS ist eine speicherinterne NoSQL-Datenbankplattform, die als DBaaS in AWS bereitgestellt wird und vollständig von Redis verwaltet wird.
6. Redis Enterprise Cloud wird innerhalb einer VPC in einem von Redis erstellten Standard-AWS-Konto bereitgestellt.
7. Aus Sicherheitsgründen wird Redis Enterprise Cloud in einem privaten Subnetz bereitgestellt, auf das sowohl private als auch öffentliche Endpunkte zugreifen können. Wir empfehlen Ihnen, Ihre Client-Anwendungen mit Redis auf privaten Endpunkten zu verbinden. Wenn Sie einen öffentlichen Endpunkt verwenden möchten, empfehlen wir dringend, TLS zu aktivieren, um die Daten zwischen Ihren Clientanwendungen und Redis Enterprise Cloud zu verschlüsseln.

Die Redis-Migrationsmethode entspricht der AWS-Migrationsmethode, die unter Mobilisieren Ihrer Organisation zur Beschleunigung umfangreicher Migrationen auf der Website AWS Prescriptive Guidance dargestellt ist.

Automatisierung und Skalierung

Die Aufgaben zur Umgebungseinrichtung für die Migration können zur Automatisierung und Skalierung über AWS Landing Zone- und Infrastructure as Code (IaC)-Vorlagen automatisiert werden. Diese werden im Abschnitt „Epics“ dieses Musters erörtert.

Tools

Je nach Ihren Anforderungen an die Datenmigration können Sie aus einer Auswahl technologischer Optionen wählen, um Ihre Daten zu Redis Enterprise Cloud in AWS zu migrieren. In der folgenden Tabelle werden diese Tools beschrieben und verglichen.

Tool	Beschreibung	Vorteile	Nachteile
RDB-Export und -Import	Sie exportieren die Daten aus der Quelldatenbank (z. B. Redis OSS oder Redis Enterprise Software) in Form von RDB-Dateien. Wenn Ihre Datenbank über einen Redis-OSS-Cluster bereitgestellt wird, exportieren Sie jeden Master-Shard in eine RDB. Anschließend importieren Sie alle RDB-Dateien in einem Schritt. Wenn Ihre Quelldatenbank auf einem OSS-Cluster basiert, Ihre Zieldatenbank jedoch nicht die OSS-Cluster-API verwendet, müssen Sie Ihren Anwendungsquellcode ändern,	• Einfach. • Funktioniert mit jeder Redis-basierten Lösung, die Daten im RDB-Format als Quelle exportieren kann (einschließlich Redis OSS und Redis Enterprise Software). • Erzielt Datenkonsistenz mit einem einfachen Prozess.	• Erfüllt keine Datentransformationsanforderungen und unterstützt keine logischen Datenbank zusammenführungen. • Zeitaufwändig für größere Datensätze. • Keine Delta-Migrationsunterstützung kann zu längeren Ausfallzeiten führen.

	um eine Standard-Redis-Clientbibliothek zu verwenden.	
	Datentransformationsanforderungen oder logische Datenbank zusammenführungen erfordern einen komplexeren Prozess, der später in dieser Tabelle unter Logische Datenbank zusammenführung erläutert wird.	

Redis-Replikationsfunktion (aktiv-passiv)	Sie können kontinuierlich Daten aus einer Redis-OSS-, Enterprise-Software- oder Enterprise-Cloud-Datenbank in eine Redis-Enterprise-Cloud-Datenbank replizieren. Nach der ersten Synchronisation führt die Redis-Replikationsfunktion (`ReplicaOf `) eine Delta-Migration durch, was bedeutet, dass es fast keine beobachteten Anwendungsausfälle gibt. Die Redis-Replikationsfunktion ist für die Verwendung auf Aktiv-Passiv- Weise vorgesehen. Es wird davon ausgegangen, dass das Ziel passiv ist und vollständig neu synchronisiert wird (aus der Quelldatenbank geschärft und synchronisiert). Daher ist das Umschalten zwischen der Quelle und dem Ziel etwas komplizierter.	• Unterstützt die kontinuierliche Replikation (anfängliches Laden von Daten gefolgt von Deltas). • Fast keine Ausfallzeit (abhängig von der Replikationsverzögerung). • Erzielt Datenkonsistenz.	• Nur ein Standort soll aktiv sein, sodass der Wechsel zwischen den Standorten komplizierter ist. • Unterstützt maximal 32 Master-Shards, wenn Sie von einem OSS-Cluster migrieren.

	Es ist möglich, eine Replikation von einem Redis-OSS -Cluster zu einer standardmäßigen geclusterten Redis Enterprise Cloud-Datenbank durchzuführen, indem Sie alle Master-Shards des OSS-Clusters als Quellen angeben. Die Redis-Replikationsfunktion erlaubt jedoch maximal 32 Quelldatenbanken.		
AWS DMS	Sie können AWS DMS verwenden, um Daten mit minimalen Ausfallzeiten von jeder unterstützten Quelldatenbank in einen Redis-Zieldatenspeicher zu migrieren. Weitere Informationen finden Sie unter Verwenden von Redis als Ziel für AWS DMS in der AWS DMS-Dokumentation.	• Unterstützt die Migration von NoSQL- und SQL-Datenquellen. • Funktioniert gut mit anderen AWS-Services. • Unterstützt Anwendungsfälle für Live-Migration und Change Data Capture (CDC).	• Redis-Schlüsselwerte dürfen keine Sonderzeichen wie % enthalten. • Unterstützt nicht die Migration von Daten, die Sonderzeichen in Zeilen oder Feldnamen enthalten. • Unterstützt den Modus des vollständigen großen Binärobjekts (LOB) nicht.

Zusammenführung logischer Datenbanken	Spezielle Anforderungen an die Datenbank zusammenführung erfordern möglicherweise eine benutzerdefinierte Datenmigrationslösung. Beispielsweise könnten Sie vier logische Datenbanken (`SELECT 0..3`) in Redis OSS haben, aber Sie möchten vielleicht einen einzelnen Datenbankendpunkt verwenden, anstatt die Daten in mehrere Redis Enterprise Cloud-Datenbanken zu verschieben. Redis Enterprise unterstützt keine auswählbaren logischen Datenbanken, daher müssten Sie das physische Datenmodell der Quelldatenbank transformieren. Sie können beispielsweise jeden Datenbankindex einem Präfix zuordnen (`0` zu `usr`, `1` zu `cmpusw`.) und dann	• Detaillierte Kontrolle über die Anpassung der Daten während der Migration zum Zielsystem mithilfe von benutzerdefinierten Skripts.	• Wenn Sie sich entscheiden, die Migration nicht abzuschließen, kann das Rollback sehr schwierig sein, insbesondere wenn neuere Daten auf Quellsysteme zurückgesetzt werden müssen. • Die Entwicklungskosten können hoch sein, wenn das Ziel darin besteht, eine einmalige Lösung für eine einmalige Migration zu entwickeln. • Die Wartungskosten für Code, Infrastruktur, Entwicklungszeit und andere Bereiche können hoch sein, wenn sich die Migration sanforderungen häufig ändern.

	ein Migrationsskript oder ein Extract, Transform, Load (ETL)-Tool verwenden , um eine RDB-Datei auszugeben, die Sie dann in die Zieldaten bank importieren können.

Darüber hinaus können Sie die folgenden Tools und Services von AWS verwenden.

Bewertungs- und Erkennungstools:

- AWS Application Discovery Service
- Migration Evaluator

Tools zur Anwendungs- und Servermigration:

- AWS Application Migration Service

Tools zur Datenbankmigration:

- AWS Schema Conversion Tool (AWS SCT)
- AWS Database Migration Service (AWS DMS)

Tools zur Datenmigration:

- AWS Storage Gateway
- AWS DataSync
- AWS Direct Connect
- AWS Snowball
- Amazon Data Firehose

Migrationsverwaltung:

- AWS Migration Hub

AWS-Partnerlösungen:

- AWS-Kompetenzpartner für Migration

Epics

Erledigen von Erkennungs- und Bewertungsaufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Workloads.	Identifizieren Sie die geeigneten Kandidaten-Workloads, die Sie migrieren möchten. Berücksichtigen Sie Folgendes, bevor Sie einen Workload für die Migration auswählen: • Was ist der geschäftliche Wert bei der Migration oder nicht? • Gibt es einen Notfallplan, wenn dieser Workload nicht erfolgreich zum Zielsystem migriert? Wählen Sie idealerweise einen Workload aus, der maximale Auswirkungen auf das Geschäft mit minimalen Risiken hat. Behalten Sie den gesamten Prozess iterativ bei und migrieren Sie sie in kleinen Schritten.	Datenarchitekt, Geschäfts experten, Sponsoren von Migrationsprojekten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Datenquellen und -anforderungen; entwerfen Sie ein Datenmodell.	Redis führt einen Workshop durch, um die Erkennung zu beschleunigen und die Migrationsplanung für das Projekt zu definieren. Im Rahmen dieses Workshops identifizieren Redis-Teams die Datenquellen und Anforderungen an das Quelldatenmodell und analysieren, wie diese in Redis Enterprise Cloud umgestellt werden können. Das Redis-Migrationsteam (Pro Professionalal Services) führt eine detaillierte Übung zum Datenmodelldesign mit Ihrer Organisation durch. Im Rahmen dieser Übung hat das Redis-Team: • Identifiziert Ziel-Redis-Datenstrukturen. • Definiert die Datenzuordnungsstrategie. • Dokumentiert den Migrationsansatz und die Empfehlungen. • Prüft und schließt das Datenmodell mit den Stakeholdern ab.	Redis-Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Eigenschaften der Quelldatenbank.	Identifizieren Sie das Redis-Produkt, das in den Quell- und Zielumgebungen verwendet wird. Beispielsweise: • Ist die Quelldatenbank eine OSS-Cluster-Datenbank, eine eigenständige Redis-Datenbank oder eine Redis-Enterprise-Datenbank? • Ist die Zieldatenbank eine Redis Enterprise-Standarddatenbank oder eine OSS Cluster-kompatible Datenbank? • Welche Auswirkungen hat der Quellcode der Anwendung?	Datenarchitekt
Erfassen Sie die aktuelle System-SLA und andere Größenmetriken.	Bestimmen Sie die aktuellen Service Level Agreements (SLAs), ausgedrückt in Bezug auf Durchsatz (Operationen pro Sekunde), Latenz, Gesamtspeichergröße pro Datenbank und Hochverfügbarkeitsanforderungen (HA).	Datenarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Eigenschaften des Zielsystems.	Bestimmen Sie die Antworten auf diese Fragen: • Wie viele Daten müssen migriert werden? • Wie lange dauert es, bis die angegebene Datenmenge migriert wird? • Was sind die Ausfallzeiten für die Migration? Ist es akzeptabel, dass Ihr Service oder Ihre Anwendung für einen bestimmten Zeitraum nicht verfügbar ist? Wenn ja, wie lange? • Wie konsistent sollten die migrierten Daten sein? Kann sich die Zieldatenbank in einem leicht inkonsistenten (veralteten) Zustand befinden? • Müssen Daten transformiert werden, bevor sie in die Zieldatenbank geladen werden? (Sie können beispielsweise auswählbare DB-Indizes vor der Migration in Präfixe konvertieren.) • Ist die Quelldatenbank vom Host der Zieldatenbank aus erreichbar (z. B. von einer Peer-VPC oder von einem öffentlichen Endpunkt mit Verschlüsselung)?	Datenarchitekt, Redis-Lösungsarchitekt (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Schließen Sie eine Übung zur Datengröße und Redis-Clustergröße mit einem Redis-Technikarchitekten ab. • Identifizieren Sie Netzwerkanforderungen, Infrastrukturanforderungen, Softwareversionen und Softwarelizenzierung und beziehen Sie alle Komponenten vor der Migration. • Sind mit der Übertragung dieser Daten Sicherheitsprobleme verbunden?	
Identifizieren Sie Abhängigkeiten.	Identifizieren Sie die Upstream- und Downstream-Abhängigkeiten des aktuellen zu migrierenden Systems. Stellen Sie sicher, dass die Migrationsarbeit mit anderen abhängigen Systemmigrationen übereinstimmt. Wenn Sie beispielsweise planen, andere Geschäftsanwendungen von On-Premises in die AWS Cloud zu migrieren, identifizieren Sie diese Anwendungen und richten Sie sie auf der Grundlage von Projektzielen, Zeitplänen und Stakeholdern aus.	Datenarchitekt, Unternehmensarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Migration stools.	Abhängig von Ihren Anforderungen an die Datenmigration (z. B. Quelldaten oder Ausfallzeiten) können Sie jedes der zuvor im Abschnitt Tools beschriebenen Tools verwenden. Darüber hinaus können Sie Folgendes verwenden: • Bidirektionale (aktiv-aktiv) Replikation mithilfe der CRDB-Bereitstellung. • Benutzerdefinierte Export-/Importskripte (z. B. mithilfe von `-DUMP/RESTORE` Befehlen). • Zusätzliche Export-/Import-Tools und Hilfstools wie RIOT-, ECstats2- oder ETL-Tools. • IaC-Tools wie Terraform oder AWS- CloudFormation Vorlagen.	Architektur für Migrationslösungen, Architekturarchitekt für Redis-Lösungen
Erstellen Sie einen Notfallplan.	Richten Sie einen Notfallplan ein, der zurückgesetzt werden soll, falls während der Migration Probleme auftreten.	Projektmanagement, technische Teams, einschließlich Architekt

Abschließen von Sicherheits- und Compliance-Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sichern Sie die Redis-Verwaltungskonsole.	Um die Administrationskonsole zu sichern, folgen Sie den Anweisungen in der Redis-Dokumentation.	IT-Infrastrukturadministrator
Sichern Sie die Redis-Datenbank.	Weitere Informationen finden Sie auf den folgenden Seiten der Redis-Dokumentation: • Definieren Sie die rollenbasierte Zugriffskontrolle . • Definieren Sie die Netzwerksicherheit. • Aktivieren Sie TLS .	
Sichere Redis-Cloud-APIs .	Wenn Sie die API aktivieren, können Sie die API-Schlüssel für alle Besitzer Ihres Redis-Cloud-Kontos verwalten. Eine Übersicht über die Sicherheitsfunktionen der API finden Sie in der Dokumentation zur API-Authentifizierung auf der Redis-Website.	IT-Infrastrukturadministrator

Einrichten der neuen Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine neue Umgebung in AWS ein.	Diese Aufgabe umfasst:	IT oder DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• AWS Landing Zone-Einrichtungsaktivitäten. Die Landing Zone unterstützt:
	  • Bereitstellungen mit mehreren Konten
	  • Minimale Sicherheitsbasis
	  • Automatisierte Methode zur Bereitstellung neuer Konten mit einer Sicherheitsbasis und ISV-Voraussetzungen (Netzwerk, Sicherheitskonfiguration usw.)
	  • Benachrichtigungen, zentrale Protokollierung und Überwachung
	• ISV-Softwarekonfigurationsaktivitäten. Dazu gehören Konfigurationen, die in die Migration aufgenommen werden müssen, wie Produkt- und Workload-Einstellungen und -Änderungen.
	• IaC-Aktivitäten wie das Konfigurieren oder Anpassen von AWS-CloudFormation oder Terraform-Vorlagen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Migration sarchitektur bereit.	1. Richten Sie Redis Enterpris e Cloud in AWS ein. 2. Installieren Sie Migration stools wie RIOT oder AWS DMS. Eine Liste der verfügbaren Tools finden Sie im Abschnitt Tools. 3. Stellen Sie die Konnektivität zwischen den Anwendung s-, Migrations- und Datenbankebenen her. 4. Erstellen Sie einen Beispiel-Workload, der jede Ebene durchlaufen und einen kleinen Satz von Beispield aten migrieren kann. Sie können jetzt die eigentlic hen Datenmigrationspipelines ausführen und testen.	IT oder DevOps Techniker

Einrichten von Netzwerken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Konnektivität her.	Stellen Sie Konnektivität zwischen der On-Premises-Infrastruktur und AWS Cloud-Ressourcen her. Verwenden Sie Sicherheitsgruppen, AWS Direct Connect und andere Ressourcen, um diese Funktionalität zu erreichen.	IT oder DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Verbinden Ihres Rechenzentrums mit AWS auf der AWS-Website.	
Richten Sie VPC-Peering ein.	Richten Sie ein VPC-Peering zwischen den VPCs ein, auf denen Geschäftsanwendungen ausgeführt werden (oder den EC2-Instances, auf denen Migrationstools oder der AWS DMS-Replikationsserver ausgeführt werden), und der VPC, auf der Redis Enterprise Cloud ausgeführt wird. Anweisungen finden Sie unter Erste Schritte mit Amazon VPC in der Amazon-VPC-Dokumentation und Aktivieren von VPC-Peering in der Redis-Dokumentation.	IT oder DevOps Techniker

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein Datenmigrationstool aus.	In der Tabelle im Abschnitt Tools finden Sie Beschreibungen, Vor- und Nachteile dieser Tools: • RDS-Export und -Import • Redis-Replikationsfunktion (`ReplicaOf `)	Architektur der Migrationslösungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• AWS DMS • Zusammenführung logischer Datenbanken In den folgenden Zeilen werden die Datenmigr ationsaufgaben beschrieben, die jedem Tool zugeordnet sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1: Verwenden Sie RDB-Export und -Import.	1. Trennen der Quelle: Stoppen Sie den Datenverkehr in der Quelldatenbank (z. B. durch Trennen der Geschäftsanwendungen). 2. Exportieren: Exportieren Sie die Daten der Quelldatenbank als RDB-Datei. 3. Stufe: Laden Sie die Daten an einen Speicherort hoch, auf den die Redis Enterprise Cloud-Instances in AWS zugreifen können (Sie können sie beispielsweise in einen S3-Bucket oder FTP-Server hochladen). 4. Import: Importieren Sie die RDB-Dateien (indem Sie sie alle in einem Importschritt auflisten) in Ihre Redis Enterprise Cloud-Zieldatenbank. 5. Cutover: Wechseln Sie zur Zieldatenbank (z. B. indem Sie Ihre Anwendung mit ihr verbinden). Weitere Informationen finden Sie in der Redis-Dokumentation.	Architektur für Migrationslösungen, Architekturarchitekt für Redis-Lösungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Verwenden Sie die Redis-Replikationsfunktion (aktiv-passiv).	1. Datenbank verbinden : Stellen Sie eine `ReplicaOf` Verbindung zwischen der Quell- und der Zieldatenbank her. 2. Führen Sie eine erste Synchronisierung aus: Warten Sie, bis die erste Synchronisierung zwischen der Quell- und der Zieldaten bank abgeschlossen ist. 3. Trennen der Quelle: Stoppen Sie den Datenverk ehr in der Quelldatenbank (z. B. durch Trennen der Anwendung). 4. Delta-Replikation ausführen : Warten Sie, bis das Delta in der Zieldatenbank repliziert ist. 5. Cutover: Wechseln Sie zur Zieldatenbank (z. B. indem Sie Ihre Anwendung mit ihr verbinden). 6. Löschen: Entfernen Sie den `ReplicaOf` Link zwischen der Quell- und der Zieldaten bank. Weitere Informationen finden Sie in der Redis-Dokumentatio n.	Architektur für Migration slösungen, Architekturarchitekt für Redis-Lösungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 3: Verwenden Sie AWS DMS.	1. Einrichten einer AWS DMS-Replikations-Instance: Diese Instance führt alle Migrationsprozesse durch. Anweisungen: Arbeiten mit einer AWS DMS-Replikations-Instance in der AWS DMS-Dokumentation. 2. Definieren Sie die Quelldatenbank: Definieren Sie den Quellendpunkt. Testen Sie die Konnektivität zwischen dem Quellendpunkt und dem AWS DMS-Replikationsserver. Anweisungen: Erstellen von Quell- und Zielendpunkten in der AWS DMS-Dokumentation. 3. Einrichten der Zieldatenbank: Richten Sie Redis Enterprise Cloud in AWS und die Datenbank ein, zu der migriert werden soll. 4. Definieren Sie die Zieldatenbank: Definieren Sie den Zielendpunkt. Stellen Sie sicher, dass das VPC-Peering zwischen der VPC, in der AWS DMS ausgeführt wird, und der VPC, die Redis Enterprise Cloud in AWS hostet, eingerichtet ist. Testen Sie die Konnektivität zwischen dem	Architektur für Migrationslösungen, Architekturarchitekt für Redis-Lösungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS DMS-Replikationsserver und der Zieldatenbank. 5. Erstellen einer AWS DMS-Aufgabe: Erstellen Sie eine Aufgabe oder eine Reihe von Aufgaben, um die Tabellen und Replikationsprozesse zu definieren, die Sie für die Migration der Daten verwenden möchten. Anweisungen: Arbeiten mit AWS DMS-Aufgaben in der AWS DMS-Dokumentation. 6. Migrieren: Migrieren Sie die Daten, indem Sie die AWS DMS-Aufgabe ausführen. 7. Cutover: Wechseln Sie zur Zieldatenbank (z. B. indem Sie Ihre Anwendung mit ihr verbinden).	
Option 4: Verwenden Sie die logische Datenbank zusammenführung.	Diese Option umfasst die Verwendung eines Migrationsskripts oder ETL-Tools, das das physische Datenmodell der Quelldatenbank transformieren und eine RDB-Datei generieren kann. Redis Professional Services c hilft bei diesem Schritt, falls erforderlich.	Architektur für Migrationslösungen, Architekturarchitekt für Redis-Lösungen

Migrieren Ihrer Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stimmen Sie die Zeitpläne und Ziele des Projektma nagements ab.	Stimmen Sie die Ziele, Meilensteine und Zeitpläne des Migrationsprojekts der Anwendungsebene mit denen des Redis-Datenmigrati onsprojekts ab.	Projektmanagement
Stimmen Sie die Testaktiv itäten ab.	Nachdem die Anwendung sebene in der AWS Cloud migriert und modernisiert wurde, verweisen Sie die Anwendungsebene zum Testen auf die neu migrierte Redis Enterprise Cloud in AWS.	Testen

Test

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie Testpläne.	Führen Sie die Datenmigr ationsroutinen und die Skripts aus, die während der Implementierungsphase in einer Testumgebung gemäß den Testanforderungen an Ihrem Standort entwickelt wurden.	Testen
Testen Sie die Datenqualität.	Testen Sie die Datenqual ität, nachdem Sie die Daten migriert haben.	Testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Funktionalität.	Testen Sie Datenabfragen und die Anwendungsebene, um sicherzustellen, dass die Anwendung auf der gleichen Ebene wie im Quellsystem funktioniert.	Testen

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Treffen Sie die Cutover-Entscheidung.	Nachdem alle Tests auf Anwendungs- und Datenbankebene abgeschlossen sind, treffen das Führungsteam und die Stakeholder die endgültige Entscheidung darüber, ob sie auf der Grundlage der von den Testteams bestätigten Endergebnisse auf die neue Umgebung in AWS umsteigen möchten.	Projektmanagement, Geschäftschampions
Wechseln Sie zur AWS Cloud.	Wenn Sie bestätigt haben, dass alles vorhanden ist, verweisen Sie die Anwendungsebene auf die neu migrierten Daten und verweisen Sie Clients auf die neue Anwendungsebene, die basierend auf dem neuen Redis Enterprise Cloud-System in AWS ausgeführt wird.	IT oder DevOps Techniker, Datenarchitekt, Architektur für Migrationslösungen, Architektur für Redis-Lösungen

Zugehörige Ressourcen

Redis-Ressourcen

- Dokumentation zu Redis Enterprise Cloud
- RIOT-Tool (GitHub Repository)
- Terraform Provider (Herunterladen)

AWS-Ressourcen

- Demo-Migrationen
- AWS-Partnerlösungen
- Dokumentation
- Blog-Posts
- Whitepaper
- Tutorials und Videos
- AWS Cloud-Migration
- AWS Prescriptive Guidance

Zusätzliche Informationen

Die Standardsicherheitsanforderungen für die Migration von Redis-Workloads in die AWS Cloud finden Sie unter Bewährte Methoden für Sicherheit, Identität und Compliance auf der AWS-Website und im Redis Trust Center auf der Redis-Website.

Migrieren von SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL – kompatibel mit AWS SCT und AWS DMS

Erstellt von Amit Kumar (AWS) und Ankit Gupta

Umgebung: PoC oder Pilotprojekt	Quelle: SAP ASE	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Plattformwechsel	Workload: SAP	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS; AWS SCT		

Übersicht

Dieses Muster beschreibt, wie Sie eine SAP Adaptive Server Enterprise (SAP ASE)-Datenbank, die auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance gehostet wird, mithilfe von AWS Schema Conversion Tool (AWS SCT) und AWS Database Migration Service (AWS DMS) zu Amazon Aurora PostgreSQL kompatible Edition migrieren. Das Muster konzentriert sich sowohl auf Data Definition Language (DDL)-Konvertierungen für gespeicherte Objekte als auch auf die Datenmigration.

Aurora PostgreSQL -kompatibel unterstützt OLTP-Workloads (Online Transaction Processing). Dieser verwaltete Service bietet Konfigurationen, die bei Bedarf automatisch skaliert werden. Es kann Ihre Datenbank je nach den Anforderungen Ihrer Anwendung automatisch starten, herunterfahren, hochskalieren oder herunterskalieren. Sie können Ihre Datenbank in der Cloud ausführen, ohne Datenbank-Instances verwalten zu müssen. Aurora PostgreSQL – kompatibel bietet eine kostengünstige Option für seltene, intermittierende oder unvorhersehbare Workloads.

Der Migrationsprozess besteht aus zwei Hauptphasen:

- Konvertieren des Datenbankschemas mithilfe von AWS SCT
- Migrieren der Daten mithilfe von AWS DMS

Detaillierte Anweisungen für beide Phasen finden Sie im Abschnitt „Epics“. Informationen zur Behebung von Problemen, die sich speziell auf die Verwendung von AWS DMS mit SAP ASE-

Datenbanken beziehen, finden Sie unter Fehlerbehebung bei Problemen mit SAP ASE in der AWS DMS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine SAP-ASE-Quelldatenbank auf einer EC2-Instance mit Server-, Datenbank- und Listener-Services, die ausgeführt werden
- Eine Aurora PostgreSQL-kompatible Zieldatenbank

Einschränkungen

- Die Portnummer für Verbindungen muss 5432 sein.
- Die Huge_Pages-Funktion ist standardmäßig aktiviert, kann aber geändert werden.
- Die Granularität der P-oint-in-time Wiederherstellung (PITR) beträgt 5 Minuten.
- Die regionsübergreifende Replikation ist derzeit nicht verfügbar.
- Die maximale Speichergröße für eine Aurora-Datenbank beträgt 128 TiB.
- Sie können bis zu 15 Lesereplikate erstellen.
- Die Tabellengrößenbeschränkung ist nur durch die Größe des Aurora-Cluster-Volumes begrenzt, sodass die maximale Tabellengröße für einen Aurora-PostgreSQL-kompatiblen DB-Cluster 32 TiB beträgt. Wir empfehlen Ihnen, bewährte Methoden für das Tabellendesign zu befolgen, z. B. die Partitionierung großer Tabellen.

Produktversionen

- Quelldatenbank: AWS DMS unterstützt derzeit SAP ASE 15, 15.5, 15.7 und 16.x. Die neuesten Informationen zur Unterstützung der SAP ASE-Version finden Sie im AWS DMS-Benutzerhandbuch.
- Zieldatenbank: PostgreSQL 9.4 und höher (für Version 9.x), 10.x, 11.x, 12.x, 13.x und 14.x. Die neuesten unterstützten PostgreSQL-Versionen finden Sie im AWS DMS-Benutzerhandbuch.
- Amazon Aurora 1.x oder höher. Die neuesten Informationen finden Sie unter Aurora PostgreSQL – Kompatible Versionen und Engine-Versionen in der Aurora-Dokumentation.

Architektur

Quelltechnologie-Stack

- SAP-ASE-Datenbank läuft auf Amazon EC2

Zieltechnologie-Stack

- Aurora PostgreSQL – Kompatible Datenbank

Migrationsarchitektur

Tools

- Amazon Aurora PostgreSQL -Compatible Edition ist eine vollständig verwaltete, ACID-kompatible relationale Datenbank-Engine, mit der Sie PostgreSQL-Bereitstellungen einrichten, betreiben und skalieren können.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und der Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- AWS DMS unterstützt mehrere verschiedene Quell- und Zieldatenbanken. Weitere Informationen finden Sie unter Quellen für die Datenmigration und Ziele für die Datenmigration in der AWS DMS-Dokumentation. Für die umfassendste Versions- und Funktionsunterstützung empfehlen wir Ihnen, die neueste Version von AWS DMS zu verwenden.

Polen

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Netzwerkzugriff in der EC2-Quell-Instance.	Richten Sie Sicherheitsgruppen in der EC2-Instance ein, die Ihre SAP-ASE-Quelldatenbank hostet.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie unter Amazon EC2-Sicherheitsgruppen für Linux-Instances in der Amazon EC2Dokumentation.	
Erstellen Sie Ihren Aurora PostgreSQL-kompatiblen DB-Ziel-Cluster.	Installieren, konfigurieren und starten Sie einen Aurora-PostgreSQL-kompatiblen Cluster für Ihre Zieldatenbank. Weitere Informationen finden Sie unter Erstellen eines Amazon-Aurora-DB-Clusters in der Aurora-Dokumentation.	DBA
Richten Sie die Autorisierung für den Ziel-DB-Cluster ein.	Richten Sie Sicherheitsgruppen und Firewalls für die Zieldatenbank ein. Anweisungen finden Sie unter Erstellen eines Amazon-Aurora-DB-Clusters in der Aurora-Dokumentation.	DBA, Systemadministrator

Konvertieren Ihres Datenbankschemas mit AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie AWS SCT.	Starten Sie AWS SCT, indem Sie den Anweisungen in der AWS SCT-Dokumentation folgen. AWS SCT bietet eine projektbasierte Benutzero	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	berfläche, mit der Sie das Datenbankschema Ihrer SAP ASE-Quelldatenbank automatisch in ein Format konvertieren können, das mit Ihrer Aurora PostgreSQL-kompatiblen DB-Ziel-Instance kompatibel ist.	
Erstellen Sie AWS SCT-Endpunkte.	Erstellen Sie Endpunkte für die SAP-ASE-Quelldaten banken und zielen Sie auf PostgreSQL-Datenbanken ab. Anweisungen finden Sie in der AWS SCT-Dokumentation.	DBA
Erstellen Sie einen Bewertungsbericht.	Erstellen Sie einen Bewertungsbericht zur Datenbank migration, um die Migration zu bewerten und inkompati ble Objekte und Funktionen zu erkennen. Anweisungen finden Sie in der AWS SCT-Dokumentation.	DBA
Konvertieren Sie das Schema.	Konvertieren Sie das Datenbankschema, indem Sie den Anweisungen in der AWS SCT-Dokumentation folgen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbank objekte.	Wenn AWS SCT ein Datenbankobjekt nicht konvertieren kann, identifiziert es seinen Namen und andere Details. Sie müssen diese Objekte manuell konvertieren. Um diese Diskrepanzen zu identifizieren, folgen Sie den Anweisungen im AWS-Blogb eitrag Validate database objects after migration from SAP ASE to Amazon RDS for PostgreSQL or Amazon Aurora PostgreSQL .	DBA

Analysieren der AWS DMS-Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.	Überprüfen Sie die SAP ASE-Datenbankversionen auf Kompatibilität mit AWS DMS. Weitere Informationen finden Sie unter Quellen für AWS DMS und Ziele für AWS DMS in der AWS DMS-Dokum entation.	DBA
Identifizieren Sie die Anforderu ngen für den Speichertyp und die Kapazität.	Wählen Sie die entsprech ende Speicherkapazität für die Zieldatenbank basierend auf der Größe Ihrer Quelldate nbank aus.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Instance-Typ, die Kapazität und andere Funktionen der Replikations-Instance aus.	Wählen Sie den Instance-Typ, die Kapazität, die Speicherf unktionen und die Netzwerkf unktionen aus, die Ihren Anforderungen entsprechen. Anleitungen finden Sie unter Auswahl der richtigen AWS DMS-Replikations-Instance für Ihre Migration in der AWS DMS-Dokumentation.	DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff.	Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken. Folgen Sie den Anweisung en unter Einrichten eines Netzwerks für eine Replikati ons-Instance in der AWS DMS-Dokumentation.	DBA, Systemadministrator

Migrieren der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten, indem Sie eine Migration saufgabe in AWS DMS erstellen.	Um Daten zu migrieren, erstellen Sie eine Aufgabe und folgen Sie den Anweisung en in der AWS DMS-Dokum entation. Wir empfehlen Ihnen, die neueste Version von AWS	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DMS für die umfassendste Versions- und Funktions unterstützung zu verwenden.	
Validieren Sie die Daten.	Um zu überprüfen, ob Ihre Daten korrekt von der Quelldatenbank zur Zieldaten bank migriert wurden, befolgen Sie die Datenvali dierungsrichtlinien in der AWS DMS-Dokumentation.	DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.	Wählen Sie eine der sieben Strategien (7Rs) für die Migration von Anwendungen in die Cloud.	DBA, App-Besitzer, Systemadministrator
Folgen Sie der Strategie zur Anwendungsmigration.	Führen Sie die vom Anwendungsteam identifiz ierten Datenbankaufgaben aus, einschließlich der Aktualisierung der DNS-Verbi ndungsdetails für die Zieldaten bank und der Aktualisierung dynamischer Abfragen.	DBA, App-Besitzer, Systemadministrator

Umstellung auf die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.	Wechseln Sie die Verbindun g von der Quelldatenbank zur Zieldatenbank. Weitere Informationen finden Sie im Abschnitt Cutover der Migrationsstrategie für relationale Datenbanken.	DBA, App-Besitzer, Systemadministrator

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.	Beenden Sie alle Migration saufgaben, Replikations-Insta nces, Endpunkte und andere AWS SCT- und AWS DMS-Ressourcen. Weitere Informationen finden Sie in der AWS DMS-Dokum entation.	DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.	Validieren Sie alle Schritte in der Projektdokumentati on, um sicherzustellen, dass alle Aufgaben erfolgreich abgeschlossen wurden.	DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt.	Schließen Sie das Migration sprojekt und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Aktivieren verschlüsselter Verbindungen für PostgreSQL-DB-Instances in Amazon RDS (AWS Prescriptive Guidance)
- Transportieren von PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport (AWS Prescriptive Guidance)
- Amazon-Aurora-Preise
- Bewährte Methoden mit Amazon Aurora PostgreSQL – kompatible Edition (Amazon Aurora-Dokumentation)
- AWS SCT-Dokumentation
- AWS DMS-Dokumentation
- Verwenden einer SAP ASE-Datenbank als Quelle für AWS DMS

Tutorials und Videos

- Erste Schritte mit AWS Database Migration Service
- AWS Database Migration Service (Video)

Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer

Erstellt von Chandra Sekhar Yaratha (AWS) und Igor Kovalchuk (AWS)

Umgebung: Produktion	Quelle: Windows-W ebanwendung	Ziel: Application Load Balancer auf AWS
R-Typ: Replatform	Arbeitslast: Microsoft	Technologien: Migration; Verwaltung und Verwaltung; Web- und mobile Apps
AWS-Services: Elastic Load Balancing (ELB); AWS Certificate Manager (ACM)		

Übersicht

Das Muster enthält Anleitungen zur Verwendung von AWS Certificate Manager (ACM) zur Migration vorhandener Secure Sockets Layer (SSL) -Zertifikate von Websites, die auf lokalen Servern oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances auf Microsoft Internet Information Services (IIS) gehostet werden. Die SSL-Zertifikate können dann mit Elastic Load Balancing auf AWS verwendet werden.

SSL schützt Ihre Daten, bestätigt Ihre Identität, sorgt für bessere Platzierungen in Suchmaschinen, trägt zur Erfüllung der Anforderungen des Payment Card Industry Data Security Standard (PCI DSS) bei und stärkt das Kundenvertrauen. Entwickler und IT-Teams, die diese Workloads verwalten, möchten, dass ihre Webanwendungen und Infrastruktur, einschließlich des IIS-Servers und des Windows-Servers, ihren grundlegenden Richtlinien entsprechen.

Dieses Muster umfasst den manuellen Export vorhandener SSL-Zertifikate aus Microsoft IIS, deren Konvertierung vom PFX-Format (Personal Information Exchange) in das von ACM unterstützte PEM-Format (Private Enhanced Mail) und das anschließende Importieren in ACM in Ihrem AWS-Konto. Außerdem wird beschrieben, wie Sie einen Application Load Balancer für Ihre Anwendung erstellen und den Application Load Balancer so konfigurieren, dass er Ihre importierten Zertifikate verwendet. HTTPS-Verbindungen werden dann auf dem Application Load Balancer beendet, und Sie benötigen

keinen weiteren Konfigurationsaufwand auf dem Webserver. Weitere Informationen finden Sie unter Einen HTTPS-Listener für Ihren Application Load Balancer erstellen.

Windows-Server verwenden PFX- oder .P12-Dateien, um die öffentliche Schlüsseldatei (SSL-Zertifikat) und ihre eindeutige private Schlüsseldatei zu speichern. Die Zertifizierungsstelle (CA) stellt Ihnen Ihre öffentliche Schlüsseldatei zur Verfügung. Sie verwenden Ihren Server, um die zugehörige private Schlüsseldatei zu generieren, in der die Certificate Signing Request (CSR) erstellt wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine virtuelle private Cloud (VPC) auf AWS mit mindestens einem privaten und einem öffentlichen Subnetz in jeder Availability Zone, die von Ihren Zielen verwendet wird
- IIS-Version 8.0 oder höher, läuft auf Windows Server 2012 oder höher
- Eine Webanwendung, die auf IIS ausgeführt wird
- Administratorzugriff auf den IIS-Server

Architektur

Quelltechnologie-Stack

- IIS-Webserver-Implementierung mit SSL, um sicherzustellen, dass Daten sicher in einer verschlüsselten Verbindung (HTTPS) übertragen werden

Quellarchitektur

Zieltechnologie-Stack

- ACM-Zertifikate in Ihrem AWS-Konto
- Ein Application Load Balancer, der für die Verwendung importierter Zertifikate konfiguriert ist
- Windows Server-Instanzen in den privaten Subnetzen

Zielarchitektur

Tools

- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf EC2-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Bewährte Methoden

- Erzwingen Sie Verkehrsumleitungen von HTTP zu HTTPS.
- Konfigurieren Sie Sicherheitsgruppen für Ihren Application Load Balancer ordnungsgemäß, um eingehenden Datenverkehr nur zu bestimmten Ports zuzulassen.
- Starten Sie Ihre EC2-Instances in verschiedenen Availability Zones, um eine hohe Verfügbarkeit sicherzustellen.
- Konfigurieren Sie die Domain Ihrer Anwendung so, dass sie auf den DNS-Namen des Application Load Balancers statt auf dessen IP-Adresse verweist.
- Stellen Sie sicher, dass für den Application Load Balancer Integritätsprüfungen auf Anwendungsebene konfiguriert sind.
- Konfigurieren Sie den Schwellenwert für Integritätsprüfungen.
- Verwenden Sie Amazon CloudWatch, um den Application Load Balancer zu überwachen.

Epen

Exportieren Sie eine PFX-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie die PFX-Datei von Windows Server.	So exportieren Sie das SSL-Zertifikat als PFX-Datei aus dem lokalen IIS-Manager in Windows Server:	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Wählen Sie Start, Verwaltung und Internetinformationsdienste-Manager (IIS). 2. Wählen Sie den Servernamen aus, und doppelklicken Sie unter Sicherheit auf Serverzertifikate. 3. Wählen Sie das Zertifikat aus, das Sie exportieren möchten, und klicken Sie dann auf Exportieren. 4. Wählen Sie im Feld Zertifikat exportieren einen Speicherort, einen Pfad und einen Namen für Ihre PFX-Datei aus. 5. Geben Sie ein Passwort für Ihre PFX-Datei ein und bestätigen Sie es. Hinweis: Sie benötigen dieses Passwort, wenn Sie die PFX-Datei installieren. 6. Wählen Sie OK aus. Ihre PFX-Datei sollte jetzt an dem von Ihnen angegebenen Speicherort und Pfad gespeichert werden.	

Konvertieren Sie das PFX-kodierte Zertifikat in das PEM-Format

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das OpenSSL-Toolkit herunter und installieren Sie es.	1. Laden Sie Win32/Win64 OpenSSL von der Shining Light Productions-Website herunter und installieren Sie es. 2. Fügen Sie den Speicherort der OpenSSL-Binärdateien zu Ihrer `PATH` Systemvariablen hinzu, sodass die Binärdateien für die Befehlszeilenverwendung verfügbar sind.	Systemadministrator
Konvertieren Sie das PFX-kodierte Zertifikat in das PEM-Format.	Mit den folgenden Schritten wird die PFX-kodierte, signierte Zertifikatsdatei in drei Dateien im PEM-Format konvertiert: • `cert-file.pem` enthält das SSL/TLS-Zertifikat für die Ressource. • `privatekey.pem` enthält den privaten Schlüssel des Zertifikats ohne Passwortschutz. • `ca-chain.pem` enthält das Stammzertifikat der CA. Um das PFX-kodierte Zertifikat zu konvertieren:	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Führen Sie Windows aus. PowerShell
	2. Verwenden Sie den folgenden Befehl, um den privaten Schlüssel des Zertifikats aus der PFX-Datei zu extrahieren. Geben Sie das Passwort für das Zertifikat ein, wenn Sie dazu aufgefordert werden.
	`openssl pkcs12 -in <filename>.pfx -nocerts -out withpw-privatekey.pem`
	Der Befehl generiert eine PEM-kodierte private Schlüsseldatei mit dem Namen. `privatekey.pem` Geben Sie eine Passphrase ein, um die private Schlüsseldatei zu schützen, wenn Sie dazu aufgefordert werden.
	3. Führen Sie den folgenden Befehl aus, um die Passphrase zu entfernen. Wenn Sie dazu aufgefordert werden, geben Sie die Passphrase ein, die Sie in Schritt 2 erstellt haben.
	`openssl rsa -in withpw-privatekey.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`pem -out privateke y.pem`
	
	Wenn der Befehl erfolgrei ch ist, wird die Meldung „RSA-Schlüssel schreiben“ angezeigt.
	4. Verwenden Sie den folgenden Befehl, um das Zertifikat von der PFX-Datei in eine PEM-Datei zu übertragen.
	
	`openssl pkcs12 -in <file_name>.pfx - clcerts -nokeys -out cert-file.pem`
	
	Dadurch wird eine PEM-kodierte Zertifikatsdatei mit dem Namen erstellt. `cert-file.pem` Wenn der Befehl erfolgreich ist, wird die Meldung „MAC verified OK“ angezeigt.
	5. Erstellen Sie eine CA-Kettendatei aus der PFX-Datei. Der folgende Befehl erstellt eine CA-Kettendatei mit dem Name `ca-chain.pem` .
	
	`openssl pkcs12 -in <file_name>.pfx -`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cacerts -nokeys -chain -out ca-chain.pem` Wenn der Befehl erfolgreich ist, wird die Meldung „MAC verified OK“ angezeigt.	

Importieren Sie ein Zertifikat in ACM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Import des Zertifikats vor.	Wählen Sie in der ACM-Konsole die Option Zertifikat importieren aus.	Cloud-Administrator
Geben Sie die Zertifizierungsstelle an.	Fügen Sie in das Feld Zertifikatshauptteil das PEM-kodierte Zertifikat ein, das Sie importieren möchten. Weitere Informationen zu den Befehlen und Schritten, die in diesem und anderen Aufgaben in diesem Epos beschrieben werden, finden Sie in der ACM-Dokumentation unter Importieren eines Zertifikats.	Cloud-Administrator
Geben Sie den privaten Schlüssel des Zertifikats an.	Fügen Sie für Certificate private key den PEM-kodierten, unverschlüsselten privaten Schlüssel ein, der mit dem öffentlichen Schlüssel des Zertifikats übereinstimmt.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Zertifikatskette an.	Fügen Sie für Certificate chain die PEM-kodierte Zertifikatskette ein, die in der Datei gespeichert ist. `CertificateChain.pem`	Cloud-Administrator
Importieren Sie das Zertifikat.	Wählen Sie Review and import. Vergewissern Sie sich, dass die Informationen zu Ihrem Zertifikat korrekt sind, und wählen Sie dann Import aus.	Cloud-Administrator

Erstellen eines Application Load Balancers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie den Load Balancer und die Listener.	Folgen Sie den Anweisungen in der Elastic Load Balancing Balancing-Dokumentation, um eine Zielgruppe zu konfigurieren, Ziele zu registrieren und einen Application Load Balancer und Listener zu erstellen. Fügen Sie einen zweiten Listener (HTTPS) für Port 443 hinzu.	Cloud-Administrator

Fehlerbehebung

Problem	Lösung
Windows PowerShell erkennt den OpenSSL-Befehl nicht, auch wenn Sie ihn dem Systempfad hinzugefügt haben.	Stellen Sie `$env:path` sicher, dass es den Speicherort der OpenSSL-Binärdateien enthält. Ist dies nicht der Fall, führen Sie den folgenden Befehl in aus: PowerShell `$env:path = $env:path + ";C:\OpenSSL-Win64\bin"`

Zugehörige Ressourcen

Ein Zertifikat in ACM importieren

- ACM-Konsole
- Zertifikat und Schlüsselformat für den Import
- Ein Zertifikat importieren
- AWS Certificate Manager Manager-Benutzerhandbuch

Einen Application Load Balancer erstellen

- Erstellen Sie einen Application Load Balancer
- Application Load Balancer Balancer-Benutzerhandbuch

Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS

R-Typ: Replatform	Quelle: Anwendungen, die Azure Service Bus-Warte schlangen verwenden	Ziel: Amazon SQS
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Web- und mobile Apps; Migration
Arbeitslast: Microsoft	AWS-Dienste: Amazon SQS	

Übersicht

Dieses Muster beschreibt, wie Sie eine.NET Framework- oder .NET Core-Web- oder Konsolenanwendung von der Microsoft Azure Service Bus-Queue-Messaging-Plattform zu Amazon Simple Queue Service (Amazon SQS) migrieren.

Anwendungen verwenden Messaging-Dienste, um Daten an andere Anwendungen zu senden und Daten von anderen Anwendungen zu empfangen. Diese Dienste helfen beim Aufbau entkoppelter, hoch skalierbarer Microservices, verteilter Systeme und serverloser Anwendungen in der Cloud.

Azure Service Bus-Warteschlangen sind Teil einer umfassenderen Azure-Messaging-Infrastruktur, die das Einstellen von Warteschlangen und das Veröffentlichen und Abonnieren von Nachrichten unterstützt.

Amazon SQS ist ein vollständig verwalteter Message Queuing-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln und skalieren können. Amazon SQS beseitigt die Komplexität und den Aufwand, die mit der Verwaltung und dem Betrieb nachrichtenorientierter Middleware verbunden sind, und ermöglicht es Entwicklern, sich auf differenzierte Aufgaben zu konzentrieren. Mit Amazon SQS können Sie Nachrichten zwischen Softwarekomponenten in beliebiger Menge senden, speichern und empfangen, ohne dass Nachrichten verloren gehen oder andere Dienste verfügbar sein müssen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine.NET Framework- oder .NET Core-Web- oder Konsolenanwendung, die Azure Service Bus-Warteschlangen verwendet (Beispielcode im Anhang)

Produktversionen

- .NET Framework 3.5 oder höher oder.NET Core 1.0.1, 2.0.0 oder höher

Architektur

Quelltechnologie-Stack

- Eine.NET-Web- oder Konsolenanwendung (Core oder Framework), die eine Azure Service Bus-Warteschlange zum Senden von Nachrichten verwendet

Zieltechnologie-Stack

- Amazon SQS

Tools

Tools

- Microsoft Visual Studio

Code

So erstellen Sie eine AWS Identity and Access Management (IAM) -Richtlinie für Amazon SQS:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

2. Wählen Sie im Navigationsbereich auf der linken Seite Policies (Richtlinien) und dann Create Policy (Richtlinie erstellen) aus.

3. Wählen Sie die Registerkarte JSON und fügen Sie den folgenden Code ein:

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:GetQueueUrl",
            "sqs:ChangeMessageVisibility",
            "sqs:SendMessageBatch",
            "sqs:ReceiveMessage",
            "sqs:SendMessage",
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
            "sqs:ListDeadLetterSourceQueues",
            "sqs:DeleteMessageBatch",
            "sqs:PurgeQueue",
            "sqs:DeleteQueue",
            "sqs:CreateQueue",
            "sqs:ChangeMessageVisibilityBatch",
            "sqs:SetQueueAttributes"
         ],
         "Resource": "arn:aws:sqs:*:<AccountId>:*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sqs:ListQueues",
         "Resource": "*"
      }
   ]
}
```

4. Wählen Sie Richtlinie überprüfen, geben Sie einen Namen ein und wählen Sie dann Richtlinie erstellen aus.

5. Fügen Sie die neu erstellte Richtlinie Ihrer vorhandenen IAM-Rolle hinzu oder erstellen Sie eine neue Rolle.

Epen

Amazon SQS in AWS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richt linie für Amazon SQS.	Erstellen Sie die IAM-Richt linie, die den Zugriff auf Amazon SQS ermöglicht. Eine Beispielrichtlinie finden Sie im Abschnitt Code.	Systemingenieur
Erstellen Sie ein AWS-Profil.	Erstellen Sie ein neues Profil, indem Sie die AWS-Tools für den PowerShell Befehl Set-ausführenAWSCredential. Dieser Befehl speichert Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel in Ihrer Standardanmeldedatei unter dem von Ihnen angegeben en Profilnamen. Verknüpfen Sie die Amazon SQS SQS-Richtlinie, die Sie zuvor erstellt haben, mit diesem Konto. Bewahren Sie die AWS-Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel auf. Diese werden in den nächsten Schritten benötigt.	Systemingenieur
Erstellen Sie eine SQS-Warte schlange.	Sie können eine Standardw arteschlange oder eine FIFO-Warteschlange (First In, First Out) erstellen. Anweisungen finden Sie unter dem Link im Abschnitt Referenzen.	Systemingenieur

Überarbeiten Sie Ihren .NET-Anwendungscode

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS Toolkit for Visual Studio.	Dieses Toolkit ist eine Erweiterung für Microsoft Visual Studio und erleichtert Ihnen das Erstellen und Bereitstellen von.NET-Anwendungen in AWS. Anweisungen zur Installation und Verwendung finden Sie unter dem Link im Abschnitt Referenzen.	Entwickler der Anwendung
Installieren Sie das AWSSDK .SQS-Paket. NuGet	Sie AWSSDK können.SQS installieren, indem Sie in Visual Studio „ NuGet Package verwalten“ wählen oder den Befehl „ AWSSDKInstall-Package .SQS“ ausführen.	Entwickler der Anwendung
Erstellen Sie ein AWSCredentials Objekt in Ihrer .NET-Anwendung.	Die Beispielanwendung im Anhang zeigt, wie Sie ein AWSCredentials Basic-Objekt erstellen, das von AWSCredentials erbt. Sie können die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel von früher verwenden oder das Objekt diese zur Laufzeit als Teil des Benutzerprofils aus dem Ordner „.aws“ auswählen lassen.	Entwickler der Anwendung
Erstellen Sie ein SQS-Client-Objekt.	Erstellen Sie ein SQS-Client-Objekt (AmazonSQSClient) für.NET Framework. Dies	Entwickler von Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist Teil des Amazon.SQS-Namespace. Dieses Objekt ist anstelle von I erforderl ichQueueClient, das Teil von Microsoft.Azure ist. ServiceBu s Namespace.	
Rufen Sie die SendMessa geAsync Methode auf, um Nachrichten an die SQS-Warteschlange zu senden.	Ändern Sie den Code, der die Nachricht an die Warteschl ange sendet, um die zu verwenden. amazonSqsClient SendMessageAsync Methode. Einzelheiten finden Sie im beigefügten Codebeispiel.	Entwickler der Anwendung
Rufen Sie die ReceiveMe ssageAsync Methode auf, um Nachrichten aus der SQS-Warteschlange zu empfangen.	Ändern Sie den Code, der die Nachricht empfängt, um den zu verwenden. amazonSqs Client ReceiveMessageAsync Methode. Einzelheiten finden Sie im beigefügten Codebeisp iel.	Entwickler der Anwendung
Rufen Sie die DeleteMes sageAsync Methode auf, um Nachrichten aus der SQS-Warteschlange zu löschen.	Um Nachrichten zu löschen, ändern Sie den Code im QueueClient. CompleteAsync Methode zum. amazonSqs Client DeleteMessageAsync Methode. Einzelheiten finden Sie im beigefügten Codebeisp iel.	Entwickler der Anwendung

Zugehörige Ressourcen

- AWS SDK for .NET Entwicklerhandbuch

- Nachrichtenübermittlung mit Amazon SQS
- Erstellen und Verwenden einer Amazon SQS SQS-Warteschlange mit dem AWS SDK for .NET
- Senden Sie eine Amazon SQS SQS-Nachricht
- Empfangen einer Nachricht aus einer Amazon SQS SQS-Warteschlange
- Eine Nachricht aus einer Amazon SQS SQS-Warteschlange löschen
- AWS Toolkit for Visual Studio

Zusätzliche Informationen

Dieses Muster umfasst zwei Beispielanwendungen (siehe Abschnitt Anlagen):

- AzureSbTestAppenthält Code, der die Azure Service Bus-Warteschlange verwendet.
- AmazonSqsTestAppverwendet Amazon SQS. Dies ist eine Konsolenanwendung, die .NET Core 2.2 verwendet und Beispiele für das Senden und Empfangen von Nachrichten enthält.

Hinweise:

- QueueClient ist ein Objekt von IQueueClient, das Teil von Microsoft.Azure ist. ServiceBus Namespace (in Microsoft.Azure enthalten). ServiceBus NuGet Paket).
- amazonSqsClient ist ein Objekt von AmazonSQSClient, das Teil des Amazon.SQS-Namespace ist (im .SQS-Paket enthalten). AWSSDK NuGet
- Je nachdem, wo der Code ausgeführt wird, z. B. ob er auf EC2 ausgeführt wird, benötigt die Rolle die Berechtigung, in die SQS-Warteschlange zu schreiben.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren einer Oracle JD Edwards- EnterpriseOne Datenbank zu AWS mithilfe von Oracle Data Pump und AWS DMS

Erstellt von Thanigaivelrumalai (AWS)

Umgebung: Produktion	Quelle: Oracle JD Edwards EnterpriseOne	Ziel: Amazon RDS für Oracle
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS; AWS DMS		

Übersicht

Sie können Ihre JD Edwards- EnterpriseOne Datenbank auf Amazon Relational Database Service (Amazon RDS) migrieren und ausführen. Wenn Sie Ihre Datenbank zu Amazon RDS migrieren, kann sich AWS um Backup-Aufgaben und die Einrichtung hoher Verfügbarkeit kümmern, sodass Sie sich auf die Wartung Ihrer EnterpriseOne Anwendung und ihrer Funktionalität konzentrieren können. Eine umfassende Liste der wichtigsten Faktoren, die Sie während des Migrationsprozesses berücksichtigen sollten, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Es gibt mehrere Möglichkeiten, eine - EnterpriseOne Datenbank zu migrieren, darunter:

- Verwenden von Oracle Universal Batch Engine (UBE) R98403 für die Schema- und Tabellenerstellung und Verwenden von AWS Database Migration Service (AWS DMS) für die Migration
- Verwenden von nativen DB-Tools für die Schema- und Tabellenerstellung und Verwenden von AWS DMS für die Migration
- Verwenden von nativen DB-Tools für die Migration vorhandener Daten (Volllast) und Verwenden von AWS DMS für Change Data Capture (CDC)-Aufgaben

Dieses Muster deckt die dritte Option ab. Es wird erläutert, wie Sie Ihre On-Premises- EnterpriseOne Datenbanken mithilfe von Oracle Data Pump mit AWS DMS und seiner CDC-Funktion zu Amazon RDS für Oracle migrieren.

Oracle JD Edwards EnterpriseOne ist eine Enterprise Resource Planning (ERP)-Lösung für Organisationen, die Produkte oder physische Komponenten herstellt, erstellt, verteilt, bedient oder verwaltet. JD Edwards EnterpriseOne unterstützt verschiedene Hardware, Betriebssysteme und Datenbankplattformen.

Wenn Sie kritische Anwendungen wie JD Edwards migrieren EnterpriseOne, ist die Minimierung von Ausfallzeiten entscheidend. AWS DMS minimiert Ausfallzeiten, indem sowohl Volllast als auch kontinuierliche Replikation von der Quelldatenbank zur Zieldatenbank unterstützt werden. AWS DMS bietet auch Echtzeit-Überwachung und -Protokollierung für die Migration, mit der Sie Probleme identifizieren und beheben können, die Ausfallzeiten verursachen könnten.

Wenn Sie Änderungen mit AWS DMS replizieren, müssen Sie eine Zeit- oder Systemänderungsnummer (SCN) als Ausgangspunkt für das Lesen von Änderungen aus den Datenbankprotokollen angeben. Es ist wichtig, diese Protokolle für einen bestimmten Zeitraum auf dem Server zugänglich zu halten (wir empfehlen 15 Tage), um sicherzustellen, dass AWS DMS Zugriff auf diese Änderungen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Datenbank von Amazon RDS für Oracle, die in Ihrer AWS Cloud-Umgebung als Zieldatenbank bereitgestellt wird. Anweisungen finden Sie in der Amazon-RDS-Dokumentation.
- Eine - EnterpriseOne Datenbank, die On-Premises oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance in AWS ausgeführt wird.

  Hinweis: Dieses Muster ist für die Migration von On-Premises zu AWS konzipiert, wurde aber mithilfe einer - EnterpriseOne Datenbank auf einer EC2-Instance getestet. Wenn Sie vorhaben, aus Ihrer On-Premises-Umgebung zu migrieren, müssen Sie die entsprechende Netzwerkkonnektivität konfigurieren.
- Schemadetails. Identifizieren Sie, welches Oracle-Datenbankschema (z. B. DV920) Sie für migrieren möchten EnterpriseOne. Bevor Sie mit dem Migrationsprozess beginnen, sammeln Sie die folgenden Details zum Schema:
  - Schemagröße
  - Die Anzahl der Objekte pro Objekttyp

- Die Anzahl ungültiger Objekte

Einschränkungen

- Sie müssen alle Schemata erstellen, die Sie für die Amazon RDS for Oracle-Zieldatenbank benötigen – AWS DMS erstellt diese nicht für Sie. (Im Abschnitt „Epics“ wird beschrieben, wie Sie Data Pump verwenden, um Schemata zu exportieren und zu importieren.) Der Schemaname muss bereits für die Oracle-Zieldatenbank vorhanden sein. Tabellen aus dem Quellschema werden in den Benutzer oder das Schema importiert, und AWS DMS verwendet das Administrator- oder Systemkonto, um eine Verbindung zur Ziel-Instance herzustellen. Um mehrere Schemata zu migrieren, können Sie mehrere Replikationsaufgaben erstellen. Sie können Daten auch zu verschiedenen Schemata auf einer Ziel-Instance migrieren. Verwenden Sie dazu Schematransformationsregeln für die AWS DMS-Tabellenzuordnungen.
- Dieses Muster wurde mit einem Demo-Datensatz getestet. Wir empfehlen Ihnen, die Kompatibilität für Ihren Datensatz und Ihre Anpassung zu überprüfen.
- Dieses Muster verwendet eine - EnterpriseOne Datenbank, die unter Microsoft Windows ausgeführt wird. Sie können jedoch denselben Prozess mit anderen Betriebssystemen verwenden, die von AWS DMS unterstützt werden.

Architektur

Das folgende Diagramm zeigt ein System, das EnterpriseOne auf einer Oracle-Datenbank als Quelldatenbank ausgeführt wird, und eine Datenbank von Amazon RDS für Oracle als Zieldatenbank. Die Daten werden mithilfe von Oracle Data Pump aus der Oracle-Quelldatenbank exportiert, in die Amazon RDS for Oracle-Zieldatenbank importiert und mithilfe von AWS DMS für CDC-Aktualisierungen repliziert.

1. Oracle Data Pump extrahiert Daten aus der Quelldatenbank und die Daten werden an das Datenbankziel von Amazon RDS für Oracle gesendet.
2. CDC-Daten werden von der Quelldatenbank an einen Quellendpunkt in AWS DMS gesendet.
3. Vom Quellendpunkt werden die Daten an die AWS DMS-Replikations-Instance gesendet, wo die Replikationsaufgabe ausgeführt wird.
4. Nachdem die Replikationsaufgabe abgeschlossen ist, werden die Daten an den Zielendpunkt in AWS DMS gesendet.

5. Vom Zielendpunkt werden die Daten an die Datenbank-Instance von Amazon RDS für Oracle gesendet.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Einrichtungen.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.

Andere -Services

- Oracle Data Pump hilft Ihnen dabei, Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere zu verschieben.

Bewährte Methoden

Migrieren von LOBs

Wenn Ihre Quelldatenbank große binäre Objekte (LOBs) enthält, die in die Zieldatenbank migriert werden müssen, bietet AWS DMS die folgenden Optionen:

- Vollständiger LOB-Modus – AWS DMS migriert alle LOBs unabhängig von ihrer Größe von der Quelle zur Zieldatenbank. Obwohl die Migration langsamer ist als die anderen Modi, besteht der Vorteil darin, dass Daten nicht gekürzt werden. Um die Leistung zu verbessern, können Sie eine separate Aufgabe auf der neuen Replikations-Instance erstellen, um die Tabellen mit LOBs zu migrieren, die größer als einige Megabyte sind.
- Eingeschränkter LOB-Modus – Sie geben die maximale Größe von LOB-Spaltendaten an, mit der AWS DMS Ressourcen vorab zuweisen und die LOBs in großen Mengen anwenden kann. Wenn die Größe der LOB-Spalten die in der Aufgabe angegebene Größe überschreitet, kürzt AWS DMS die Daten und sendet Warnungen an die AWS DMS-Protokolldatei. Sie können die Leistung verbessern, indem Sie den eingeschränkten LOB-Modus verwenden, wenn Ihre LOB-Datengröße innerhalb der begrenzten LOB-Größe liegt.

- Inline-LOB-Modus – Sie können LOBs migrieren, ohne die Daten zu kürzen oder die Leistung Ihrer Aufgabe zu verlangsamen, indem Sie sowohl kleine als auch große LOBs replizieren. Geben Sie zunächst einen Wert für den `InlineLobMaxSize` Parameter an, der nur verfügbar ist, wenn der vollständige LOB-Modus auf festgelegt ist`true`. Die AWS DMS-Aufgabe überträgt die kleinen LOBs inline, was effizienter ist. Anschließend migriert AWS DMS die großen LOBs, indem es eine Suche aus der Quelltabelle durchführt. Der Inline-LOB-Modus funktioniert jedoch nur während der Volllastphase.

Generieren von Sequenzwerten

Während des AWS DMS-CDC-Prozesses werden inkrementelle Sequenznummern nicht aus der Quelldatenbank repliziert. Um Diskrepanzen bei den Sequenzwerten zu vermeiden, müssen Sie den neuesten Sequenzwert aus der Quelle für alle Sequenzen generieren und ihn auf die Zieldatenbank von Amazon RDS für Oracle anwenden.

AWS Secrets Manager

Um die Verwaltung Ihrer Anmeldeinformationen zu erleichtern, empfehlen wir Ihnen, die Anweisungen im Blogbeitrag Verwalten Ihrer AWS DMS-Endpunkt-Anmeldeinformationen mit AWS Secrets Manager zu befolgen.

Leistung

- Replikations-Instances Anleitungen zur Auswahl der besten Instance-Größe finden Sie unter Auswahl der besten Größe für eine Replikations-Instance in der AWS DMS-Dokumentation.
- Konnektivitätsoptionen Um Latenzprobleme zu vermeiden, empfehlen wir Ihnen, die richtige Konnektivitätsoption zu wählen. AWS Direct Connect bietet den kürzesten Weg zu AWS-Ressourcen, da es sich um eine dedizierte Verbindung zwischen Ihren Unternehmensrechenzentren und AWS handelt. Während der Übertragung verbleibt Ihr Netzwerkdatenverkehr im globalen AWS-Netzwerk und wird niemals über das Internet übertragen. Dadurch wird das Risiko verringert, dass Engpässe oder unerwartete Erhöhungen der Latenz im Vergleich zur Verwendung von VPN oder dem öffentlichen Internet auftreten.
- Netzwerkbandbreite Um die Leistung zu optimieren, überprüfen Sie, ob Ihr Netzwerkdurchsatz schnell ist. Wenn Sie einen VPN-Tunnel zwischen Ihrer On-Premises-Quelldatenbank und AWS DMS verwenden, stellen Sie sicher, dass die Bandbreite für Ihre Workload ausreicht.
- Aufgabenparallelität Sie können die Datenreplikation beschleunigen, indem Sie mehrere Tabellen während des vollständigen Ladens parallel laden. Dieses Muster verwendet RDBMS-Endpunkte, daher gilt diese Option nur für den Volllastprozess. Die Aufgabenparallelität wird durch den

-`MaxFullLoadSubTasks`Parameter gesteuert, der bestimmt, wie viele Volllast-Unteraufgaben parallel ausgeführt werden. Standardmäßig ist dieser Parameter auf 8 gesetzt, was bedeutet, dass acht Tabellen (falls in der Tabellenzuordnung ausgewählt) im Vollmodus zusammen geladen werden. Sie können diesen Parameter im Abschnitt mit den Einstellungen für Volllastaufgaben des JSON-Skripts für die Aufgabe anpassen.

- Mit der Tabellenparallelität AWS DMS können Sie auch eine einzelne große Tabelle mithilfe mehrerer paralleler Threads laden. Dies ist besonders nützlich für Oracle-Quelltabellen mit Milliarden von Datensätzen sowie mehreren Partitionen und Unterpartitionen. Wenn die Quelltabelle nicht partitioniert ist, können Sie Spaltengrenzen für parallele Ladevorgänge verwenden.
- Aufteilen von Ladevorgängen – Wenn Sie Ladevorgänge auf mehrere Aufgaben oder AWS DMS-Instances aufteilen, speichern Sie Transaktionsgrenzen, wenn Sie Änderungen erfassen.

Polen

Verwenden von Oracle Data Pump zum Exportieren des EnterpriseOne Schemas

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die SCN.	Wenn die Quelldatenbank aktiv ist und von der EnterpriseOne Anwendung verwendet wird, initiieren Sie den Datenexport mit Oracle Data Pump. Sie müssen zunächst eine Systemänderungsnummer (SCN) aus der Quelldatenbank generieren, um sowohl Datenkonsistenz während des Exports mit Oracle Data Pump als auch als Ausgangspunkt für CDC in AWS DMS zu gewährleisten. Verwenden Sie die folgende SQL-Anweisung, um die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	aktuelle SCN aus Ihrer Quelldatenbank zu generieren:
	
	`SQL> select current_scn from v$database;`
	
	`CURRENT_SCN`
	`-----------`
	`30009727`
	
	Speichern Sie die generierte SCN. Sie verwenden die SCN, wenn Sie die Daten exportieren und die AWS DMS-Replikationsaufgabe erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Parameter datei.	Um eine Parameterdatei für den Export des Schemas zu erstellen, können Sie den folgenden Code verwenden.
	`directory=DMS_DATA _PUMP_DIR logfile=export_dms.log dumpfile=export_dms_d ata.dmp schemas=<schema name> flashback_scn=<SCN from previous command>`
	Hinweis: Sie können Ihre eigenen auch definieren, `DATA_PUMP_DIR` indem Sie die folgenden Befehle verwenden, basierend auf Ihren Anforderungen.
	`SQL> CREATE OR REPLACE DIRECTORY DMS_DATA_ PUMP_DIR AS '<Directo ry for dump>'; Directory created.`
	`SQL> GRANT READ, WRITE ON DIRECTORY DMS_DATA_ PUMP_DIR TO SYSTEM; Grant succeeded.`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie das Schema.	Verwenden Sie das `expdp` Dienstprogramm wie folgt, um den Export durchzuführen:
	
	`C:\Users\Administrator>expdp system/********@<DB Name> PARFILE='<Path to PAR file create above>'`
	
	`Export: Release 19.0.0.0.0 - Production on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production Starting "SYSTEM"."SYS_EXPORT_SCHEMA_02": system/******@<DB Name>PARFILE='E:\exp_dms_datapump.par' Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA Processing object type SCHEMA_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS Processing object type SCHEMA_EXPORT/TABL`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	E/STATISTICS/TABLE _STATISTICS Processing object type SCHEMA_EXPORT/STAT ISTICS/MARKER Processing object type SCHEMA_EXPORT/USER Processing object type SCHEMA_EXPORT/ROLE _GRANT Processing object type SCHEMA_EXPORT/DEFA ULT_ROLE Processing object type SCHEMA_EXPORT/TABL ESPACE_QUOTA Processing object type SCHEMA_EXPORT/PRE_ SCHEMA/PROCACT_SCHEMA Processing object type SCHEMA_EXPORT/TABLE/ TABLE Processing object type SCHEMA_EXPORT/TABL E/GRANT/OWNER_GRANT/ OBJECT_GRANT Processing object type SCHEMA_EXPORT/TABLE/ INDEX/INDEX Processing object type SCHEMA_EXPORT/TABLE/ CONSTRAINT/CONSTRAINT . . exported "<Schema Name>"."<Table Name>" 228.9 MB 496397 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _02" successfully loaded/unloaded	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ********** ********** ********** ********** **** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_02 is: E:\DMSDUMP\EXPORT_ DMS_DATA.DMP Job "SYSTEM"."SYS_EXPO RT_SCHEMA_02" successfully completed at *** *** ** **:**:** **** elapsed 0 00:01:57 ```	

Verwenden von Oracle Data Pump zum Importieren des EnterpriseOne Schemas

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Dump-Datei auf die Ziel-Instance.	Um Ihre Dateien mit dem `DBMS_FILE_TRANSFER` Dienstprogramm zu übertragen, müssen Sie einen Datenbanklink von der Quelldatenbank zur Amazon RDS for Oracle-Instance erstellen. Nachdem der Link eingerichtet wurde, können Sie das Dienstprogramm verwenden, um die Data Pump-Dateien direkt in die Amazon RDS-Instance zu übertragen. Alternativ können Sie die Data Pump-Dateien an Amazon	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Simple Storage Service (Amazon S3) übertragen und dann in die Amazon RDS for Oracle-Instance importieren. Weitere Informationen zu dieser Option finden Sie im Abschnitt Zusätzliche Informationen.
	
	Führen Sie die folgenden Befehle in der Quelldatenbank aus0RARDSDB, um einen Datenbanklink zu erstellen, der eine Verbindung zum Amazon-RDS-Hauptbenutzer in der Ziel-DB-Instance herstellt:
	
	`sqlplus / as sysdba`
	
	`SQL*Plus: Release 19.0.0.0.0 on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 Version 19.3.0.0.0`
	
	`SQL> create database link orardsdb connect to admin identified by "******" using`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`'(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = orcl.******.us-east-1.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	
	`Database link created.`
	
	`SQL>`	

Testen Sie den Datenbanklink.	Testen Sie den Datenbanklink, um sicherzustellen, dass Sie mithilfe von eine Verbindung mit der Zieldatenbank von Amazon RDS für Oracle herstellen können `sqlplus`.
	
	`SQL> select name from v$database@orardsdb;`
	
	`NAME`
	`---------`
	`ORCL`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übertragen Sie die Dump-Datei in die Zieldatenbank.	Um die Dump-Datei in die Datenbank von Amazon RDS für Oracle zu kopieren, können Sie entweder das `DATA_PUMP_DIR` Standardverzeichnis verwenden oder Ihr eigenes Verzeichnis erstellen, indem Sie den folgenden Code verwenden, der auf der Amazon-RDS-Ziel-Instance ausgeführt werden muss:
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'DMS_TARGET_PUMP_DIR');`
	`PL/SQL procedure successfully completed.`
	Das folgende Skript kopiert eine Dump-Datei mit dem Namen `EXPORT_DMS_DATA.DMP` aus der Quell-Instance in eine Zieldatenbank von Amazon RDS für Oracle unter Verwendung des Datenbank links mit dem Namen `orardsdb`. Sie müssen das Skript auf der Quelldatenbank-Instance ausführen.
	`BEGIN`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`DBMS_FILE_TRANSFER.PUT_FILE( source_directory_object => 'DMS_DATA_PUMP_DIR', source_file_name => 'EXPORT_DMS_DATA.DMP', destination_directory_object => 'DMS_TARGET_PUMP_DIR', destination_file_name => 'EXPORT_DMS_DATA.DMP', destination_database => 'orardsdb'); END;`
	
	`PL/SQL procedure successfully completed.`	

Listen Sie die Dump-Datei in der Zieldatenbank auf.	Nachdem die PL/SQL-Prozedur abgeschlossen ist, können Sie die Datenabbilddatei in der Datenbank von Amazon RDS für Oracle mit dem folgenden Code auflisten: `select * from table (rdsadmin.rds_file_util.listdir(p_directory => 'DMS_TARGET_PUMP_DIR'));`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie JDE-spezifische Benutzer in der Ziel-Instance.	Erstellen Sie ein JD Edwards-Profil und eine Rolle, indem Sie die folgenden Befehle in der Ziel-Instance verwenden:
	`SQL> CREATE PROFILE "JDEPROFILE" LIMIT IDLE_TIME 15;`
	`Profile created.`
	
	`SQL> CREATE ROLE "JDE_ROLE";`
	`Role created.`
	
	`SQL> CREATE ROLE "JDEADMIN";`
	`CREATE ROLE "JDEUSER";`
	`Role created.`
	`Role created.`
	
	Erteilen Sie der Rolle die erforderlichen Berechtigungen:
	`SQL> GRANT CREATE ANY SEQUENCE TO JDE_ROLE;`
	`GRANT DROP ANY SEQUENCE TO JDE_ROLE;`
	`GRANT CREATE ANY TRIGGER TO JDE_ROLE;`
	`GRANT DROP ANY TRIGGER TO JDE_ROLE;`
		DBA, JDESpeed

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Tablespaces in der Ziel-Instance.	Erstellen Sie die erforderlichen Tablespaces in der Ziel-Instance, indem Sie die folgenden Befehle für die Schemata verwenden, die an dieser Migration beteiligt sind:
	`SQL> CREATE TABLESPACE <Tablespace Name for Tables>;`
	`Tablespace created.`
	
	`SQL> CREATE TABLESPACE <Tablespace Name for Indexes>;`
	`Tablespace created.`
		DBA, JDESpeed

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie den Import in die Zieldatenbank.	Bevor Sie den Importvorgang starten, richten Sie die Rollen, Schemata und Tabellenr äume in der Zieldatenbank von Amazon RDS für Oracle mithilfe der Datenabbilddatei ein. Um den Import durchzuführen, greifen Sie mit dem primären Amazon-RDS-Benutzerkonto auf die Zieldatenbank zu und verwenden Sie den Namen der Verbindungszeichen folge in der `tnsnames.ora` Datei, die die Amazon RDS for Oracle Database enthält`tns-entry` . Bei Bedarf können Sie eine Neuzuweisungsoption hinzufügen, um die Datenabbi lddatei in einen anderen Tabellenraum oder unter einem anderen Schemanamen zu importieren. Verwenden Sie den folgenden Code, um den Import zu starten: `impdp admin@orardsdb directory=DMS_TARG ET_PUMP_DIR logfile=i mport.log dumpfile= EXPORT_DMS_DATA.DMP`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um einen erfolgreichen Import sicherzustellen, überprüfen Sie die Importprotokolldatei auf Fehler und überprüfen Sie Details wie Objektanzahl, Zeilenanzahl und ungültige Objekte. Wenn es ungültige Objekte gibt, kompilieren Sie sie neu. Vergleichen Sie außerdem die Quell- und Zieldatenbankobjekte, um zu bestätigen, dass sie übereinst immen.	

Bereitstellen einer AWS DMS-Replikations-Instance mit den Quell- und Zielendpunkten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Vorlage für herunter.	Laden Sie die Vorlage AWS CloudFormation DMS_instance.yaml herunter, um die AWS DMS-Replikations-Instance und ihre Quell- und Zielendpunkte bereitzustellen.	Cloud-Administrator, DBA
Starten Sie die Stack-Erstellung.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS- CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation. 2. Wählen Sie Stack erstellen aus.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. 4. Wählen Sie Datei auswählen aus. 5. Wählen Sie die `DMS_instance.yaml` Datei aus. 6. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Parameter an.	1. Geben Sie für Stack-Name Ihren Stack-Namen ein. 2. Geben Sie für AWS DMS-Instance-Parameter die folgenden Parameter ein: • DMSInstanceType – Wählen Sie je nach Ihren Geschäftsanforderungen die erforderliche Instance für die AWS DMS-Replikations-Instance aus. • DMSStorageSize – Geben Sie die Speichergröße für die AWS DMS-Instance basierend auf der Größe Ihrer Migration ein. 3. Geben Sie für Oracle-Quelldatenbankkonfiguration die folgenden Parameter ein: • SourceOracleEndpointID – Der Name des Oracle-Quelldatenbankservers • SourceOracleDatabaseName – Gegebenen falls der Name oder die Sitzungs-ID (SID) des Quelldatenbank-Service • SourceOracleUserName – Der Benutzername der Quelldatenbank (Standard ist `system`)	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• SourceOracleDBPassword – Das Passwort des Benutzernamens der Quelldatenbank • SourceOracleDBPort – Der Quelldatenbankport 4. Geben Sie für Zielkonfiguration von RDS für Oracle Database die folgenden Parameter ein: • TargetRDSOracleEndpoint ID – Der Ziel-RDS-Datenbankendpunkt • TargetRDSOracleDatabaseName – Der Name der RDS-Zieldatenbank • TargetRSOracleUserName – Der Ziel-RDS-Benutzername • TargetRDSOracleDBPassword – Das Ziel-RDS-Passwort • TargetOracleDBPort – Der Ziel-RDS-Datenbankport 5. Geben Sie für VPC-, Subnetz- und Sicherheitsgruppenkonfiguration die folgenden Parameter ein: • VPCID – Die VPC für die Replikations-Instance • VPCSecurityGroupId – Die VPC-Sicherheitsgru	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ppe für die Replikations-Instance • DMSSubnet1 – Das Subnetz für Availability Zone 1 • DMSSubnet2 – Das Subnetz für Availability Zone 2 6. Wählen Sie Weiter aus.	
Erstellen Sie den Stack.	1. Geben Sie auf der Seite Stack-Optionen konfiguri eren für Tags alle optionale n Werte ein. 2. Wählen Sie Weiter aus. 3. Überprüfen Sie auf der Seite Überprüfen die Details und wählen Sie dann Absenden aus. Die Bereitstellung sollte in etwa 5–10 Minuten abgeschlo ssen sein. Er ist abgeschlo ssen, wenn auf der Seite AWS CloudFormation Stacks CREATE_COMPLETE angezeigt wird.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Endpunkte ein.	1. Öffnen Sie die AWS DMS-Konsole unter https://console.aws.amazon.com/dms/v2/. 2. Wählen Sie für Ressourcenverwaltung die Option Replikations-Instances aus und überprüfen Sie dann die Replikations-Instances. 3. Wählen Sie für Ressourcenverwaltung Endpunkte aus und überprüfen Sie dann die Endpunkte.	Cloud-Administrator, DBA
Testen Sie die Konnektivität.	Nachdem die Quell- und Zielendpunkte den Status Aktiv angezeigt haben, testen Sie die Konnektivität. Wählen Sie Test ausführen für jeden Endpunkt (Quelle und Ziel), um sicherzustellen, dass der Status als erfolgreich angezeigt wird.	Cloud-Administrator, DBA

Erstellen einer AWS DMS-Replikationsaufgabe für die Live-Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Replikationsaufgabe.	Erstellen Sie die AWS DMS-Replikationsaufgabe mithilfe der folgenden Schritte: 1. Öffnen Sie die AWS DMS-Konsole unter https://	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	console.aws.amazon.com/dms/v2/. 2. Wählen Sie im Navigationsbereich unter Daten migrieren die Option Datenbankmigration saufgabe aus. 3. Geben Sie im Feld Aufgabenkonfiguration für Aufgaben-ID Ihre Aufgaben-ID ein. 4. Wählen Sie für Replikations-Instance die DMS-Replikations-Instance aus, die Sie erstellt haben. 5. Wählen Sie für Quelldatenbank-Endpunkt Ihren Quellendpunkt aus. 6. Wählen Sie für Zieldatenbank-Endpunkt Ihre Zieldatenbank von Amazon RDS für Oracle aus. 7. Wählen Sie für Migrationstyp die Option Datenänderungen nur replizieren aus. Wenn Sie die Meldung erhalten, dass die zusätzliche Protokollierung aktiviert werden muss, folgen Sie den Anweisungen im Abschnitt Fehlerbehebung. 8. Wählen Sie im Feld Aufgabeneinstellungen die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Option Protokollsequenznummer angeben aus. 9. Geben Sie für Systemänderungsnummer die Oracle-Datenbank-SCN ein, die Sie aus der Oracle-Quelldatenbank generiert haben. 10. Wählen Sie Validierung aktivieren aus. 11. Wählen Sie CloudWatch Protokolle aktivieren aus. Durch die Aktivierung dieser Funktion können Sie die Daten und Amazon CloudWatch-Protokolle validieren, um die AWS DMS-Replikations-Instance-Protokolle zu überprüfen. 12. Führen Sie unter Auswahlregeln Folgendes aus: • Wählen Sie für Schema die Option Schema eingeben aus. • Geben Sie für Schemaname den JDE-Schemanamen ein (z. B. DV920). • Geben Sie für Tabellenname % ein. • Wählen Sie für Aktion die Option Einschließen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	13. Wählen Sie Create task aus. Nachdem Sie die Aufgabe erstellt haben, migriert AWS DMS fortlaufende Änderungen an der Datenbank-Instance von Amazon RDS für Oracle von der SCN, die Sie im CDC-Startmodus angegeben haben. Sie können die Migration auch überprüfen, indem Sie die CloudWatch Protokolle überprüfen.	
Wiederholen Sie die Replikationsaufgabe.	Wiederholen Sie die vorherigen Schritte, um Replikationsaufgaben für andere JD Edwards-Schemas zu erstellen, die Teil der Migration sind.	Cloud-Administrator, DBA-, JDE-Administrator

Validieren des Datenbankschemas in der Zieldatenbank von Amazon RDS für Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Datenübertragung.	Nachdem die AWS DMS-Aufgabe gestartet wurde, können Sie die Registerkarte Tabellenstatistiken auf der Seite Aufgaben überprüfen, um die an den Daten vorgenommenen Änderungen anzuzeigen.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können den Status der laufenden Replikation in der -Konsole auf der Seite Datenbankmigrationsaufgaben überwachen. Weitere Informationen finden Sie unter AWS DMS-Daten validierung.	

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Replikation.	Beenden Sie das Replikati onsverfahren und beenden Sie die Quellanwendungsservices.	Cloud-Administrator, DBA
Starten Sie die JD Edwards-A nwendung.	Starten Sie die JD Edwards-Zielanwendung auf der Präsentations- und Logikeben e in AWS und leiten Sie sie an die Datenbank von Amazon RDS für Oracle weiter. Wenn Sie auf die Anwendung zugreifen, sollten Sie beachten, dass jetzt alle Verbindungen mit der Datenbank von Amazon RDS für Oracle hergestellt sind.	DBA-, JDE-Administrator
Deaktivieren Sie die Quelldate nbank.	Nachdem Sie bestätigt haben, dass keine Verbindungen mehr vorhanden sind, können	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Quelldatenbank ausschalten.	

Fehlerbehebung

Problem	Lösung

Sie erhalten eine Warnmeldung, um die zusätzliche Protokollierung in der Quelldatenbank für die fortlaufende Replikation zu aktivieren.	Geben Sie diese Befehle ein, um die zusätzliche Protokollierung zu aktivieren:
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`

AWS DMS hat die zusätzliche Protokollierung deaktiviert.	Die ergänzende Protokollierung ist in AWS DMS standardmäßig deaktiviert. So aktivieren Sie es für einen Oracle-Quellendpunkt: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS DMS-Konsole unter https://console.aws.amazon.com/dms/v2/. 2. Wählen Sie Endpunkte aus. 3. Wählen Sie den Oracle-Quellendpunkt, dem Sie die zusätzliche Protokollierung hinzufügen möchten. 4. Wählen Sie Ändern aus.

Problem	Lösung
	5. Wählen Sie Erweitert aus und fügen Sie dann den folgenden Code im Textfeld Extra Verbindungsattribute hinzu: `addSupplementalLogging=Y` 6. Wählen Sie Ändern aus.

Die ergänzende Protokollierung ist auf CDB-Ebene nicht aktiviert.	1. Geben Sie diesen Befehl ein:
	`SQL> alter session set container = CDB$ROOT;`
	`Session altered.`
	2. Wiederholen Sie die Schritte, um die zusätzliche Protokollierung zu aktivieren.

Sie erhalten die Fehlermeldung: „Testendpunkt fehlgeschlagen: Anwendungsstatus: 1020912, Application-Message: LogMiner wird in der Oracle-PDB-Umgebung nicht unterstützt Endpunktinitialisierung fehlgeschlagen“.	Wenn diese Fehlermeldung angezeigt wird, können Sie Binary Reader anstelle von verwenden LogMiner. Fügen Sie unter Endpunkteinstellungen diese Zeile zu den zusätzlichen Verbindungsattributen für Ihre Quelldatenbank hinzu: `useLogMinerReader=N;useBfile=Y;`

Zugehörige Ressourcen

- Erste Schritte mit AWS Database Migration Service
- Bewährte Methoden für AWS Database Migration Service
- Migrieren von Oracle-Datenbanken in die AWS Cloud
- Ressourcentypreferenz für AWS Database Migration Service für AWS CloudFormation
- Verwalten Ihrer AWS DMS-Endpunkt-Anmeldeinformationen mit AWS Secrets Manager

- Fehlerbehebung bei Migrationsaufgaben in AWS Database Migration Service
- Bewährte Methoden für AWS Database Migration Service

Zusätzliche Informationen

Übertragen von Dateien mit Amazon S3

Um die Dateien an Amazon S3 zu übertragen, können Sie die AWS CLI oder die Amazon S3-Konsole verwenden. Nachdem Sie die Dateien in Amazon S3 übertragen haben, können Sie die Amazon RDS for Oracle-Instance verwenden, um die Data Pump-Dateien aus Amazon S3 zu importieren.

Wenn Sie die Dump-Datei mithilfe der Amazon S3-Integration als alternative Methode übertragen möchten, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen S3-Bucket.
2. Exportieren Sie die Daten aus der Quelldatenbank mit Oracle Data Pump.
3. Laden Sie die Data Pump-Dateien in den S3-Bucket hoch.
4. Laden Sie die Data Pump-Dateien aus dem S3-Bucket in die Zieldatenbank von Amazon RDS für Oracle herunter.
5. Führen Sie den Import mithilfe der Data Pump-Dateien durch.

Hinweis: Um große Datenübertragungen zwischen S3- und RDS-Instances zu übertragen, empfehlen wir Ihnen, die Funktion Amazon S3 Transfer Acceleration zu verwenden.

Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS

Umgebung: Produktion	Quelle: Oracle PeopleSoft	Ziel: Amazon RDS for Oracle
R-Typ: Replatform	Arbeitslast: Oracle	Technologien: Migration; Datenbanken
AWS-Dienste: AWS DMS; Amazon RDS		

Übersicht

Oracle PeopleSoft ist eine ERP-Lösung (Enterprise Resource Planning) für unternehmensweite Prozesse. PeopleSoft hat eine dreistufige Architektur: Client, Anwendung und Datenbank. PeopleSoft kann auf Amazon Relational Database Service (Amazon RDS) ausgeführt werden.

Wenn Sie Ihre Oracle-Datenbank zu Amazon RDS migrieren, kann Amazon Web Services (AWS) Backup-Aufgaben und Hochverfügbarkeit übernehmen, sodass Sie sich auf die Wartung Ihrer PeopleSoft Anwendung und ihrer Funktionalität konzentrieren können. Eine umfassende Liste der wichtigsten Faktoren, die während des Migrationsprozesses zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster bietet eine Lösung für die Migration Ihrer lokalen Oracle-Datenbanken zu Amazon RDS for Oracle mithilfe von Oracle Data Pump mit AWS Database Migration Service (AWS DMS) und seiner Change Data Capture (CDC) -Funktion.

Bei der Migration kritischer ERP-Anwendungen wie Oracle PeopleSoft ist die Minimierung der Ausfallzeiten von entscheidender Bedeutung. AWS DMS minimiert Ausfallzeiten, indem es sowohl Volllast- als auch kontinuierliche Replikation von der Quelldatenbank zur Zieldatenbank unterstützt. AWS DMS bietet außerdem eine Überwachung und Protokollierung der Migration in Echtzeit, sodass Sie Probleme, die zu Ausfallzeiten führen könnten, identifizieren und lösen können.

Wenn Sie Änderungen mit AWS DMS replizieren, müssen Sie eine Uhrzeit oder eine Systemänderungsnummer (SCN) als Ausgangspunkt angeben, damit AWS DMS Änderungen aus den Datenbankprotokollen lesen kann. Es ist wichtig, diese Protokolle für einen bestimmten

Zeitraum auf dem Server zugänglich zu halten, um sicherzustellen, dass AWS DMS Zugriff auf diese Änderungen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Bereitgestellte Amazon RDS for Oracle Oracle-Datenbank in Ihrer AWS-Cloud-Umgebung als Zieldatenbank.
- Eine PeopleSoft Oracle-Datenbank, die lokal oder auf Amazon Elastic Compute Cloud (Amazon EC2) in der AWS-Cloud ausgeführt wird.

  Hinweis: Dieses Muster ist für die Migration von lokalen Systemen zu AWS konzipiert, wurde jedoch mithilfe von Oracle Database auf einer Amazon EC2 EC2-Instance getestet. Für die Migration von einer lokalen Infrastruktur müssen Sie die entsprechende Netzwerkkonnektivität konfigurieren.
- Schemadetails. Bei der Migration einer PeopleSoft Oracle-Anwendung zu Amazon RDS for Oracle muss angegeben werden, welches Oracle-Datenbankschema (z. B.`SYSADM`) migriert werden soll. Bevor Sie mit dem Migrationsprozess beginnen, sollten Sie die folgenden Informationen über das Schema sammeln:
  - Größe
  - Die Anzahl der Objekte pro Objekttyp
  - Die Anzahl der ungültigen Objekte.

  Diese Informationen helfen beim Migrationsprozess.

Einschränkungen

- Dieses Szenario wurde nur mit der PeopleSoft DEMO-Datenbank getestet. Es wurde nicht mit einem großen Datensatz getestet.

Architektur

Das folgende Diagramm zeigt eine Instance, auf der eine Oracle-Datenbank als Quelldatenbank und eine Amazon RDS for Oracle Oracle-Datenbank als Zieldatenbank ausgeführt wird. Die Daten werden mit Oracle Data Pump aus der Oracle-Quelldatenbank in die Amazon RDS for Oracle Oracle-Zieldatenbank exportiert und importiert und für CDC-Änderungen mit AWS DMS repliziert.

1. Im ersten Schritt werden Daten mithilfe von Oracle Data Pump aus der Quelldatenbank extrahiert und anschließend an das Datenbankziel Amazon RDS for Oracle gesendet.
2. Daten werden von der Quelldatenbank an einen Quellendpunkt in AWS DMS gesendet.
3. Vom Quellendpunkt werden die Daten an die AWS DMS-Replikationsinstanz gesendet, wo die Replikationsaufgabe ausgeführt wird.
4. Nach Abschluss der Replikationsaufgabe werden die Daten an den Zielendpunkt in AWS DMS gesendet.
5. Vom Zielendpunkt werden die Daten an die Amazon RDS for Oracle Oracle-Datenbank-Instance gesendet.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.

Andere Dienste

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere verschieben.

Bewährte Methoden

LOBs migrieren

Wenn Ihre Quelldatenbank große binäre Objekte (LOBs) enthält, die in die Zieldatenbank migriert werden müssen, bietet AWS DMS die folgenden Optionen:

- Vollständiger LOB-Modus — AWS DMS migriert alle LOBs unabhängig von ihrer Größe von der Quell- zur Zieldatenbank. Die Migration ist zwar langsamer, hat aber den Vorteil, dass die Daten nicht gekürzt werden. Für eine bessere Leistung können Sie eine separate Aufgabe für die neue

Replikationsinstanz erstellen, um die Tabellen zu migrieren, deren LOBs größer als ein paar Megabyte sind.

- Eingeschränkter LOB-Modus — Sie geben die maximale Größe der LOB-Spaltendaten an, sodass AWS DMS Ressourcen vorab zuweisen und die LOBs in großen Mengen anwenden kann. Wenn die Größe der LOB-Spalten die in der Aufgabe angegebene Größe überschreitet, kürzt AWS DMS die Daten und sendet Warnungen an die AWS DMS-Protokolldatei. Sie können die Leistung verbessern, indem Sie den eingeschränkten LOB-Modus verwenden, wenn Ihre LOB-Datengröße innerhalb der begrenzten LOB-Größe liegt.
- Inline-LOB-Modus — Sie können LOBs migrieren, ohne die Daten zu kürzen oder die Leistung Ihrer Aufgabe zu beeinträchtigen, indem Sie sowohl kleine als auch große LOBs replizieren. Geben Sie zunächst einen Wert für den InlineLobMaxSize Parameter an, der nur verfügbar ist, wenn der Full-LOB-Modus auf true gesetzt ist. Die AWS DMS-Aufgabe überträgt die kleinen LOBs inline, was effizienter ist. Anschließend migriert AWS DMS die großen LOBs, indem es eine Suche aus der Quelltabelle durchführt. Der Inline-LOB-Modus funktioniert jedoch nur während der Volllastphase.

Generieren von Sequenzwerten

Beachten Sie, dass während der Erfassung von Änderungsdaten mit AWS DMS inkrementelle Sequenznummern nicht aus der Quelldatenbank repliziert werden. Um Diskrepanzen bei den Sequenzwerten zu vermeiden, müssen Sie für alle Sequenzen den neuesten Sequenzwert aus der Quelle generieren und ihn auf die Amazon RDS for Oracle Oracle-Zieldatenbank anwenden.

Verwaltung von Anmeldeinformationen

Um Ihre AWS-Ressourcen zu schützen, empfehlen wir, die Best Practices für AWS Identity and Access Management (IAM) zu befolgen.

Epen

Stellen Sie eine AWS-DMS-Replikationsinstanz mit den Quell- und Zielendpunkten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Vorlage für herunter.	Laden Sie die CloudFormation AWS-Vorlage DMS_Instance.yaml herunter, um die AWS-DMS-Replikatio	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nsinstanz und ihre Quell- und Zielendpunkte bereitzustellen.	
Starten Sie die Stack-Erstellung.	1. Wählen Sie in der AWS-Managementkonsole CloudFormation. 2. Wählen Sie Stack erstellen aus. 3. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. 4. Wählen Sie Datei auswählen. 5. Wählen Sie die `DMS_instance.yaml` Datei aus. 6. Wählen Sie Weiter aus.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Parameter an.	1. Geben Sie unter Stack-Name Ihren Stack-Namen ein. 2. Geben Sie unter AWS DMS-Instanzparameter die folgenden Parameter ein: • DMS InstanceType — Wählen Sie die erforderliche Instanz für die AWS DMS-Replikationsinstanz, basierend auf Ihren Geschäftsanforderungen. • DMS StorageSize — Geben Sie die Speichergröße für die AWS DMS-Instanz ein, basierend auf der Größe Ihrer Migration. 3. Geben Sie unter Konfiguration der Oracle-Quelldatenbank die folgenden Parameter ein: • SourceOracleEndpointID — Der Name des Oracle-Quelldatenbankservers • SourceOracleDatabaseName— Der Dienstname oder die Sitzungs-ID (SID) der Quelldatenbank, sofern zutreffend • SourceOracleUserName— Der Benutzername der Quelldatenbank (die	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardeinstellung ist System) • SourceOracledbPassword — Das Passwort des Benutzernamens der Quelldatenbank • SourceOracledbPort — Der Port der Quelldatenbank 4. Geben Sie unter Target RDS for Oracle Database Configuration die folgenden Parameter ein: • targetRDS OracleEndpoint ID — Der Ziel-RDS-Datenbank-Endpunkt • OracleDatabasetargetRDS-Name — Der Name der Ziel-RDS-Datenbank • OracleUsertargetRS-Name — Der RDS-Zielbenutzername • targetRDSOracleDBPassword — Das Ziel-RDS-Passwort • TargetOracledbPort — Der Ziel-RDS-Datenbankport 5. Geben Sie unter VPC-, Subnetz- und Sicherheitsgruppenkonfiguration die folgenden Parameter ein:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• VPCID — Die VPC für die Replikationsinstanz • SecurityGroupVPC-ID — Die VPC-Sicherheitsgruppe für die Replikationsinstanz • DMSSubnet1 — Das Subnetz für Availability Zone 1 • DMSSubnet2 — Das Subnetz für Availability Zone 2 6. Wählen Sie Weiter aus.	
Erstellen Sie den Stack.	1. Geben Sie auf der Seite „Stack-Optionen konfigurieren“ für Tags beliebige optionale Werte ein. 2. Wählen Sie Weiter aus. 3. Überprüfen Sie auf der Seite „Überprüfen“ die Details und wählen Sie dann Senden aus. Die Bereitstellung sollte in etwa 5—10 Minuten abgeschlossen sein. Es ist abgeschlossen, wenn auf der Seite AWS CloudFormation Stacks CREATE_COMPLETE angezeigt wird.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Endpunkte ein.	1. Wählen Sie in der AWS-Managementkonsole Database Migration Services aus. 2. Wählen Sie unter Ressourcenmanagement die Option Replication instances aus. 3. Wählen Sie unter Ressourcenverwaltung die Option Endpoints aus.	Cloud-Administrator, DBA
Testen Sie die Konnektivität.	Nachdem der Quell- und der Zielendpunkt den Status Aktiv angezeigt haben, testen Sie die Konnektivität. Wählen Sie für jeden Endpunkt (Quell- und Zielpunkt) die Option Test ausführen aus, um sicherzustellen, dass der Status als erfolgreich angezeigt wird.	Cloud-Administrator, DBA

Exportieren Sie das PeopleSoft Schema mithilfe von Oracle Data Pump aus der lokalen Oracle-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie das SCN.	Wenn die Quelldatenbank aktiv ist und von der Anwendung verwendet wird, initiieren Sie den Datenexport mit Oracle Data Pump. Sie müssen zunächst eine System Change Number	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(SCN) aus der Quelldatenbank generieren, um sowohl die Datenkonsistenz beim Export mit Oracle Data Pump als auch als Ausgangspunkt für die Erfassung von Änderungsdaten in AWS DMS zu gewährleisten.
	
	Um die aktuelle SCN aus Ihrer Quelldatenbank zu generieren, geben Sie die folgende SQL-Anweisung ein.
	
	`SQL> select name from v$database;`
	`SQL> select name from v$database;`
	`NAME`
	`---------`
	`PSFTDMO`
	`SQL> SELECT current_scn FROM v$database;`
	`CURRENT_SCN`
	`-----------`
	`23792008`
	
	Speichern Sie die generierte SCN, um sie beim Exportieren der Daten und zur Erstellung der AWS DMS-Replikationsaufgabe zu verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Parameter datei.	Um eine Parameterdatei für den Export des Schemas zu erstellen, können Sie den folgenden Code verwenden.
	`$ cat exp_datapmp.par`
	`userid=system/*******`
	`directory=DATA_P`
	`UMP_DIR`
	`logfile=export_dms_`
	`sample_user.log`
	`dumpfile=export_dms_`
	`sample_data_%U.dmp`
	`schemas=SYSADM`
	`flashback_scn=237920`
	`08`
	Hinweis: Sie können je nach Ihren Anforderungen auch Ihren eigenen definieren, `DATA_PUMP_DIR` indem Sie die folgenden Befehle verwenden.
	`SQL> CREATE OR REPLACE`
	` DIRECTORY DATA_PUMP`
	`_DIR AS '/opt/oracle/`
	`product/19c/dbhome_1/`
	`dmsdump/';`
	`Directory created.`
	`SQL> GRANT READ, WRITE`
	` ON DIRECTORY DATA_PUMP`
	`_DIR TO system;`
	`Grant succeeded.`
	`SQL>`
	`SQL> SELECT owner,`
	` directory_name,`
	` directory_path FROM`
	` dba_directories WHERE`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	directory_name='DA TA_PUMP_DIR'; OWNER DIRECTORY_NAME DIRECTORY_PATH ---------- ---------- ---------- ---------- ---------- ---------- SYS DATA_PUMP_DIR /opt/ oracle/product/19c/dbh ome_1/dmsdump/	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie das Schema.	Verwenden Sie das `expdp` Hilfsprogramm, um den Export durchzuführen. `$ expdp parfile=e xp_datapmp.par .... Transferring the dump file with DBMS_FILE _TRANSFER to Target: . . exported "SYSADM". "PS_XML_TEMPLT_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_TEMPLT_LNK" 6.328 KB 0 rows . . exported "SYSADM". "PS_XML_XLATDEF_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_XLATITM_LNG" 7.171 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNCNTL" 7.601 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNPARM" 7.210 KB 0 rows . . exported "SYSADM". "PS_YE_AMOUNTS" 9.351 KB 0 rows . . exported "SYSADM". "PS_YE_DATA" 16.58 KB 0 rows . . exported "SYSADM". "PS_YE_EE" 6.75 KB 0 rows . . exported "SYSADM". "PS_YE_W2CP_AMOUNTS" 9.414 KB 0 rows`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	. . exported "SYSADM". "PS_YE_W2CP_DATA" 20.94 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_AMOUNTS" 10.27 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_DATA" 20.95 KB 0 rows . . exported "SYSADM". "PS_ZBD_JOBCODE_TBL" 14.60 KB 0 rows . . exported "SYSADM". "PTGRANTTBL" 5.468 KB 0 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _01" successfully loaded/unloaded ** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_01 is: /opt/oracle/pr oduct/19c/dbhome_1 /dmsdump/export_dm s_sample_data_01.dmp Job "SYSTEM"."SYS_EXPO RT_SCHEMA_01" successfully completed at Mon Dec 19 20:13:57 2022 elapsed 0 00:38:22	

Importieren Sie das PeopleSoft Schema mithilfe von Oracle Data Pump in die Amazon RDS for Oracle-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Dump-Datei auf die Zielinstanz.	Um Ihre Dateien mit zu übertragen`DBMS_FILE_TRANSFER`, müssen Sie einen Datenbank-Link von der Quelldatenbank zur Amazon RDS for Oracle Oracle-Instance erstellen. Nachdem die Verbindung hergestellt wurde, können Sie das Hilfsprogramm verwenden, um die Data Pump-Dateien direkt auf die RDS-Instance zu übertragen. Alternativ können Sie die Data Pump-Dateien an Amazon Simple Storage Service (Amazon S3) übertragen und sie dann in die Amazon RDS for Oracle Oracle-Instance importieren. Weitere Informationen zu dieser Option finden Sie im Abschnitt Zusätzliche Informationen. Um einen Datenbank-Link zu erstellen`ORARDSDB`, der eine Verbindung zum Amazon RDS-Master-Benutzer auf der Ziel-DB-Instance herstellt, führen Sie die folgenden Befehle in der Quelldatenbank aus.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$sqlplus / as sysdba`
	`$ SQL> create database link orardsdb connect to admin identified by "*****" using '(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testpsft.*******.us-west-2.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	`Database link created.`	

Testen Sie den Datenbank-Link.	Testen Sie den Datenbank-Link, um sicherzustellen, dass Sie mit sqlplus eine Verbindung zur Amazon RDS for Oracle Oracle-Zieldatenbank herstellen können.
	`SQL>`
	`SQL> select name from v$database@orardsdb;`
	`NAME`
	`---------`
	`ORCL`
	`SQL>`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übertragen Sie die Dump-Datei in die Zieldatenbank.	Um die Dump-Datei in die Amazon RDS for Oracle Oracle-Datenbank zu kopieren, können Sie entweder das `DATA_PUMP_DIR` Standardverzeichnis verwenden oder mit dem folgenden Code Ihr eigenes Verzeichnis erstellen.
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'TARGET_PUMP_DIR');`
	Das folgende Skript kopiert eine `export_dms_sample_data_01.dmp` aus der Quell-Instance benannte Dump-Datei mithilfe des angegebenen Datenbank-Links in eine Amazon RDS for Oracle Oracle-Zieldatenbank. `orardsdb`
	`$ sqlplus / as sysdba`
	`SQL>`
	`BEGIN`
	`DBMS_FILE_TRANSFER.PUT_FILE(`
	`source_directory_object => 'DATA_PUMP_DIR',`
	`source_file_name => 'export_dms_sample_data_01.dmp',`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`destination_directory _object => 'TARGET_P UMP_DIR'', destination_file_name => 'export_dms_sample _data_01.dmp', destination_database => 'orardsdb' ); END; / PL/SQL procedure successfully completed .`	
Listet die Dump-Datei in der Zieldatenbank auf.	Nachdem das PL/SQL-Verfahren abgeschlossen ist, können Sie die Datendump-Datei in der Amazon RDS for Oracle Oracle-Datenbank auflisten, indem Sie den folgenden Code verwenden. `SQL> select * from table (rdsadmin.rds_file _util.listdir(p_di rectory => 'TARGET_P UMP_DIR'));`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie den Import in der Zieldatenbank.	Bevor Sie den Importvorgang starten, richten Sie die Rollen, Schemas und Tablespaces in der Amazon RDS for Oracle Oracle-Zieldatenbank mithilfe der Datendumpdatei ein. Um den Import durchzuführen, greifen Sie mit dem Amazon RDS-Master-Benutzerkonto auf die Zieldatenbank zu und verwenden Sie den Namen der Verbindungszeichen folge in der `tnsnames.ora` Datei, die die Amazon RDS for Oracle Database enthält`tns-entry` . Bei Bedarf können Sie eine Remap-Option hinzufügen, um die Datendumpdatei in einen anderen Tablespace oder unter einem anderen Schemanamen zu importieren. Verwenden Sie den folgenden Code, um den Import zu starten. `impdp admin@orardsdb directory=TARGET_PUMP_DIR logfile=import.log dumpfile=export_dms_sample_data_01.dmp`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um einen erfolgreichen Import sicherzustellen, überprüfen Sie die Import-Protokolldatei auf Fehler und überprüfen Sie Details wie Objektanzahl, Zeilenanzahl und ungültige Objekte. Wenn ungültige Objekte vorhanden sind, kompilieren Sie sie erneut. Vergleichen Sie außerdem die Quell- und Zieldatenbankobjekte, um sicherzustellen, dass sie übereinstimmen.	

Erstellen Sie eine AWS DMS-Replikationsaufgabe mithilfe von CDC, um die Live-Replikation durchzuführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Replikationsaufgabe.	Erstellen Sie die AWS DMS-Replikationsaufgabe mithilfe der folgenden Schritte: 1. Wählen Sie in der AWS DMS-Konsole unter Konvertierung und Migration die Option Datenbankmigrationsaufgabe aus. 2. Geben Sie unter Aufgabenkonfiguration für Task-ID Ihre Task-ID ein. 3. Wählen Sie für Replikationsinstanz die DMS-Repli	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	kationsinstanz aus, die Sie erstellt haben. 4. Wählen Sie für Quelldatenbank-Endpunkt Ihren Quellendpunkt aus. 5. Wählen Sie als Zieldatenbank-Endpunkt Ihre Amazon RDS for Oracle Oracle-Zieldatenbank aus. 6. Wählen Sie als Migrationstyp die Option Nur Datenänderungen replizieren aus. Wenn Sie eine Meldung erhalten, dass die zusätzliche Protokollierung aktiviert werden muss, folgen Sie den Anweisungen im Abschnitt Zusätzliche Informationen. 7. Wählen Sie unter Taskeinstellungen die Option Protokollsequenznummer angeben aus. 8. Geben Sie als Systemänderungsnummer die Oracle-Datenbank-SCN ein, die Sie aus der Oracle-Quelldatenbank generiert haben. 9. Wählen Sie Validierung aktivieren. 10. Wählen Sie „ CloudWatch Protokolle aktivieren“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie diese Funktion aktivieren, können Sie die Daten und CloudWatchAmazon-Protokolle validieren, um die Protokolle der AWS DMS-Replikationsinstanz zu überprüfen. 11. Gehen Sie unter Auswahlregeln wie folgt vor: • Wählen Sie unter Schema die Option Schema eingeben aus. • Geben Sie als Schemaname SYSADM ein. • Geben Sie als Tabellenname% ein. • Wählen Sie für Aktion die Option Include aus. 12. Gehen Sie unter Transformationsregeln wie folgt vor: • Wählen Sie für Target die Option Tabelle aus. • Wählen Sie unter Schemaname die Option Schema eingeben aus. • Geben Sie als Schemaname SYSADM ein. • Wählen Sie für Aktion die Option Umbenennen in.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	13. Wählen Sie Create task aus. Nachdem Sie die Aufgabe erstellt haben, migriert sie das CDC von der SCN, die Sie im CDC-Startmodus bereitgestellt haben, zur Amazon RDS for Oracle Oracle-Datenbank-Instance. Sie können dies auch überprüfen, indem Sie die Protokolle überprüfen. CloudWatch	

Überprüfen Sie das Datenbankschema auf der Amazon RDS for Oracle Oracle-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Datenübertragung.	Nachdem die AWS DMS-Aufgabe gestartet wurde, können Sie auf der Seite Aufgaben auf der Registerkarte Tabellenstatistiken nachsehen, welche Änderungen an den Daten vorgenommen wurden. Sie können den Status der laufenden Replikation in der Konsole auf der Seite mit den Aufgaben zur Datenbankmigration überwachen.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter AWS DMS-Daten validierung.	

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Replikation.	Brechen Sie den Replikationsvorgang ab und halten Sie die Dienste der Quellanwendung an.	Cloud-Administrator, DBA
Starten Sie die PeopleSoft mittlere Stufe.	Starten Sie die PeopleSoft Middle-Tier-Zielanwendung in AWS und leiten Sie sie an die kürzlich migrierte Amazon RDS for Oracle Oracle-Datenbank weiter. Wenn Sie auf die Anwendung zugreifen, sollten Sie feststellen, dass jetzt alle App-Verbindungen mit der Amazon RDS for Oracle Oracle-Datenbank hergestellt sind.	DBA, Administrator PeopleSoft
Schalten Sie die Quelldatenbank aus.	Nachdem Sie bestätigt haben, dass keine Verbindungen mehr zur Quelldatenbank bestehen, kann sie ausgeschaltet werden.	DBA

Zugehörige Ressourcen

- Erste Schritte mit AWS Database Migration Service
- Bewährte Methoden für den AWS Database Migration Service
- Migration von Oracle-Datenbanken in die AWS-Cloud

Zusätzliche Informationen

Dateien mit Amazon S3 übertragen

Um die Dateien auf Amazon S3 zu übertragen, können Sie die AWS-CLI oder die Amazon S3 S3-Konsole verwenden. Nachdem Sie die Dateien zu Amazon S3 übertragen haben, können Sie die Amazon RDS for Oracle Oracle-Instance verwenden, um die Data Pump-Dateien aus Amazon S3 zu importieren.

Wenn Sie die Dump-Datei mithilfe der Amazon S3 S3-Integration als alternative Methode übertragen möchten, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen S3-Bucket.
2. Exportieren Sie die Daten mit Oracle Data Pump aus der Quelldatenbank.
3. Laden Sie die Data Pump-Dateien in den S3-Bucket hoch.
4. Laden Sie die Data Pump-Dateien aus dem S3-Bucket in die Amazon RDS for Oracle Oracle-Zieldatenbank herunter.
5. Führen Sie den Import mithilfe der Data Pump-Dateien durch.

Hinweis: Um große Datendateien zwischen S3- und RDS-Instances zu übertragen, wird empfohlen, die Amazon S3 Transfer Acceleration Acceleration-Funktion zu verwenden.

Aktivieren Sie die zusätzliche Protokollierung

Wenn Sie eine Warnmeldung erhalten, um die zusätzliche Protokollierung in der Quelldatenbank für die laufende Replikation zu aktivieren, gehen Sie wie folgt vor.

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS
```

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
```

Migrieren einer On-Premises-MySQL-Datenbank zu Amazon RDS für MySQL

Erstellt von Bolenzo Mota (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises-MySQL-Datenbank	Ziel: Amazon RDS für MySQL
R-Typ: Plattformwechsel	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer On-Premises-MySQL-Datenbank zu Amazon Relational Database Service (Amazon RDS) für MySQL . Das Muster erläutert die Verwendung von AWS Database Migration Service (AWS DMS) oder nativen MySQL-Tools wie mysqldbcopy und mysqldump für eine vollständige Datenbankmigration. Dieses Muster gilt hauptsächlich für DBAs und Lösungsarchitekten. Es kann in kleinen oder großen Projekten als Testverfahren (wir empfehlen mindestens einen Testzyklus) oder als endgültiges Migrationsverfahren verwendet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine MySQL-Quelldatenbank in einem On-Premises-Rechenzentrum

Einschränkungen

- Datenbankgrößenbeschränkung: 64 TB

Produktversionen

- MySQL-Versionen 5.5, 5.6, 5.7, 8.0. Die neueste Liste der unterstützten Versionen finden Sie unter MySQL in Amazon RDS in der AWS-Dokumentation. Wenn Sie AWS DMS verwenden, finden Sie

weitere Informationen unterVerwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS for MySQL-Versionen, die derzeit von AWS DMS unterstützt werden.

Architektur

Quelltechnologie-Stack

- Eine lokale MySQL-Datenbank

Zieltechnologie-Stack

- Eine Amazon RDS-DB-Instance, auf der MySQL ausgeführt wird

Zielarchitektur

Das folgende Diagramm zeigt die Zielimplementierung von Amazon RDS für MySQL nach der Migration.

AWS-Datenmigrationsarchitektur

Verwenden von AWS DMS:

Das folgende Diagramm zeigt die Datenmigrationsarchitektur, wenn Sie AWS DMS verwenden, um vollständige und inkrementelle Änderungen bis zum Cutover zu senden. Die Netzwerkverbindung von On-Premises zu AWS hängt von Ihren Anforderungen ab und liegt außerhalb des Bereichs für dieses Muster.

Verwenden nativer MySQL-Tools:

Das folgende Diagramm zeigt die Datenmigrationsarchitektur, wenn Sie native MySQL-Tools verwenden. Die Export-Dump-Dateien werden vor dem Cutover in Amazon Simple Storage Service (Amazon S3) kopiert und in die Datenbank von Amazon RDS für MySQL in AWS importiert. Die Netzwerkverbindung von On-Premises zu AWS hängt von Ihren Anforderungen ab und liegt außerhalb des Bereichs für dieses Muster.

Hinweise:

- Abhängig von den Ausfallzeiten und der Größe der Datenbank minimiert die Verwendung von AWS DMS oder einem Change Data Capture (CDC)-Tool die Cutover-Zeit. AWS DMS kann dazu beitragen, die Cutover-Zeit auf das neue Ziel auf ein Minimum (in der Regel Minuten) zu reduzieren. Eine Offline-Strategie mit mysqldump oder mysqldbcopy kann ausreichen, wenn die Größe der Datenbank und die Netzwerklatenz ein kurzes Zeitfenster zulassen. (Wir empfehlen Tests, um eine ungefähre Zeit zu erhalten.)
- Normalerweise erfordert eine CDC-Strategie wie AWS DMS mehr Überwachung und Komplexität als Offline-Optionen.

Tools

- AWS-Services: AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen aus Cloud- und On-Premises-Einrichtungen. Informationen zu MySQL-Quell- und Zieldatenbanken, die von AWS DMS unterstützt werden, finden Sie unter Migrieren von MySQL-kompatiblen Datenbanken zu AWS . Wenn Ihre Quelldatenbank nicht von AWS DMS unterstützt wird, müssen Sie eine andere Methode für die Migration Ihrer Daten wählen.
- Native MySQL-Tools: mysqldbcopy und mysqldump
- Tools von Drittanbietern: Percona XtraBackup

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbank versionen.	Validieren Sie die Quell- und Zieldatenbankversionen.	DBA
Identifizieren Sie Hardwarea nforderungen.	Identifizieren Sie die Hardwareanforderungen für den Zielserver.	DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen.	Identifizieren Sie Speichera nforderungen (wie Speichert	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	yp und Kapazität) für die Zieldatenbank.	
Wählen Sie den Instance-Typ aus.	Wählen Sie den Ziel-Instance-Typ basierend auf Kapazität , Speicherfunktionen und Netzwerkfunktionen aus.	DBA, Systemadministrator
Identifizieren Sie die Netzwerkzugriffsanforderungen.	Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	DBA, Systemadministrator
Identifizieren Sie nicht unterstützte Objekte.	Identifizieren Sie nicht unterstützte Objekte (falls vorhanden) und bestimmen Sie den Migrationsaufwand.	DBA
Identifizieren Sie Abhängigkeiten.	Identifizieren Sie alle Abhängigkeiten von Remote-Datenbanken.	DBA
Bestimmen Sie die Strategie für die Anwendungsmigration.	Legen Sie die Strategie für die Migration von Clientanwendungen fest.	DBA, App-Besitzer, Systemadministrator

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Konfigurieren Sie Routing-Tabellen, Internet-Gateways, NAT-Gateways und Subnetze. Weitere Informationen finden Sie unter VPCs und Amazon	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	RDS in der Amazon-RDS-Dokumentation.	
Erstellen Sie Sicherheitsgruppen.	Konfigurieren Sie Ports und CIDR-Bereiche oder bestimmte IPs je nach Ihren Anforderungen. Der Standardport für MySQL ist 3306. Weitere Informationen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen in der Amazon-RDS-Dokumentation.	Systemadministrator
Konfigurieren und starten Sie eine DB-Instance von Amazon RDS für MySQL.	Anweisungen finden Sie unter Erstellen einer Amazon-RDS-DB-Instance in der Amazon-RDS-Dokumentation. Suchen Sie nach unterstützten Versionen.	Systemadministrator

Migrieren von Daten – Option 1 (mit nativen Tools)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbietern, um Datenbankobjekte und -daten zu migrieren.	Anweisungen finden Sie in der Dokumentation für MySQL-Tools wie mysqldbcopy ,mysqldump und Percona XtraBackup (für physische Migration). Weitere Informationen zu Optionen finden Sie im Blogbeitrag Migrationsoptionen für MySQL zu	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon RDS für MySQL oder Amazon Aurora MySQL .	

Migrieren von Daten – Option 2 (mit AWS DMS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.	Anweisungen finden Sie in der AWS DMS-Dokumentation.	DBA

Vorläufige Aufgaben vor dem Cutover ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie Abweichungen bei der Anzahl der Objekte.	Erfasst die Anzahl der Objekte aus der Quelldatenbank und der neuen Zieldatenbank. Korrigieren Sie Diskrepanzen in der Zieldatenbank.	DBA
Überprüfen Sie Abhängigkeiten.	Überprüfen Sie, ob Abhängigkeiten (Links) zu und von anderen Datenbanken gültig sind und wie erwartet funktionieren.	DBA
Führen Sie Tests durch.	Wenn es sich um einen Testzyklus handelt, führen Sie Abfragetests durch, sammeln Sie Metriken und beheben Sie Probleme.	DBA

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zur Zieldatenbank.	Wechseln Sie Clientanwendungen zur neuen Infrastruktur.	DBA, App-Besitzer, Systemadministrator
Stellen Sie Testunterstützung bereit.	Bietet Unterstützung für funktionale Anwendungstests.	DBA

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie Ressourcen herunter.	Fahren Sie die temporären AWS-Ressourcen herunter, die Sie für die Migration erstellt haben.	DBA, Systemadministrator
Validieren Sie Projektdokumente.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer, Systemadministrator
Erfassen Sie Metriken.	Erfassen Sie Metriken wie die Zeit für die Migration, den Prozentsatz manueller oder automatisierter Bemühungen, Kosteneinsparungen usw.	DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt.	Schließen Sie das Projekt ab und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator
Außerbetriebnahme der Quelldatenbank.	Wenn alle Migrations- und Cutover-Aufgaben abgeschlossen sind, nehmen Sie die On-Premises-Datenbank außer Betrieb.	DBA, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Migrationsstrategie für relationale Datenbanken
- AWS DMS-Website
- AWS DMS-Dokumentation
- Dokumentation zu Amazon RDS
- Amazon-RDS-Preise
- VPCs und Amazon RDS
- Amazon-RDS-Multi-AZ-Bereitstellungen
- Migrieren Sie On-Premises-MySQL-Datenbanken zu Aurora MySQL mit Percona XtraBackup, Amazon EFS und Amazon S3

Tutorials

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS

Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server

Erstellt von Henrique Lobao (AWS), Jonathan Pere Bol Bolz (AWS) und Vishal Singh (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Microsoft SQL Server	Ziel: Amazon RDS für SQL Server
R-Typ: Plattformwechsel	Workload: Microsoft	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster bietet Anleitungen für die Migration von einer lokalen Microsoft SQL Server-Datenbank zu Amazon Relational Database Service (Amazon RDS) für SQL Server. Es werden zwei Optionen für die Migration beschrieben: die Verwendung von AWS Data Migration Service (AWS DMS) oder die Verwendung nativer Microsoft SQL Server-Tools wie Copy Database Wizard.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Quelldatenbank von Microsoft SQL Server in einem On-Premises-Rechenzentrum

Einschränkungen

- Datenbankgrößenbeschränkung: 16 TB

Produktversionen

- SQL Server 2014-2019, Enterprise, Standard, Arbeitsgruppe und Entwickler Editionen. Die neueste Liste der unterstützten Versionen und Funktionen finden Sie unter Microsoft SQL Server in Amazon RDS in der AWS-Dokumentation. Wenn Sie AWS DMS verwenden, finden Sie weitere

Informationen unter Verwenden einer Microsoft SQL Server-Datenbank als Ziel für AWS DMS for SQL Server-Versionen, die von AWS DMS unterstützt werden.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Eine DB-Instance von Amazon RDS für SQL Server

Quell- und Zielarchitektur

Verwenden von AWS DMS:

Verwenden nativer SQL Server-Tools:

Tools

- AWS DMS unterstützt verschiedene Arten von Quell- und Zieldatenbanken. Weitere Informationen finden Sie unter Schrittweise Anleitungen zu AWS DMS. Wenn AWS DMS die Quelldatenbank nicht unterstützt, wählen Sie eine andere Methode für die Migration der Daten aus.
- Zu den nativen Microsoft SQL Server-Tools gehören Sicherung und Wiederherstellung, Datenbankassistent kopieren, Datenbank kopieren und anfügen.

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserver-Instance.		DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie basierend auf Kapazität, Speicherfunktionen und Netzwerkfunktionen den richtigen Instance-Typ aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA, Systemadministrator
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, Systemadministrator

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherheitsgruppen.		Systemadministrator
Konfigurieren und starten Sie eine Amazon RDS-DB-Instance.		DBA, Systemadministrator

Daten migrieren – Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native SQL Server-Tools oder Tools von Drittanbietern, um Datenbankobjekte und -daten zu migrieren.		DBA

Daten migrieren – Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.		DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie die Anwendungsclients auf die neue Infrastruktur.		DBA, App-Besitzer, Systemadministrator

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Erfassen Sie Metriken wie die Zeit für die Migration, den Prozentsatz manueller und automatisierter Aufgaben sowie Kosteneinsparungen.		DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Bereitstellen von Microsoft SQL Server auf Amazon Web Services
- AWS DMS-Website
- Amazon RDS – Preise
- Microsoft-Produkte in AWS
- Microsoft-Lizenzierung in AWS

- Microsoft SQL Server auf AWS
- Verwenden der Windows-Authentifizierung mit einer Microsoft SQL Server-DB-Instance
- Amazon-RDS-Multi-AZ-Bereitstellungen

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS DMS (Video)
- Amazon RDS (Video)

Migrieren von Daten von Microsoft Azure Blob zu Amazon S3 mithilfe von Rclone

Erstellt von Suhas Basavaraj (AWS), An Keane (AWS) und Corey Bole (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Microsoft Azure-Speichercontainer	Ziel: Amazon S3-Bucket
R-Typ: Plattformwechsel	Workload: Microsoft	Technologien: Migration; Speicher und Backup
AWS-Services: Amazon S3		

Übersicht

Dieses Muster beschreibt, wie Sie Rclone verwenden, um Daten aus dem Microsoft Azure Blob-Objektspeicher in einen Amazon Simple Storage Service (Amazon S3)-Bucket zu migrieren. Sie können dieses Muster verwenden, um eine einmalige Migration oder eine fortlaufende Synchronisation der Daten durchzuführen. Rclone ist ein in Go geschriebenes Befehlszeilenprogramm und wird verwendet, um Daten über verschiedene Speichertechnologien von Cloud-Anbietern zu verschieben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Im Azure-Blob-Container-Service gespeicherte Daten

Architektur

Quelltechnologie-Stack

- Azure-Blob-Speichercontainer

Zieltechnologie-Stack

- Amazon S3-Bucket
- Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instance

Architektur

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Rclone ist ein Open-Source-Befehlszeilenprogramm, das von rsync unterstützt wird. Es wird verwendet, um Dateien auf vielen Cloud-Speicherplattformen zu verwalten.

Bewährte Methoden

Beachten Sie beim Migrieren von Daten von Azure zu Amazon S3 diese Überlegungen, um unnötige Kosten oder langsame Übertragungsgeschwindigkeiten zu vermeiden:

- Erstellen Sie Ihre AWS-Infrastruktur in derselben geografischen Region wie das Azure-Speicherkonto und der Blob-Container, z. B. AWS-Region `us-east-1` (Nord-Virginia) und Azure-Region `East US`.
- Vermeiden Sie nach Möglichkeit die Verwendung von NAT Gateway, da dadurch Datenübertragungsgebühren sowohl für die eingehende als auch für die ausgehende Bandbreite anfallen.
- Verwenden Sie einen VPC-Gateway-Endpunkt für Amazon S3, um die Leistung zu erhöhen.
- Erwägen Sie die Verwendung einer prozessorbasierten AWS Graviton2 (ARM) EC2-Instance für niedrigere Kosten und höhere Leistung als Intel x86-Instances. Der Klon ist stark kompiliert und bietet eine vorkompilierte ARM-Binärdatei.

Polen

Vorbereiten von AWS- und Azure-Cloud-Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie einen S3-Ziel-Bucket vor.	Erstellen Sie einen neuen S3-Bucket in der entsprechenden AWS-Region oder wählen Sie einen vorhandenen Bucket als Ziel für die Daten aus, die Sie migrieren möchten.	AWS-Administrator
Erstellen Sie eine IAM-Instance-Rolle für Amazon EC2.	Erstellen Sie eine neue AWS Identity and Access Management (IAM)-Rolle für Amazon EC2. Diese Rolle gibt Ihrer EC2-Instance Schreibzugriff auf den S3-Ziel-Bucket.	AWS-Administrator
Fügen Sie der IAM-Instance-Rolle eine Richtlinie hinzu.	Verwenden Sie die IAM-Konsole oder AWS Command Line Interface (AWS CLI), um eine Inline-Richtlinie für die EC2-Instance-Rolle zu erstellen, die Schreibzugriffsberechtigungen für den S3-Ziel-Bucket zulässt. Eine Beispielrichtlinie finden Sie im Abschnitt Zusätzliche Informationen.	AWS-Administrator
Starten einer EC2-Instance.	Starten Sie eine Amazon Linux 2 EC2-Instance, die für die Verwendung der neu erstellten IAM-Servicerolle konfiguriert ist. Diese Instance benötigt auch Zugriff	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf öffentliche Azure-API-Endpunkte über das Internet. Hinweis: Erwägen Sie, AWS Graviton-basierte EC2-Instances zu verwenden, um die Kosten zu senken. Rclone stellt ARM-kompilierte Binärdateien bereit.	
Erstellen Sie einen Azure-AD-Service-Prinzipal.	Verwenden Sie die Azure CLI, um einen Azure Active Directory (Azure AD)-Service-Prinzipal zu erstellen, der schreibgeschützten Zugriff auf den Azure Blob-Quellspeichercontainer hat. Anweisungen finden Sie im Abschnitt Zusätzliche Informationen. Speichern Sie diese Anmeldeinformationen auf Ihrer EC2-Instance am Speicherort `~/azure-principal.json` .	Cloud-Administrator, Azure

Installieren und Konfigurieren von Rclone

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Rclone herunter und installieren Sie es.	Laden Sie das Rclone-Befehlszeilenprogramm herunter und installieren Sie es. Installationsanweisungen finden Sie in der Rclone-Installationsdokumentation.	Allgemeines AWS, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Rclone.	Kopieren Sie die folgende `rclone.conf` Beispieldatei. Ersetzen Sie durch `AZStorageAccount` Ihren Azure Storage-Kontonamen und `us-east-1` durch die AWS-Region, in der sich Ihr S3-Bucket befindet. Speichern Sie diese Datei am Speicherort `~/.config/rclone/rclone.conf` auf Ihrer EC2-Instance.
	
	`[AZStorageAccount]`
	`type = azureblob`
	`account = AZStorageAccount`
	`service_principal_file = azure-principal.json`
	
	`[s3]`
	`type = s3`
	`provider = AWS`
	`env_auth = true`
	`region = us-east-1`
		Allgemeines AWS, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Konfiguration des Klons.	Um zu bestätigen, dass Rclone konfiguriert ist und die Berechtigungen ordnungsgemäß funktionieren, stellen Sie sicher, dass Rclone Ihre Konfigurationsdatei analysieren kann und dass auf Objekte in Ihrem Azure-Blob-Container und S3-Bucket zugegriffen werden kann. Im Folgenden finden Sie Beispiele für Validierungsbefehle. • Listen Sie die konfigurierten Remotes in der Konfigurationsdatei auf. Dadurch wird sichergestellt, dass Ihre Konfigurationsdatei korrekt analysiert wird. Überprüfen Sie die Ausgabe, um sicherzustellen, dass sie mit Ihrer `rclone.conf` Datei übereinstimmt. `rclone listremotes AZStorageAccount: s3:` • Listen Sie die Azure-Blob-Container im konfigurierten Konto auf. Ersetzen Sie durch `AZStorageAccount` den Namen des Speicherkontos, den Sie in der `rclone.conf` Datei verwendet haben.	Allgemeines AWS, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>rclone lsd AZStorage
	Account:
	2020-04-29 08:29:26
	docs</pre>
	• Listen Sie die Dateien im Azure-Blob-Container auf. Ersetzen Sie docs in diesem Befehl durch einen tatsächlichen Blob-Containernamen in Ihrem Azure-Speicherkonto.
	<pre>rclone ls AZStorage
	Account:docs
	824884 administr
	ator-en.a4.pdf</pre>
	• Listen Sie die Buckets in Ihrem AWS-Konto auf.
	<pre>[root@ip-10-0-20-157
	~]# rclone lsd s3:
	2022-03-07 01:44:40
	examplebu
	cket-01
	2022-03-07 01:45:16
	examplebu
	cket-02
	2022-03-07 02:12:07
	examplebu
	cket-03</pre>
	• Listen Sie die Dateien im S3-Bucket auf.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`[root@ip-10-0-20-157 ~]# rclone ls s3:examplebucket-01`
	`template0.yaml`
	`template1.yaml`	

Migrieren von Daten mit Rclone

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Migrieren Sie Daten aus Ihren Containern.	Führen Sie den Befehl Kopieren oder Synchronisieren klonen aus.
	
	Beispiel: Kopieren
	
	Dieser Befehl kopiert Daten aus dem Azure-Blob-Quellcontainer in den S3-Ziel-Bucket.
	
	`rclone copy AZStorageAccount:blob-container s3:examplebucket-01`
	
	Beispiel: Synchronisierung
	
	Dieser Befehl synchronisiert Daten zwischen dem Azure-Blob-Quellcontainer und dem S3-Ziel-Bucket.
	
	`rclone sync AZStorageAccount:blob-conta`
		Allgemeines AWS, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`iner s3:exampl ebucket-01` Wichtig: Wenn Sie den Synchronisierungsbefehl verwenden, werden Daten, die nicht im Quellcontainer vorhanden sind, aus dem Ziel-S3-Bucket gelöscht.	
Synchronisieren Sie Ihre Container.	Nachdem die erste Kopie abgeschlossen ist, führen Sie den Befehl Rclone sync für die laufende Migration aus, damit nur neue Dateien kopiert werden, die im Ziel-S3-Bucket fehlen.	Allgemeines AWS, Cloud-Administrator
Überprüfen Sie, ob die Daten erfolgreich migriert wurden.	Um zu überprüfen, ob die Daten erfolgreich in den S3-Ziel-Bucket kopiert wurden, führen Sie die Befehle Rclone lsd und ls aus.	Allgemeines AWS, Cloud-Administrator

Zugehörige Ressourcen

- Amazon S3-Benutzerhandbuch (AWS-Dokumentation)
- IAM-Rollen für Amazon EC2 (AWS-Dokumentation)
- Erstellen eines Microsoft Azure Blob-Containers (Microsoft Azure-Dokumentation)
- Rclone-Befehle (Rclone-Dokumentation)

Zusätzliche Informationen

Beispiel für eine Rollenrichtlinie für EC2-Instances

Diese Richtlinie gewährt Ihrer EC2-Instance Lese- und Schreibzugriff auf einen bestimmten Bucket in Ihrem Konto. Wenn Ihr Bucket einen vom Kunden verwalteten Schlüssel für die serverseitige Verschlüsselung verwendet, benötigt die Richtlinie möglicherweise zusätzlichen Zugriff auf AWS Key Management Service (AWS KMS).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
              "arn:aws:s3:::BUCKET_NAME/*",
              "arn:aws:s3:::BUCKET_NAME"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Erstellen eines schreibgeschützten Azure-AD-Service-Prinzipals

Ein Azure-Service-Prinzipal ist eine Sicherheitsidentität, die von Kundenanwendungen, Services und Automatisierungstools für den Zugriff auf bestimmte Azure-Ressourcen verwendet wird. Stellen Sie sich diese als Benutzeridentität (Anmeldung und Passwort oder Zertifikat) mit einer bestimmten Rolle und genau kontrollierten Berechtigungen für den Zugriff auf Ihre -Ressourcen vor. Gehen Sie wie folgt vor, um einen schreibgeschützten Service-Prinzipal zu erstellen, der die geringsten Berechtigungen befolgt und Daten in Azure vor versehentlichem Löschen schützt:

1. Melden Sie sich bei Ihrem Microsoft-Azure-Cloud-Kontoportal an und starten Sie Cloud Shell in PowerShell oder verwenden Sie die Azure Command-Line Interface (CLI) auf Ihrer Workstation.

2. Erstellen Sie einen Service-Prinzipal und konfigurieren Sie ihn mit schreibgeschütztem Zugriff auf Ihr Azure-Blob-Speicherkonto. Speichern Sie die JSON-Ausgabe dieses Befehls in einer lokalen Datei namens `azure-principal.json`. Die Datei wird in Ihre EC2-Instance hochgeladen. Ersetzen Sie die Platzhaltervariablen, die in Klammern ({ und }) angezeigt werden, durch Ihre Azure-Abonnement-ID, den Namen der Ressourcengruppe und den Namen des Speicherkontos.

```
az ad sp create-for-rbac `
--name AWS-Rclone-Reader `
--role "Storage Blob Data Reader" `
--scopes /subscriptions/{Subscription ID}/resourceGroups/{Resource Group Name}/
providers/Microsoft.Storage/storageAccounts/{Storage Account Name}
```

Migrieren Sie von Couchbase Server zu Couchbase Capella auf AWS

Erstellt von Battulga Purevragchaa (AWS), Mark Gamble und Saurabh Shanbhag (AWS)

Umgebung: Produktion	Quelle: Couchbase Server	Ziel: Couchbase Capella
R-Typ: Replatform	Arbeitslast: Alle anderen Workloads	Technologien: Migration; Analytik; Datenbanken

Übersicht

Couchbase Capella ist eine vollständig verwaltete NoSQL-Datenbank als Service (DBaaS) für unternehmenskritische Anwendungen (z. B. Benutzerprofile oder Online-Kataloge und Inventarverwaltung). Couchbase Capella verwaltet Ihre DBaaS-Arbeitslast in einem von Couchbase verwalteten Amazon Web Services (AWS) -Konto. Capella macht es einfach, die Replikation mit mehreren Clustern, mehreren AWS-Regionen, Multicloud und Hybrid-Clouds über eine einzige Oberfläche auszuführen und zu verwalten.

Couchbase Capella hilft Ihnen dabei, Ihre Couchbase Server-Anwendungen sofort zu skalieren, sodass Sie innerhalb von Minuten Cluster mit mehreren Knoten erstellen können. Couchbase Capella unterstützt alle Couchbase Server-Funktionen, einschließlich SQL++, Volltextsuche, Eventing Service und Analytics Service. Außerdem entfällt die Notwendigkeit, Installationen, Upgrades, Backups und die allgemeine Datenbankwartung zu verwalten.

Dieses Muster beschreibt die Schritte und bewährten Methoden für die Migration einer selbstverwalteten Couchbase Server-Umgebung in die AWS-Cloud. Das Muster bietet einen wiederholbaren Prozess für die Migration von Daten und Indizes von Couchbase Serverclustern, die entweder vor Ort oder in der Cloud ausgeführt werden, zu Couchbase Capella. Mithilfe dieser Schritte können Sie Probleme bei der Migration vermeiden und den gesamten Migrationsprozess beschleunigen.

Dieses Muster bietet die folgenden zwei Migrationsoptionen:

- Option 1 ist geeignet, wenn Sie weniger als 50 Indizes migrieren müssen.
- Option 2 ist geeignet, wenn Sie mehr als 50 Indizes migrieren müssen.

Sie können auch Beispieldaten auf Ihrem selbst verwalteten Couchbase-Server einrichten, um sie zusammen mit dem Migrationsleitfaden zu befolgen.

Wenn Sie die Migrationsoption 2 wählen oder Bereiche oder Sammlungen verwenden, die nicht dem Standardwert entsprechen, müssen Sie die Beispielkonfigurationsdatei verwenden, die sich im Abschnitt Zusätzliche Informationen befindet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandenes kostenpflichtiges Couchbase Capella-Konto. Sie können auch ein Couchbase Capella-Konto auf AWS erstellen und die kostenlose Testversion von Couchbase Capella nutzen und dann auf ein kostenpflichtiges Konto upgraden, um Ihren Cluster für die Migration zu konfigurieren. Folgen Sie den Anweisungen unter Erste Schritte mit Couchbase Capella, um mit der Testversion zu beginnen.
- Eine bestehende, selbstverwaltete Couchbase Server-Umgebung, entweder vor Ort oder bei einem Cloud-Dienstanbieter bereitgestellt.
- Für Migrationsoption 2 Couchbase Shell und eine Konfigurationsdatei. Um die Konfigurationsdatei zu erstellen, können Sie die Beispieldatei verwenden, die sich im Abschnitt Zusätzliche Informationen befindet.
- Vertrautheit mit der Verwaltung von Couchbase Server und Couchbase Capella.
- Vertrautheit mit dem Öffnen von TCP-Ports und dem Ausführen von Befehlen in einer Befehlszeilenschnittstelle (CLI).

Für den Migrationsprozess sind außerdem die in der folgenden Tabelle beschriebenen Rollen und Fachkenntnisse erforderlich.

Rolle	Fachwissen	Verantwortlichkeiten
Couchbase-Administrator	• Vertrautheit mit Couchbase Server und Couchbase Capella • Grundkenntnisse in der Befehlszeile sind hilfreich, aber nicht erforderlich	• Couchbase Server- und Capella-spezifische Aufgaben

Systemadministrator, IT-Administrator	• Vertrautheit mit der selbstverwalteten Couchbase Server-Systemumgebung und Verwaltung	• Öffnen von Ports und Ermitteln von IP-Adressen auf selbstverwalteten Couchbase Server-Clusterknoten

Einschränkungen

- Dieses Muster wird verwendet, um Daten, Indizes und Couchbase-Volltextsuchindizes von Couchbase Server zu Couchbase Capella auf AWS zu migrieren. Das Muster gilt nicht für die Migration von Couchbase Eventing Service oder Couchbase Analytics.
- Couchbase Capella ist in mehreren AWS-Regionen verfügbar. up-to-date Informationen zu den Regionen, die Capella unterstützt, finden Sie unter Amazon Web Services in der Couchbase-Dokumentation.

Produktversionen

- Couchbase Server (Community oder Enterprise) Edition Version 5.x oder höher

Architektur

Quelltechnologie-Stack

- Couchbase-Server

Zieltechnologie-Stack

- Couchbase Capella

Zielarchitektur

1. Sie greifen über die Capella Control Plane auf Couchbase Capella zu. Sie können die Capella Control Plane verwenden, um Folgendes zu tun:
   - Kontrollieren und überwachen Sie Ihr Konto.

- Verwalten Sie Cluster und Daten, Indizes, Benutzer und Gruppen, Zugriffsberechtigungen, Überwachung und Ereignisse.

2. Cluster werden erstellt.
3. Die Capella-Datenebene befindet sich im von Couchbase verwalteten AWS-Konto. Nachdem Sie einen neuen Cluster erstellt haben, stellt Couchbase Capella ihn in mehreren Availability Zones in der ausgewählten AWS-Region bereit.
4. Sie können Couchbase-Anwendungen in einer VPC in Ihrem AWS-Konto entwickeln und bereitstellen. In der Regel greift diese VPC über VPC-Peering auf die Capella-Datenebene zu.

Tools

- Couchbase Cross Data Center Replication (XDCR) hilft bei der Replikation von Daten über Cluster hinweg, die sich bei verschiedenen Cloud-Anbietern und verschiedenen Rechenzentren befinden. Es wird verwendet, um Daten aus selbstverwalteten Couchbase Server-Clustern nach Couchbase Capella zu migrieren.

  Hinweis: XDCR kann nicht mit Couchbase Server Community Edition für die Migration zu Couchbase Capella verwendet werden. Stattdessen können Sie cbexport verwenden. Weitere Informationen finden Sie im Abschnitt Daten aus der Community Edition migrieren.
- Couchbase Shell ist eine Befehlszeilen-Shell für Couchbase Server und Couchbase Capella für den Zugriff auf lokale und entfernte Couchbase-Cluster. In diesem Muster wird Couchbase Shell zur Migration von Indizes verwendet.
- cbexport ist ein Couchbase-Hilfsprogramm zum Exportieren von Daten aus einem Couchbase-Cluster. In den Couchbase Server CLI-Tools enthalten.

Epen

Bereiten Sie die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bewerten Sie die Größe des selbstverwalteten Couchbase Server-Clusters.	Melden Sie sich bei der Couchbase-Webkonsole für Couchbase Server an und überprüfen Sie die Knoten	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Buckets Ihres selbstver walteten Clusters. 1. Um eine Liste der Clusterkn oten anzuzeigen, wählen Sie in der Navigationsleiste die Registerkarte Server. 2. Notieren Sie sich die Anzahl der Knoten und wählen Sie dann jeden Knoten in der Liste aus, um seine Eigenschaften anzuzeigen. 3. Notieren Sie den Arbeitssp eicher und den Speicherp latz für jeden einzelnen Knoten. 4. Wählen Sie in der Navigatio nsleiste die Registerk arte Buckets und wählen Sie dann jeden Bucket in der Liste aus, um dessen Eigenschaften anzuzeigen. Notieren Sie sich das RAM-Kontingent und die Einstellu ng zur Konfliktlösung für jeden Bucket. Sie verwenden Ihre selbst verwalteten Couchbase Server-Clusterkonfiguration en als allgemeinen Leitfaden für die Dimensionierung und Konfiguration des Zielclusters auf Couchbase Capella.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie Hilfe bei einer detaillierteren Anleitung zur Dimensionierung von Couchbase Capella benötigen , wenden Sie sich an Couchbase.	
Zeichnen Sie die Couchbase -Dienstverteilung auf dem selbstverwalteten Couchbase Server-Cluster auf.	1. Wählen Sie in der Couchbase-Webkonsole die Registerkarte Server, um die Liste der Clusterknoten anzuzeigen. 2. Wählen Sie jeden Knoten aus, um seine Eigenschaften anzuzeigen, und zeichnen Sie dann die Couchbase Service-Verteilung für jeden Knoten auf (Data Service, Query Service, Index Service, Search Service, Analytics Serviceund Eventing Service).	Couchbase-Administrator
Notieren Sie sich die IP-Adressen der selbstverwalteten Couchbase Server-Clusterknoten.	(Ignorieren Sie diesen Schritt, wenn Sie die Community Edition verwenden.) Notieren Sie sich die IP-Adresse für jeden Knoten in Ihrem Cluster. Sie werden später zur Zulassungsliste auf Ihrem Couchbase Capella-Cluster hinzugefügt.	Couchbase-Administrator, Systemadministrator

Stellen Sie Ressourcen auf Couchbase Capella bereit und konfigurieren Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Auswahl einer Vorlage.	1. Melden Sie sich bei Ihrer Couchbase Capella Control Plane an, wählen Sie in der Hauptnavigation die Registerkarte Dashboard oder die Registerkarte Cluster und wählen Sie dann Create Cluster. 2. Wählen Sie anhand der Informationen, die Sie bei der Evaluierung Ihres selbstverwalteten Couchbase Server-Clusters aufgezeichnet haben, die Clustervorlage aus, die den Anforderungen der Konfiguration entspricht. Wenn Sie keine geeignete Vorlage finden, wählen Sie im Editor für die Clustergröße die Option Benutzerdefinierte Vorlage aus.	Couchbase-Administrator
Wählen und konfigurieren Sie die Knoten.	Wählen und konfigurieren Sie die Knoten so, dass sie zu Ihrer selbstverwalteten Couchbase Server-Cluster-Umgebung passen, einschließlich der Anzahl der Knoten, der Dienstverteilung, der Rechenleistung oder des Arbeitsspeichers und des Speichers.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Couchbase Capella verwendet bewährte Methoden zur multidimensionalen Skalierung. Dienste und Knoten können nur gemäß den bewährten Bereitstellungsmethoden ausgewählt werden. Dies kann bedeuten, dass Sie die Konfigurationen Ihres selbstverwalteten Couchbase Server-Clusters nicht genau anpassen können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Cluster bereit.	Wählen Sie eine Supportzone und ein Supportpaket aus und stellen Sie dann den Cluster bereit. Ausführliche Schritte und Anweisungen finden Sie in der Couchbase-Dokumentation unter Cluster erstellen. Wichtig: Wenn Sie die kostenlose Testversion von Couchbase Capella verwenden, müssen Sie sie in ein kostenpflichtiges Konto umwandeln, bevor Sie mit der Migration beginnen. Um Ihr Konto zu konvertieren, öffnen Sie in der Couchbase Capella Control Plane den Bereich Abrechnung und wählen Sie dann Aktivierungs-ID hinzufügen. Die Aktivierungs-ID wird an Ihre Rechnungskontakt-E-Mail-Adresse gesendet, nachdem Sie einen Kaufvertrag mit Couchbase Sales abgeschlossen haben oder nachdem Sie einen Kauf über AWS Marketplace getätigt haben.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzer mit Datenbankanmeldedaten.	Ein Benutzer mit Datenbank anmeldedaten ist clustersp ezifisch und besteht aus einem Benutzernamen, einem Passwort und einer Reihe von Bucket-Rechten. Dieser Benutzer ist erforderlich, um Buckets zu erstellen und auf Bucket-Daten zuzugreifen. Erstellen Sie in der Couchbase Capella Control Plane Datenbankanmeldeda ten für den neuen Cluster, indem Sie den Anweisungen unter Datenbankanmeldeda ten konfigurieren in der Couchbase Capella-D okumentation folgen. Hinweis: Einem Organisat ionsbenutzer müssen Anmeldeinformationen für die Organisationsrolle zugewiesen werden, wenn er entweder remote oder über die Couchbase Capella-B enutzeroberfläche auf Bucket-Daten in einem bestimmten Cluster zugreifen möchte. Dies ist unabhängig von Datenbank anmeldedaten, die normalerw eise von Apps und Integrati onen verwendet werden. Wenn Sie den Organisat	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ionsbenutzer erstellen, können Sie die Ziel-Buckets auf Ihrem Couchbase Capella-Cluster erstellen und verwalten.	
Wenn Sie die Migrationsoption 2 verwenden, installieren Sie Couchbase Shell.	Sie können Couchbase Shell auf jedem System installieren, das Netzwerkzugriff sowohl auf Ihren selbst verwaltet en Couchbase-Server als auch auf die Couchbase Capella-Cluster hat. Weitere Informationen finden Sie unter Installieren von Couchbase Shell Version 1.0.0-beta.5 in der Couchbase Shell-Dok umentation. Stellen Sie sicher, dass Couchbase Shell installiert ist, indem Sie eine Verbindun g zu Ihrem selbstverwalteten Cluster in einem Befehlsze ilenterminal testen.	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
IP-Adressen zulassen.	1. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann Ihren Zielcluster aus. 2. Wählen Sie die Registerk arte Connect für den Cluster und notieren Sie den Verbindungsendpunkt für Ihren Cluster, der unter Zulässige IP verwalten aufgeführt ist. 3. Gehen Sie wie folgt vor, um die IP-Adresse für das System, auf dem Sie Couchbase Shell installiert haben, und die IP-Adress e Ihrer selbstverwalteten Couchbase Server-Cluster-Instanzen als zulässige IP-Adressen hinzuzufügen: a. Wählen Sie unter Wide Area Network die Option Zulässige IP verwalten aus. b. Wählen Sie Add Allowed IP, geben Sie die IP-Adresse für das System ein, auf dem Sie Couchbase Shell installie rt haben, und wählen Sie dann Add IP. c. Wiederholen Sie den vorherigen Schritt,	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um die IP-Adresse Ihrer selbstverwalteten Couchbase Server-Cl usterinstanz hinzuzufü gen. Weitere Informationen zu zulässigen IP-Adressen finden Sie unter Zulässige IP-Adressen konfigurieren in der Couchbase-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zertifikate konfigurieren.	1. Um das Stammzertifikat für Ihren Cluster herunterz uladen, wählen Sie unter Stammzertifikat die Option Herunterladen aus. 2. Speichern Sie das Stammzertifikat mit der Dateierweiterung.pem in einem Ordner auf dem System, auf dem Couchbase Shell ausgeführ t werden soll. 3. Melden Sie sich als Nächstes bei Ihrer selbst verwalteten Couchbase Server-Webkonsole an, wählen Sie in der linken Navigationsleiste Sicherheit und dann die Registerkarte Zertifikate. 4. Kopieren Sie das Stammzertifikat für Ihren selbstverwalteten Couchbase Server-Cl uster und speichern Sie es als.pem-Datei in demselben Ordner, in dem Sie die Stammzertifikatsdatei für Ihren Couchbase Capella-Cluster gespeichert haben. Weitere Informationen zum Stammzertifikat finden Sie unter Root-Zertifikat in der	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Couchbase Server-Dokumentation.	
Erstellen Sie die Konfigurationsdatei für Couchbase Shell.	Erstellen Sie eine Konfigurations-Punktdatei im Home-Verzeichnis der Couchbase Shell-Installation (z. B.). `/<HOME_DIRECTORY>/.cbsh/config` Weitere Informationen finden Sie unter Config Dotfiles in der Couchbase-Dokumentation. Fügen Sie der Konfigurationsdatei Verbindungseigenschaften für die Quell- und Zielcluster hinzu. Sie können die Beispielkonfigurationsdatei im Abschnitt Zusätzliche Informationen verwenden und die Einstellungen für Ihre Cluster bearbeiten. Speichern Sie die Konfigurationsdatei mit den aktualisierten Einstellungen in dem `.cbsh` Ordner (z. B.`/<HOME_DIRECTORY>/.cbsh/config`).	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ziel-Buckets erstellen.	Erstellen Sie für jeden Quell-Bucket einen Ziel-Bucket in Ihrem Couchbase Capella-Cluster, indem Sie den Anweisungen unter Bucket erstellen in der Couchbase-Dokumentation folgen. Ihre Ziel-Bucket-Konfigurationen müssen mit den Bucket-Namen, Speichereinstellungen und Konfliktlösungseinstellungen der Buckets in Ihrem selbstverwalteten Couchbase Server-Cluster übereinstimmen.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiche und Sammlungen erstellen.	Jeder Bucket enthält einen Standardbereich und eine Standardsammlung mit dem `_default._default` Schlüsselraum. Wenn Sie andere Schlüsselräume für Ihren Bereich und Ihre Sammlung verwenden , müssen Sie identische Schlüsselräume im Capella-Zielcluster erstellen. 1. Öffnen Sie das Befehlszeilenterminal auf dem System, auf dem Sie Couchbase Shell installiert haben. 2. Führen Sie den folgenden Befehl aus, um Couchbase Shell zu starten. `./cbsh` 3. Erstellen Sie für jeden Bucket, den Sie migrieren möchten, Bereiche und Sammlungen im Capella-Cluster, indem Sie die folgenden Befehle ausführen. Stellen Sie sicher, dass Sie es <BUCKET_NAME>durch den Namen des Buckets ersetzen, den Sie migrieren möchten.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`scopes --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope | where scope != "_default" | each { |it| scopes create $it.scope --clusters "Capella-Cluster" } collections --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope collection | where $it.scope != "_default" | where $it.collection != "_default" | each { |it| collections create $it.collection --clusters "Capella-Cluster" --bucket <BUCKET_NAME> --scope $it.scope }`	

Migrieren Sie die Daten aus der Enterprise Edition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie TCP-Ports auf den selbstverwalteten Couchbase Server-Clusterknoten.	Stellen Sie sicher, dass die entsprechenden Ports für die XDCR-Kommunikation auf den Knoten des selbstverwalteten Couchbase Server-Clusters geöffnet sind. Weitere Informationen finden Sie in der Dokumentation zu den Couchbase Server-Ports.	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenn Sie Couchbase Server Enterprise Edition verwenden, richten Sie Couchbase XDCR ein.	1. Wählen Sie in der Hauptnavigation der Couchbase Capella Control Plane die Option Clusters und dann den Zielcluster für die Migration aus. 2. Wählen Sie unter Stammzertifikat die Option Kopieren aus. 3. Melden Sie sich bei Ihrer selbst verwalteten Couchbase Server-We bkonsole an und wählen Sie in der Hauptnavigation XDCR aus. Wählen Sie dann „Fernbedienung hinzufügen“. 4. Geben Sie die folgenden Einstellungen ein: • Clustername — Ein Name für die Capella-C luster-Verbindung • IP/Hostname — Der Verbindungsendpunk t für Ihren Couchbase Capella-Cluster • Benutzername für Remote Cluster — Der Datenbankbenutzer für Ihren Couchbase Capella-Cluster • Passwort — Das Datenbankbenutzerp	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	asswort für Ihren Couchbase Capella-Cluster • Sichere Verbindung aktivieren — Ausgewählt • Vollständig (TLS-Verschlüsselung von Passwort und Daten) — Ausgewählt 5. Fügen Sie das Capella-Cluster-Root-Zertifikat ein, das Sie zuvor kopiert haben, und wählen Sie dann Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Couchbase XDCR.	1. Wählen Sie in Ihrer selbst verwalteten Couchbase Server-Webkonsole in der Hauptnavigation XDCR und dann Add Replication aus. 2. Geben Sie die folgenden Einstellungen ein: • Aus Bucket replizieren — Wählen Sie den Quell-Bucket für die Migration aus. • Remote-Bucket — Geben Sie den Namen des Ziel-Buckets ein. • Remote-Cluster — Wählen Sie den Zielclust er aus, den Sie zuvor erstellt haben. 3. Wählen Sie „Replizier ung speichern“. Der Replikationsvorgang sollte innerhalb weniger Sekunden beginnen.	Couchbase-Administrator

Migrieren Sie die Indizes mithilfe von Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie selbstverwaltete Cluster-Indizes zu Couchbase Capella.	Wichtig: Wir empfehlen diesen Vorgang, wenn Sie weniger als 50 Indizes migrieren müssen. Wenn Sie mehr als 50 Indizes migrieren	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	müssen, empfehlen wir Ihnen, die Migrationsoption 2 zu verwenden. 1. Wählen Sie auf der Couchbase-Webkonsole Indizes aus. 2. Wählen Sie in der Liste der Indizes den ersten Index aus, den Sie migrieren möchten. Die Indexdefinition wird dann angezeigt. 3. Kopieren Sie die Indexdefinition mithilfe der `CREATE` Anweisung, aber kopieren Sie sie nicht`WITH { "defer_build":true }` . Aus der folgenden Beispielindexdefinition würden Sie beispielsweise nur kopieren`CREATE INDEX` `` `cityindex` `` `ON` `` `travel-sample`(`city`) ``. ``` CREATE INDEX `cityindex` ON `travel-sample`(`city`) WITH { "defer_build":true } ``` 4. Wählen Sie in der Couchbase Capella Control	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Plane Clusters und dann den Zielcluster aus. 5. Wählen Sie in der Dropdownliste Tools die Option Query Workbench aus. Fügen Sie die **`CREATE`** Anweisung, die Sie zuvor kopiert haben, in den Abfrage-Editor ein, und wählen Sie dann Ausführen . Dadurch wird der Index erstellt und erstellt. 6. Um zu bestätigen, dass der Index erstellt wurde, wählen Sie Indizes aus der Dropdownliste Tools aus. Die Liste zeigt, dass der Index erstellt und erstellt wurde. 7. Wiederholen Sie diesen Vorgang für jeden Index, der migriert werden muss.	

Migrieren Sie die Indizes mithilfe von Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Indexdefi nitionen.	Wichtig: Wir empfehlen diesen Vorgang, wenn Sie mehr als 50 Indizes migrieren möchten. Wenn Sie weniger als 50 Indizes migrieren müssen, empfehlen wir Ihnen,	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die Migrationsoption 1 zu verwenden.
	
	1. Öffnen Sie das Befehlsze ilenterminal auf dem System, auf dem Sie Couchbase Shell installiert haben.
	2. Führen Sie den folgenden Befehl aus, um Couchbase Shell zu starten.
	
	`./cbsh`
	
	3. Führen Sie den folgenden Befehl aus, um eine Verbindung zum selbstver walteten Couchbase Server-Cluster herzustellen.
	
	`cb-env cluster On-Prem-Cluster`
	
	4. Um Indexdefinitionen vom selbstverwalteten Couchbase Server-Cluster zum Couchbase Capella-C luster zu migrieren, führen Sie den folgenden Befehl für jeden Bucket aus, den Sie migrieren möchten. Stellen Sie sicher, dass Sie es durch den Bucket-Na men <BUCKET_NAME> ersetzen, der den Indizes entspricht, die Sie migrieren	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten. Diese Migration soption setzt voraus, dass Ihre Ziel-Bucket-Namen mit den Quell-Bucket-Namen identisch sind. `query indexes --definitions | where bucket =~ <BUCKET_NAME>| get definition | each { |it| query $it --clusters Capella-Cluster }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Indexdefinitionen.	1. Führen Sie den folgenden Befehl aus, um den Kontext zum Couchbase Capella-Cluster zu wechseln:
	`cb-env cluster Capella-Cluster`
	2. Um die Indexdefinitionen zu erstellen, die auf den Couchbase Capella-Cluster migriert wurden, führen Sie den folgenden Befehl aus und <BUCKET_NAME> ersetzen Sie ihn durch den Bucket-Namen, der den Indizes entspricht, die Sie erstellen möchten.
	`query 'SELECT RAW CONCAT("BUILD INDEX ON ", k , "(['", CONCAT2 ("','", inames), "']);") FROM system:indexes AS s LET bid = CONCAT("` ",s.bucket_id, "`"), sid = CONCAT("`", s.scope_id, "`"), kid = CONCAT("` ", s.keyspace_id, "`"), k = NVL2(bid, CONCAT2(".", bid, sid, kid), kid) WHERE s.namespa ce_id = "default" AND s.bucket_id = "" GROUP BY k LETTING`
		Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	inames = ARRAY_AGG (s.name) FILTER (WHERE s.state = 'deferred') HAVING ARRAY_LENGTH(iname s) > 0;' | each { | it| query $it } 3. Wiederholen Sie den Vorgang für jeden Bucket.	

Migrieren Sie Volltext-Suchindexe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie selbstverwaltete Cluster-Volltextsuchindizes zu Couchbase Capella.	1. Wählen Sie in der Couchbase-Webkonsole Suchen aus. 2. Wählen Sie in der Liste der Indizes für die Volltexts uche (FTS) den ersten FTS-Index aus, den Sie migrieren möchten, wählen Sie Indexdefinition anzeigen und anschließend In die Zwischenablage kopieren. Notieren Sie sich den Indexnamen und den Bucket, zu dem er gehört. 3. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster aus.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie in der Dropdownliste Tools die Option Volltextsuche aus. 5. Wählen Sie Index importieren und fügen Sie die FTS-Indexdefinition ein. 6. Geben Sie den Indexnamen ein, wählen Sie den richtigen Bucket aus, wie auf dem selbstverwalteten Cluster angegeben, und wählen Sie dann Create aus. 7. Wiederholen Sie diesen Vorgang für jeden FTS-Index, der migriert werden muss.	

Migrieren Sie Daten aus der Couchbase Community Edition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie Daten aus der selbstverwalteten Couchbase Server Community Edition.	Verschlüsseltes XDCR ist in der Couchbase Community Edition nicht verfügbar. Sie können Daten aus der Couchbase Community Edition exportieren und die Daten dann manuell in Couchbase Capella importieren. Verwenden `cbexport` Sie die Befehlszeile, um Daten aus	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Quell-Bucket zu exportieren. Der folgende Befehl dient als Beispiel. `cbexport json \ --cluster localhost \ --bucket <SOURCE BUCKET NAME> \ --format lines \ --username <USERNAME> \ --password <PASSWORD> \ --include-key cbkey \ --scope-field cbscope \ --collection-field cbcoll \ --output cbexported_data.json` Beachten Sie`cbkey`, dass `cbscope`und `cbcoll` beliebige Bezeichnungen `cbexported_data.json` sind. Sie werden später im Prozess referenziert. Wenn Sie sie also anders benennen möchten, notieren Sie sich das.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten in Couchbase Capella importieren.	1. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster aus. 2. Wählen Sie in der Dropdownliste Tools die Option Import aus. Dadurch wird ein Assistent mit den folgenden sechs Schritten geöffnet: a. Bucket — Wählen Sie den Ziel-Bucket aus. b. Datei — Wählen Sie JSON, dann Lines und anschließend Using your web browser aus. Wenn Sie über eine große Datenmenge verfügen, können Sie die Option Manuell ausprobieren. Wählen Sie die Datei aus, die von erstellt wurde`cbexport`. c. Sammlungen — Wählen Sie „Benutzerdefiniertes Sammlungs-Mapping“. Wenn Ihre Community Edition-Datenbank keine Bereiche oder Sammlungen oder nur _default verwendet, können Sie stattdess en die Option Einzelne	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sammlung auswählen wählen. Geben Sie als Ausdruck für die Zuordnung von Sammlungen den Wert ein. `%cbscope %.%cbcoll%` Um zu überprüfen, ob dieser Ausdruck korrekt funktioniert, können Sie Beispieldaten einfügen, z. B. die folgenden. `{ "cbscope" :"inventory", "cbcoll":"landmark", "cbkey":" landmark_3991" }` d. Schlüssel — Wählen Sie Customer Generation. (Wenn Sie die Schlüssel der importierten Daten nicht beibehalten möchten, können Sie stattdessen Automatisch generierte UUID auswählen und mit Schritt 5 fortfahren.) Geben Sie für Key Name Generator Expression %cbkey% ein. Um zu überprüfen, ob dieser Ausdruck korrekt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	funktioniert, fügen Sie einige Beispieldaten ein. e. Konfigurationen — Wählen Sie Felder ignorieren und geben Sie cbscope, cbcoll, cbkey ein. Diese Felder enthalten vorüberge hende Informationen, die sich nach einem Import nicht im Ziel-Buck et befinden müssen. Übernehmen Sie für die anderen Einstellungen die Standardwerte. f. Import — Überprüfen Sie den Vorgang und wählen Sie Import, wenn Sie bereit sind. Warten Sie auf den Upload und den Datenimport. Für große Dateien unterstüt zt Couchbase Capella den Befehlszeilenimport mit cURL. Weitere Informationen zu den Importoptionen finden Sie unter Daten importieren in der Couchbase Capella-D okumentation.	

Testen und verifizieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenmigration.	1. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster in Ihrer Cluster-Liste aus. 2. Wählen Sie die Registerkarte Buckets für Ihren Zielcluster. Stellen Sie sicher, dass die Anzahl der Elemente (Dokumente) im Ziel-Bucket mit der Anzahl der Elemente im Quell-Bucket übereinstimmt. 3. Wählen Sie im Zielcluster in der Dropdownliste Tools die Option Dokumente aus. Stellen Sie sicher, dass alle Dokumente migriert wurden. 4. (Optional) Nachdem alle Daten migriert wurden, können Sie die Replikation beenden, indem Sie sie löschen. Weitere Informationen finden Sie in der Couchbase-Dokumentation unter Löschen einer Replikation.	Couchbase-Administrator
Überprüfen Sie die Indexmigration.	Wählen Sie in der Couchbase Capella Control Plane in der Dropdownliste Tools für Ihren	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zielcluster die Option Indizes aus. Stellen Sie sicher, dass die Indizes migriert und erstellt wurden.	
Überprüfen Sie die Abfrageergebnisse.	1. Wählen Sie in der Couchbase Capella Control Plane in der Dropdownliste Tools für Ihren Zielcluster die Option Query Workbench aus. 2. Führen Sie eine N1QL-Beispielabfrage oder eine in Ihrer Anwendung verwendete Abfrage aus. Stellen Sie sicher, dass Sie dieselben Ergebnisse erhalten wie bei der Ausführung der Abfrage in Ihrem selbstverwalteten Couchbase Server-Cluster.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ergebnisse der Volltextsuche (gilt, wenn Sie FTS-Indizes migriert haben).	1. Wählen Sie in der Couchbase Capella Control Plane in der Dropdownliste Tools für Ihren Zielcluster die Option Volltextsuche aus. 2. Wählen Sie einen FTS-Index aus, indem Sie seinen Namen wählen. 3. Wählen Sie Search (Suchen) aus. 4. Geben Sie eine Beispielsuchabfrage ein und wählen Sie Suchen aus. 5. Stellen Sie sicher, dass die Ergebnisse dieselben sind wie bei der Ausführung der Suche auf Ihrem selbstverwalteten Cluster.	Couchbase-Administrator

Zugehörige Ressourcen

Bereiten Sie die Migration vor

- Beginnen Sie mit der kostenlosen Testversion von Couchbase Capella
- Anforderungen des Cloud-Anbieters für Couchbase Capella
- Größenrichtlinien für Couchbase Capella

Migrieren Sie die Daten und Indizes

- Couchbase XDCR
- Couchbase Shell-Dokumentation

Couchbase Capella SLAs und Support

- Couchbase Capella Service Level Agreements (SLAs)
- Support-Richtlinie für den Couchbase Capella Service

Zusätzliche Informationen

Der folgende Code ist eine Beispielkonfigurationsdatei für Couchbase Shell.

```
Version = 1

[[clusters]]
identifier = "On-Prem-Cluster"
hostnames = ["<SELF_MANAGED_COUCHBASE_CLUSTER>"]
default-bucket = "travel-sample"
username = "<SELF_MANAGED_ADMIN>"
password = "<SELF_MANAGED_ADMIN_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"

[[clusters]]
identifier = "Capella-Cluster"
hostnames = ["<COUCHBASE_CAPELLA_ENDPOINT>"]
default-bucket = "travel-sample"
username = "<CAPELLA_DATABASE_USER>"
password = "<CAPELLA_DATABASE_USER_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"
```

Bevor Sie die Konfigurationsdatei speichern, stellen Sie anhand der folgenden Tabelle sicher, dass Sie Ihre eigenen Quell- und Zielclusterinformationen hinzugefügt haben.

<SELF_MANAGED_COUCHBASE_CLUSTER>	Verwenden Sie die IP-Adresse für Ihren selbstverwalteten Couchbase Server-Cluster.

<SELF_MANAGED_ADMIN>	Verwenden Sie den Administratorbenutzer für Ihren selbstverwalteten Couchbase Server-Cluster.
<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>	Verwenden Sie den absoluten Pfad zur gespeicherten Root-Zertifikatsdatei für Ihren selbstverwalteten Couchbase Server-Cluster.
<COUCHBASE_CAPELLA_ENDPOINT>	Verwenden Sie den Verbindungsendpunkt für Ihren Couchbase Capella-Cluster.
<CAPELLA_DATABASE_USER>	Verwenden Sie den Datenbankbenutzer für Ihren Couchbase Capella-Cluster.
<CAPELLA_DATABASE_USER_PWD>	Verwenden Sie das Datenbank-Benutzerpasswort für Ihren Couchbase Capella-Cluster.
<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>	Verwenden Sie den absoluten Pfad zur gespeicherten Root-Zertifikatsdatei für Ihren Couchbase Capella-Cluster.

Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2

Erstellt von Neal Ardeljan (AWS) und Afroz Khan (AWS)

Umwelt: Produktion	Quelle: Anwendungen	Ziel: Apache Tomcat auf einer Amazon EC2 EC2-Instance
R-Typ: Replatform	Arbeitslast: IBM; Open Source	Technologien: Migration; Web- und mobile Apps
AWS-Dienste: Amazon EC2		

Übersicht

Dieses Muster führt Sie durch die Schritte für die Migration von einem lokalen System mit Red Hat Enterprise Linux (RHEL) 6.9 oder höher, auf dem IBM WebSphere Application Server (WAS) ausgeführt wird, zu RHEL 8 mit Apache Tomcat auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Das Muster kann auf die folgenden Quell- und Zielversionen angewendet werden:

- WebSphere Application Server 7.x auf Apache Tomcat 8 (mit Java 7 oder höher)
- WebSphere Anwendungsserver 8.x auf Apache Tomcat 8 (mit Java 7 oder höher)
- WebSphere Anwendungsserver 8.5.5.x auf Apache Tomcat 9 (mit Java 8 oder höher)
- WebSphere Anwendungsserver 8.5.5.x auf Apache Tomcat 10 (mit Java 8 oder höher)

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java-Quellcode mit den folgenden Annahmen:
  - Verwendet die Java Development Kit (JDK) -Version von Java 7 oder höher
  - Verwendet das Spring- oder Apache Struts-Framework

  - Verwendet weder das Enterprise Java Beans (EJB) -Framework noch andere WebSphere Serverfunktionen, die für Tomcat nicht ohne weiteres verfügbar sind
  - Verwendet hauptsächlich Servlets oder Java Server Pages (JSPs)
  - Verwendet JDBC-Konnektoren (Java Database Connectivity), um eine Verbindung zu Datenbanken herzustellen
- Quelle: IBM WebSphere Application Server Version 7.x oder höher
- Zielversion von Apache Tomcat 8.5 oder höher

Architektur

Quelltechnologie-Stack

- Eine Webanwendung, die mit dem Apache Struts Model-View-Controller (MVC) -Framework erstellt wurde
- Eine Webanwendung, die auf IBM WebSphere Application Server Version 7.x oder 8.x ausgeführt wird
- Eine Webanwendung, die einen LDAP-Connector (Lightweight Directory Access Protocol) verwendet, um eine Verbindung zu einem LDAP-Verzeichnis (iPlanet/eTrust) herzustellen
- Eine Anwendung, die IBM Tivoli Access Manager (TAM) -Konnektivität verwendet, um das TAM-Benutzerkennwort zu aktualisieren (in der aktuellen Implementierung verwenden Anwendungen PD.jar)

Lokale Datenbanken

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Release 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1.0.2)

Zieltechnologie-Stack

- Apache Tomcat Version 8 (oder höher) läuft auf RHEL auf einer EC2-Instance
- Amazon Relational Database Service (Amazon RDS) für Oracle

Weitere Informationen zu den von Amazon RDS unterstützten Oracle-Versionen finden Sie auf der Website Amazon RDS for Oracle.

Zielarchitektur

Tools

- Anwendungsebene: Neuaufbau der Java-Anwendung in eine WAR-Datei.
- Datenbankebene: systemeigenes Backup und Wiederherstellung von Oracle.
- Apache Tomcat-Migrationstool für Jakarta EE. Dieses Tool konvertiert eine für Java EE 8 geschriebene Webanwendung, die auf Apache Tomcat 9 läuft, automatisch in die Ausführung auf Apache Tomcat 10, das Jakarta EE 9 implementiert.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vervollständigen Sie die Anwendungserkennung, den aktuellen Status und die Leistungsbasis.		BA, Leiter Migration
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Hardwareanforderungen für die EC2-Instance des Zielservers.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen EC2-Instance-Typ auf der Grundlage von Kapazität , Speicherfunktionen und Netzwerkfunktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie die Strategie und die Tools für die Anwendungsmigration.		DBA, Leiter der Migration
Vervollständigen Sie das Migrationsdesign und den Migrationsleitfaden für die Anwendung.		Leitung aufbauen, Leitung Migration
Vervollständigen Sie das Runbook zur Anwendungsmigration.		Leiter Aufbau, Leiter der Umstellung, Leiter des Tests, Leiter der Migration

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		SysAdmin
Erstellen Sie die Sicherheitsgruppen.		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie Amazon RDS for Oracle.		DBA, SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Endpoints oder verschaffen Sie sich Zugriff auf diese, um die Datenbank-Backupdateien abzurufen.		DBA
Verwenden Sie die native Datenbank-Engine oder ein Drittanbieter-Tool, um Datenbankobjekte und Daten zu migrieren.	Einzelheiten finden Sie unter „Migrieren von Datenbank objekten und Daten“ im Abschnitt Zusätzliche Informati onen.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie den Änderungs antrag (CR) für die Migration ein.		Übernahme (Leitung)
Besorgen Sie sich die CR-Genehmigung für die Migration.		Übernahme (Leitung)
Folgen Sie der Strategie zur Anwendungsmigration gemäß	Einzelheiten finden Sie unter „Einrichtung der Anwendung	DBA, Migrationsingenieur, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
dem Runbook zur Anwendung smigration.	sebene“ im Abschnitt Zusätzlic he Informationen.	
Aktualisieren Sie die Anwendung (falls erforderlich).		DBA, Migrationsingenieur, App-Besitzer
Führen Sie die Funktions- und Nichtfunktionstests sowie die Datenvalidierungs-, SLA- und Leistungstests durch.		Testleiter, App-Besitzer, App-Nutzer

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lassen Sie sich vom Inhaber der Anwendung oder dem Geschäftsinhaber genehmige n.		Übernahme (Leitung)
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA, Migrationsingenieur, App-Besitzer

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Migrationsingenieur, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie Kennzahlen wie die Zeit bis zur Migration , den Prozentsatz manueller Aufgaben im Vergleich zu automatisierten Aufgaben und Kosteneinsparungen.		Leiter der Migration
Schließe das Projekt ab und gib Feedback.		Leiter der Migration, Inhaber der App

Zugehörige Ressourcen

Referenzen

- Dokumentation zu Apache Tomcat 10.0
- Apache Tomcat 9.0-Dokumentation
- Apache Tomcat 8.0-Dokumentation
- Installationsanleitung für Apache Tomcat 8.0
- Apache Tomcat JNDI-Dokumentation
- Website von Amazon RDS for Oracle
- Amazon-RDS-Preise
- Oracle und Amazon Web Services
- Oracle auf Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen

Tutorials und Videos

- Erste Schritte mit Amazon RDS

Zusätzliche Informationen

Migrieren von Datenbankobjekten und Daten

Wenn Sie beispielsweise native Oracle-Dienstprogramme für Backup/Restore verwenden:

1. Erstellen Sie das Amazon Simple Storage Service (Amazon S3) -Backup für Datenbank-Backup-Dateien (optional).
2. Sichern Sie die Oracle-DB-Daten im gemeinsam genutzten Netzwerkordner.
3. Melden Sie sich beim Migration Staging Server an, um den Netzwerkfreigabeordner zuzuordnen.
4. Kopieren Sie Daten aus dem Netzwerkfreigabeordner in den S3-Bucket.
5. Fordern Sie eine Amazon RDS Multi-AZ-Bereitstellung für Oracle an.
6. Stellen Sie die lokale Datenbanksicherung auf Amazon RDS for Oracle wieder her.

Einrichtung der Anwendungsebene

1. Installieren Sie Tomcat 8 (oder 9/10) von der Apache Tomcat-Website.
2. Package Sie die Anwendung und die gemeinsam genutzten Bibliotheken in eine WAR-Datei.
3. Stellen Sie die WAR-Datei in Tomcat bereit.
4. Überwachen Sie das Startprotokoll `Linux cat` aller fehlenden gemeinsam genutzten Bibliotheken von WebSphere.
5. Sehen Sie sich den Startdatensatz `Linux cat` aller WebSphere -spezifischen Deployment-Deskriptor-Erweiterungen an.
6. Sammeln Sie alle fehlenden abhängigen Java-Bibliotheken vom WebSphere Server.
7. Ändern Sie WebSphere spezifische Deployment-Deskriptorelemente durch Tomcat-kompatible Äquivalente.
8. Erstellen Sie die WAR-Datei mit den abhängigen Java-Bibliotheken und den aktualisierten Deployment-Deskriptoren neu.
9. Aktualisieren Sie die LDAP-Konfiguration, die Datenbankkonfiguration und testen Sie die Verbindungen (siehe Realm Configuration HOW-TO und JNDI Datasource HOW-TO in der Apache Tomcat-Dokumentation).
10. Testen Sie die installierte Anwendung anhand der wiederhergestellten Amazon RDS for Oracle Oracle-Datenbank.
11. Erstellen Sie ein Amazon Machine Image (AMI) für Linux aus der EC2-Instance.
12. Starten Sie die fertige Architektur mit der Application Load Balancer- und Auto Scaling Scaling-Gruppe.

13 Aktualisieren Sie die URLs (mithilfe der WebSeal-Verbindung) so, dass sie auf den Application Load Balancer verweisen.

14 Aktualisieren Sie die Configuration Management Database (CMDB).

Migrieren Sie mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2

R-Typ: Replatform	Quelle: Anwendungen	Ziel: Apache Tomcat auf einer Amazon EC2 EC2-Instance mit aktiviertem Auto Scaling
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Web- und mobile Apps; Migration
Arbeitslast: Open Source; IBM	AWS-Dienste: Amazon EC2	

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Java-Anwendung von IBM WebSphere Application Server zu Apache Tomcat auf einer Amazon Elastic Compute Cloud (Amazon EC2) - Instance mit aktiviertem Amazon EC2 Auto Scaling.

Mit diesem Muster können Sie Folgendes erreichen:

- Eine Senkung der IBM-Lizenzkosten
- Hohe Verfügbarkeit durch Multi-AZ-Bereitstellung
- Verbesserte Anwendungsausfallsicherheit mit Amazon EC2 Auto Scaling

Voraussetzungen und Einschränkungen

Voraussetzungen

- Java-Anwendungen (Version 7). x oder 8. x) sollte in LAMP-Stacks entwickelt werden.
- Der Zielstatus besteht darin, Java-Anwendungen auf Linux-Hosts zu hosten. Dieses Muster wurde erfolgreich in einer Red Hat Enterprise Linux (RHEL) 7-Umgebung implementiert. Andere Linux-Distributionen können diesem Muster folgen, es sollte jedoch auf die Konfiguration der Apache Tomcat-Distribution verwiesen werden.
- Sie sollten die Abhängigkeiten der Java-Anwendung verstehen.

- Sie müssen Zugriff auf den Quellcode der Java-Anwendung haben, um Änderungen vornehmen zu können.

Einschränkungen und Änderungen an der Platformierung

- Sie sollten sich mit den Komponenten des Unternehmensarchivs (EAR) auskennen und sicherstellen, dass alle Bibliotheken in den WAR-Dateien der Webkomponente enthalten sind. Sie müssen das Apache Maven WAR-Plugin konfigurieren und WAR-Dateiartefakte erzeugen.
- Bei der Verwendung von Apache Tomcat 8 besteht ein bekannter Konflikt zwischen servlet-api.jar und den in das Anwendungspaket integrierten JAR-Dateien. Um dieses Problem zu beheben, löschen Sie servlet-api.jar aus dem Anwendungspaket.
- Sie müssen WEB-INF/Resources konfigurieren, das sich im Klassenpfad der Apache Tomcat-Konfiguration befindet. Standardmäßig werden die JAR-Bibliotheken nicht in das Verzeichnis geladen. Alternativ können Sie alle Ressourcen unter src/main/resources bereitstellen.
- Suchen Sie in der Java-Anwendung nach fest codierten Kontextwurzeln und aktualisieren Sie das neue Kontextstammverzeichnis von Apache Tomcat.
- Um die JVM-Laufzeitoptionen festzulegen, können Sie die Konfigurationsdatei setenv.sh im bin-Ordner von Apache Tomcat erstellen, z. B. JAVA_OPTS, JAVA_HOME usw.
- Die Authentifizierung wird auf Containerebene konfiguriert und in Apache Tomcat-Konfigurationen als Realm eingerichtet. Die Authentifizierung wird für einen der folgenden drei Bereiche eingerichtet:
  - JDBC Database Realm sucht nach Benutzern in einer relationalen Datenbank, auf die der JDBC-Treiber zugreift.
  - DataSource Database Realm sucht nach Benutzern in einer Datenbank, auf die JNDI zugreift.
  - JNDI Directory Realm sucht nach Benutzern im LDAP-Verzeichnis (Lightweight Directory Access Protocol), auf das der JNDI-Anbieter zugreift. Für die Suchvorgänge ist Folgendes erforderlich:
    - LDAP-Verbindungsdetails: Benutzersuchbasis, Suchfilter, Rollenbasis, Rollenfilter
    - Der wichtige JNDI-Verzeichnisbereich: Stellt eine Verbindung zu LDAP her, authentifiziert Benutzer und ruft alle Gruppen ab, in denen ein Benutzer Mitglied ist
- Autorisierung: Im Fall eines Containers mit einer rollenbasierten Autorisierung, die die Autorisierungseinschränkungen in web.xml überprüft, müssen Webressourcen definiert und mit den in den Einschränkungen definierten Rollen verglichen werden. Wenn LDAP nicht über eine Gruppenrollen-Zuordnung verfügt, müssen Sie das Attribut <security-role-ref>in web.xml festlegen,

um eine Gruppenrollen-Zuordnung zu erreichen. Ein Beispiel für ein Konfigurationsdokument finden Sie in der Oracle-Dokumentation.

- Datenbankverbindung: Erstellen Sie eine Ressourcendefinition in Apache Tomcat mit einer Amazon Relational Database Service (Amazon RDS) -Endpunkt-URL und Verbindungsdetails. Aktualisieren Sie den Anwendungscode mithilfe der JNDI-Suche so, dass er auf a DataSource verweist. Eine in definierte bestehende DB-Verbindung WebSphere würde nicht funktionieren, da sie die WebSphere JNDI-Namen verwendet. Sie können <resource-ref>in web.xml einen Eintrag mit dem JNDI-Namen und der DataSource Typdefinition hinzufügen. Ein Beispiel für ein Konfigurationsdokument finden Sie in der Apache Tomcat-Dokumentation.
- Protokollierung: Standardmäßig protokolliert Apache Tomcat in der Konsole oder in einer Protokolldatei. Sie können die Ablaufverfolgung auf Realmebene aktivieren, indem Sie logging.properties aktualisieren (siehe Logging in Tomcat). Wenn Sie Apache Log4j verwenden, um Logs an eine Datei anzuhängen, müssen Sie tomcat-juli herunterladen und es dem Klassenpfad hinzufügen.
- Sitzungsmanagement: Wenn Sie IBM WebSEAL für den Lastenausgleich von Anwendungen und das Sitzungsmanagement beibehalten, sind keine Änderungen erforderlich. Wenn Sie einen Application Load Balancer oder Network Load Balancer auf AWS verwenden, um die IBM WebSeal-Komponente zu ersetzen, müssen Sie das Sitzungsmanagement mithilfe einer ElastiCache Amazon-Instance mit einem Memcache-Cluster einrichten und Apache Tomcat für die Verwendung von Open-Source-Sitzungsmanagement einrichten.
- Wenn Sie den IBM WebSeal Forward Proxy verwenden, müssen Sie einen neuen Network Load Balancer auf AWS einrichten. Verwenden Sie die vom Network Load Balancer bereitgestellten IPs für WebSeal-Junction-Konfigurationen.
- SSL-Konfiguration: Wir empfehlen, Secure Sockets Layer (SSL) für end-to-end die Kommunikation zu verwenden. Folgen Sie den Anweisungen in der Apache Tomcat-Dokumentation, um eine SSL-Serverkonfiguration in Apache Tomcat einzurichten.

Architektur

Quelltechnologie-Stack

- IBM WebSphere Anwendungsserver

Zieltechnologie-Stack

- Die Architektur verwendet Elastic Load Balancing (Version 2). Wenn Sie IBM WebSeal für Identify Management und Load Balancing verwenden, können Sie einen Network Load Balancer auf AWS auswählen, der in den IBM WebSeal Reverse-Proxy integriert werden soll.
- Java-Anwendungen werden auf einem Apache Tomcat-Anwendungsserver bereitgestellt, der auf einer EC2-Instance in einer Amazon EC2 Auto Scaling Scaling-Gruppe ausgeführt wird. Sie können eine Skalierungsrichtlinie einrichten, die auf CloudWatch Amazon-Metriken wie der CPU-Auslastung basiert.
- Wenn Sie die Verwendung von IBM WebSeal für den Lastenausgleich einstellen, können Sie Amazon ElastiCache for Memcached für die Sitzungsverwaltung verwenden.
- Für die Back-End-Datenbank können Sie High Availability (Multi-AZ) für Amazon RDS bereitstellen und einen Datenbank-Engine-Typ auswählen.

Zielarchitektur

Tools

- AWS CloudFormation
- AWS-Befehlszeilenschnittstelle (AWS CLI)
- Apache Tomcat (Version 7). x oder 8. x)
- RHEL 7 oder Centos 7
- Bereitstellung von Amazon RDS Multi-AZ
- Amazon ElastiCache für Memcached (optional)

Epen

VPC einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Subnetze.		
Erstellen Sie bei Bedarf Routing-Tabellen.		
Erstellen Sie Netzwerkz ugriffskontrolllisten (ACLs).		
Richten Sie AWS Direct Connect oder eine Unternehm ens-VPN-Verbindung ein.		

Führen Sie die Anwendung auf eine neue Plattform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Refaktorieren Sie die Maven-Konfiguration des Anwendung sbuilds, um die WAR-Artefakte zu generieren.		
Refaktorieren Sie die Datenquellen für Anwendung sabhängigkeiten in Apache Tomcat.		
Refaktorieren Sie die Anwendungsquellcodes so, dass sie JNDI-Namen in Apache Tomcat verwenden.		
Stellen Sie die WAR-Artefakte in Apache Tomcat bereit.		
Vollständige Anwendung svalidierungen und Tests.		

Konfigurieren Sie das Netzwerk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Unternehmensfirewall so, dass die Verbindung zu den Abhängigkeitsdiensten möglich ist.		
Konfigurieren Sie die Unternehmensfirewall so, dass Endbenutzer auf Elastic Load Balancing auf AWS zugreifen können.		

Erstellen Sie die Anwendungsinfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendung und stellen Sie sie auf einer EC2-Instance bereit.		
Erstellen Sie einen Amazon ElastiCache for Memcached -Cluster für die Sitzungsv erwaltung.		
Erstellen Sie eine Amazon RDS Multi-AZ-Instance für die Backend-Datenbank.		
Erstellen Sie SSL-Zertifikate und importieren Sie sie in AWS Certificate Manager (ACM).		

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie SSL-Zertifikate auf Load Balancern.		
Installieren Sie SSL-Zertifikate für Apache Tomcat-Server.		
Führen Sie die Validierungen und Tests der Anwendungen durch.		

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die bestehende Infrastruktur herunter.		
Stellen Sie die Datenbank aus der Produktion in Amazon RDS wieder her.		
Überarbeiten Sie die Anwendung, indem Sie DNS-Änderungen vornehmen.		

Zugehörige Ressourcen

Referenzen

- Dokumentation zu Apache Tomcat 7.0
- Installationsanleitung für Apache Tomcat 7.0
- Apache Tomcat JNDI-Dokumentation
- Amazon RDS Multi-AZ-Bereitstellungen
- Amazon ElastiCache für Memcached

Tutorials und Videos

- Erste Schritte mit Amazon RDS

Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk

Erstellt von Raghavender Madamshitti (AWS)

Umgebung: PoC oder Pilot	Quelle: Anwendungen	Ziel: AWS Elastic Beanstalk
R-Typ: Replatform	Arbeitslast: Microsoft	Technologien: Migration; Web- und mobile Apps

Übersicht

Dieses Muster beschreibt, wie eine auf Microsoft Azure App Service gehostete .NET-Webanwendung zu AWS Elastic Beanstalk migriert wird. Es gibt zwei Möglichkeiten, Anwendungen zu Elastic Beanstalk zu migrieren:

- Verwenden Sie AWS Toolkit for Visual Studio — Dieses Plugin für die Microsoft Visual Studio IDE bietet die einfachste und unkomplizierteste Möglichkeit, benutzerdefinierte.NET-Anwendungen in AWS bereitzustellen. Sie können diesen Ansatz verwenden, um .NET-Code direkt in AWS bereitzustellen und unterstützende Ressourcen wie Amazon Relational Database Service (Amazon RDS) für SQL Server-Datenbanken direkt aus Visual Studio zu erstellen.
- Upload und Bereitstellung auf Elastic Beanstalk — Jeder Azure App Service umfasst einen Hintergrunddienst namens Kudu, der für die Erfassung von Speicherabbildern und Bereitstellungsprotokollen, die Anzeige von Konfigurationsparametern und den Zugriff auf Bereitstellungspakete nützlich ist. Sie können die Kudu-Konsole verwenden, um auf Azure App Service-Inhalte zuzugreifen, das Bereitstellungspaket zu extrahieren und das Paket dann mithilfe der Upload- und Bereitstellungsoption in der Elastic Beanstalk-Konsole auf Elastic Beanstalk hochzuladen.

Dieses Muster beschreibt den zweiten Ansatz (Hochladen Ihrer Anwendung über Kudu auf Elastic Beanstalk). Das Muster verwendet auch die folgenden AWS-Services: AWS Elastic Beanstalk, Amazon Virtual Private Cloud (Amazon VPC), Amazon CloudWatch, Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling, Amazon Simple Storage Service (Amazon S3) und Amazon Route 53

Die.NET-Webanwendung wird auf AWS Elastic Beanstalk bereitgestellt, das in einer Amazon EC2 Auto Scaling Group ausgeführt wird. Sie können eine Skalierungsrichtlinie einrichten, die auf

CloudWatch Amazon-Metriken wie der CPU-Auslastung basiert. Für eine Datenbank können Sie je nach Anwendung und Geschäftsanforderungen Amazon RDS in einer Multi-AZ-Umgebung oder Amazon DynamoDB verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine .NET-Webanwendung, die in Azure App Service ausgeführt wird
- Erlaubnis zur Verwendung der Azure App Service Kudu-Konsole

Produktversionen

- .NET Core (x64) 1.0.1, 2.0.0 oder höher oder.NET Framework 4.x, 3.5 (siehe Plattformhistorie von.NET auf Windows Server)
- Internetinformationsdienste (IIS) Version 8.0 oder höher, ausgeführt auf Windows Server 2012 oder höher
- .NET 2.0 oder 4.0 Runtime.

Architektur

Quelltechnologie-Stack

- Anwendung, die mit.NET Framework 3.5 oder höher oder .NET Core 1.0.1, 2.0.0 oder höher entwickelt und auf Azure App Service (Web-App oder API-App) gehostet wird

Zieltechnologie-Stack

- AWS Elastic Beanstalk wird in einer Amazon EC2 Auto Scaling Scaling-Gruppe ausgeführt

Migrationsarchitektur

Arbeitsablauf bei der Bereitstellung

Tools

Tools

- .NET Core oder.NET Framework
- C#
- IIS
- Kudu-Konsole

AWS-Services und -Funktionen

- AWS Elastic Beanstalk — Elastic Beanstalk ist ein easy-to-use Service für die Bereitstellung und Skalierung von.NET-Webanwendungen. Elastic Beanstalk verwaltet automatisch die Kapazitätsbereitstellung, den Lastausgleich und die auto Skalierung.
- Amazon EC2 Auto Scaling Scaling-Gruppe — Elastic Beanstalk umfasst eine Auto Scaling Scaling-Gruppe, die die Amazon EC2 EC2-Instances in der Umgebung verwaltet. In einer Umgebung mit nur einer Instance stellt die Auto Scaling-Gruppe sicher, dass immer eine Instance ausgeführt wird. In einer Umgebung mit Lastenausgleich können Sie die Gruppe mit einer Reihe von Instances konfigurieren, die ausgeführt werden sollen, und Amazon EC2 Auto Scaling fügt Instances je nach Bedarf hinzu oder entfernt sie, je nach Auslastung.
- Elastic Load Balancing — Wenn Sie Load Balancing in AWS Elastic Beanstalk aktivieren, wird ein Load Balancer erstellt, der den Traffic auf die EC2-Instances in der Umgebung verteilt.
- Amazon CloudWatch — Elastic Beanstalk verwendet Amazon automatisch CloudWatch , um Informationen über Ihre Anwendungs- und Umgebungsressourcen bereitzustellen. Amazon CloudWatch unterstützt Standardmetriken, benutzerdefinierte Metriken und Alarme.
- Amazon Route 53 — Amazon Route 53 ist ein hochverfügbarer und skalierbarer Cloud-Webservice für das Domain Name System (DNS). Sie können Route 53-Aliaseinträge verwenden, um benutzerdefinierte Domainnamen AWS Elastic Beanstalk-Umgebungen zuzuordnen.

Epen

Richten Sie eine VPC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine virtuelle private Cloud (VPC) ein.	Erstellen Sie in Ihrem AWS-Konto eine VPC mit den erforderlichen Informationen.	Systemadministrator
Erstellen Sie Subnetze.	Erstellen Sie zwei oder mehr Subnetze in Ihrer VPC.	Systemadministrator
Erstellen Sie eine Routentab elle.	Erstellen Sie eine Routentab elle, die Ihren Anforderungen entspricht.	Systemadministrator

Elastic Beanstalk einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Azure App Service Kudu-Konsole zu.	Greifen Sie über das Azure-Portal auf Kudu zu, indem Sie zum App Service-D ashboard navigieren und dann Advanced Tools, Go auswählen. Oder Sie können die Azure App Service-URL wie folgt ändern:. `https://<appservicename>.sc m.azurewebsites.net`	App-Entwickler, Systemadm inistrator
Laden Sie das Bereitste llungspaket von Kudu herunter.	Navigieren Sie zu Windows, PowerShell indem Sie die DebugConsoleOption auswählen. Dadurch wird die Kudo-Konsole geöffnet. Gehe	App-Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zum `wwwroot` Ordner und lade ihn herunter. Dadurch wird das Azure App Service-Bereitstellungspaket als ZIP-Datei heruntergeladen. Ein Beispiel finden Sie im Anhang.	
Erstellen Sie ein Paket für Elastic Beanstalk.	Entpacken Sie das Bereitstellungspaket, das Sie von Azure App Service heruntergeladen haben. Erstellen Sie eine JSON-Datei mit dem Namen `aws-windows-deployment-manifest.json` (diese Datei ist nur für.NET Core-Anwendungen erforderlich). Erstellen Sie eine ZIP-Datei, die die Azure App Service-Bereitstellungspaketdatei enthält`aws-windows-deployment-manifest.json` . Ein Beispiel finden Sie im Anhang.	App-Entwickler, Systemadministrator
Erstellen Sie eine neue Elastic Beanstalk Beanstalk-Anwendung.	In der Elastic-Beanstalk-Konsole öffnen. Wählen Sie eine bestehende Anwendung oder erstellen Sie eine neue Anwendung.	App-Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Umgebung.	Wählen Sie im Aktionsmenü der Elastic Beanstalk Beanstalk-Konsole die Option Umgebung erstellen aus. Wählen Sie die Webserver-Umgebung und die .NET/IIS-Plattform aus. Wählen Sie für Anwendungscode Upload aus. Laden Sie die ZIP-Datei hoch, die Sie für Elastic Beanstalk vorbereitet haben, und wählen Sie dann Create Environment.	App-Entwickler, Systemadministrator
Konfigurieren Sie Amazon CloudWatch.	Standardmäßig ist die grundlegende CloudWatch Überwachung aktiviert. Wenn Sie die Konfiguration ändern möchten, wählen Sie im Elastic Beanstalk-Assistenten die veröffentlichte Anwendung und dann Monitoring aus.	Systemadministrator
Stellen Sie sicher, dass sich das Bereitstellungspaket in Amazon S3 befindet.	Wenn die Anwendungsumgebung erstellt wurde, finden Sie das Bereitstellungspaket im S3-Bucket.	App-Entwickler, Systemadministrator
Testen Sie die Anwendung.	Wenn die Umgebung erstellt wurde, verwenden Sie die in der Elastic Beanstalk Beanstalk-Konsole angegebene URL, um die Anwendung zu testen.	Systemadministrator

Zugehörige Ressourcen

- Konzepte von AWS Elastic Beanstack (Elastic Beanstalk Beanstalk-Dokumentation)
- Erste Schritte mit.NET auf Elastic Beanstalk (Elastic Beanstalk Beanstalk-Dokumentation)
- Kudu-Konsole () GitHub
- Verwendung von „Kudu“ zur Verwaltung von Azure Web Apps (GS Lab-Artikel)
- Benutzerdefinierte ASP.NET Core Elastic Beanstalk Beanstalk-Bereitstellungen (AWS Toolkit for Visual Studio Studio-Benutzerhandbuch)
- Dokumentation zu Elastic Load Balancing
- Von AWS Elastic Beanstalk unterstützte Plattformen (Elastic Beanstalk Beanstalk-Dokumentation)
- Bereitstellen einer Webanwendung in AWS (C# Corner-Artikel)
- Skalieren der Größe Ihrer Auto Scaling Scaling-Gruppe (Amazon EC2 EC2-Dokumentation)
- Hochverfügbarkeit (Multi-AZ) für Amazon RDS (Amazon RDS-Dokumentation)

Zusätzliche Informationen

Hinweise

- Wenn Sie eine lokale Datenbank oder eine Azure SQL Server-Datenbank zu Amazon RDS migrieren, müssen Sie auch die Datenbankverbindungsdetails aktualisieren.
- Zu Testzwecken ist eine Beispiel-Demoanwendung beigefügt.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas in der AWS-Cloud

Quelle: MongoDB	Ziel: MongoDB Atlas auf AWS	R-Typ: Replatform
Umgebung: Produktion	Technologien: Migration; Analytik; Datenbanken	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon EC2; Amazon VPC		

Übersicht

Dieses Muster beschreibt die Schritte für die Migration von einer selbstverwalteten MongoDB-Umgebung (einschließlich MongoDB Community Server, Enterprise Server, Enterprise Advanced, mLab oder einem beliebigen verwalteten MongoDB-Cluster) zu MongoDB Atlas in der Amazon Web Services (AWS) -Cloud. Es verwendet den Atlas Live Migration Service, um die Datenmigration von MongoDB zu MongoDB Atlas zu beschleunigen.

Das Muster ist dem Leitfaden Migration von MongoDB zu MongoDB Atlas in der AWS-Cloud auf der AWS Prescriptive Guidance-Website beigefügt. Es enthält die Implementierungsschritte für die Migration.

Das Muster ist für AWS Service Integrator-Partner (SI-Partner) und AWS-Benutzer vorgesehen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine MongoDB-Quellumgebung für die Migration zu MongoDB Atlas

Fachwissen

- Dieses Muster erfordert Vertrautheit mit MongoDB-, MongoDB Atlas- und AWS-Services. Weitere Informationen finden Sie unter Rollen und Verantwortlichkeiten im Leitfaden Migration von MongoDB zu MongoDB Atlas in der AWS-Cloud auf der AWS Prescriptive Guidance-Website.

Produktversionen

- MongoDB Version 2.6 oder höher

Architektur

Informationen zu MongoDB Atlas-Referenzarchitekturen, die verschiedene Nutzungsszenarien unterstützen, finden Sie unter MongoDB Atlas-Referenzarchitekturen auf AWS im Leitfaden Migration von MongoDB zu MongoDB Atlas in der AWS-Cloud auf der AWS Prescriptive Guidance-Website.

Tools

- Atlas Live Migration Service — Ein kostenloses MongoDB-Hilfsprogramm, das bei der Migration von Datenbanken zu Atlas hilft. Dieser Dienst hält die Quelldatenbank bis zur Umstellung mit der Zieldatenbank synchron. Wenn Sie bereit sind, die Übertragung vorzunehmen, beenden Sie Ihre Anwendungsinstanzen, verweisen sie auf den Atlas-Ziel-Cluster und starten sie neu.

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Clustergröße.	Schätzen Sie die Größe des Arbeitssets, indem Sie die Informationen aus db.stats () für den gesamten Indexraum verwenden. Gehen Sie davon aus, dass auf einen Prozentsatz Ihres Datenspeichers häufig zugegriffen wird. Oder Sie können Ihren Speicherbedarf auf der Grundlage Ihrer eigenen Annahmen abschätzen. Diese Aufgabe sollte ungefähr eine Woche dauern. Weitere Informationen und Beispiele für diese	MongoDB DBA, Anwendungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und die anderen Geschicht en in diesem Epos finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie die Anforderungen an die Netzwerkbandbreite.	Um Ihre Netzwerkbandbreitenanforderungen zu schätzen, multiplizieren Sie die durchschnittliche Dokumentengröße mit der Anzahl der pro Sekunde bereitgestellten Dokumente. Berücksichtigen Sie den maximalen Datenverkehr, den jeder Knoten in Ihrem Cluster als Grundlage tragen kann. Um die Downstream-Datenübertragungsraten von Ihrem Cluster zu den Client-Anwendungen zu berechnen, verwenden Sie die Summe aller Dokumente, die über einen bestimmten Zeitraum zurückgegeben wurden. Wenn Ihre Anwendungen von sekundären Knoten lesen, teilen Sie diese Gesamtzahl der Dokumente durch die Anzahl der Knoten, die Lesevorgänge ausführen können. Verwenden Sie db.stats (), um die durchschnittliche Dokumentgröße für eine Datenbank zu ermitteln. avgObjSize Befehl. Diese Aufgabe dauert in der Regel einen Tag.	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Atlas-Stufe aus.	Folgen Sie den Anweisungen in der MongoDB-Dokumentation, um die richtige Atlas-Clusterstufe auszuwählen.	MongoDB DBA
Planen Sie die Umstellung der Anwendung ein.		MongoDB DBA, Anwendungsarchitekt

Richten Sie eine neue MongoDB Atlas-Umgebung auf AWS ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen neuen MongoDB Atlas-Cluster auf AWS.	Wählen Sie in MongoDB Atlas „Build a Cluster“, um das Dialogfeld „Create New Cluster“ anzuzeigen. Wählen Sie AWS als Cloud-Anbieter aus.	MongoDB DBA
Wählen Sie Regionen und globale Clusterkonfiguration aus.	Wählen Sie aus der Liste der verfügbaren AWS-Regionen für Ihren Atlas-Cluster aus. Konfigurieren Sie bei Bedarf globale Cluster.	MongoDB DBA
Wählen Sie die Clusterebene aus.	Wählen Sie Ihre bevorzugte Clusterstufe aus. Ihre Tierauswahl bestimmt Faktoren wie Arbeitsspeicher, Speicher und IOPS-Spezifikation.	MongoDB DBA
Konfigurieren Sie zusätzliche Cluster-Einstellungen.	Konfigurieren Sie zusätzliche Clustereinstellungen wie MongoDB-Version, Sicherung	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	s- und Verschlüsselungsop tionen. Weitere Informationen zu diesen Optionen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	

Konfigurieren Sie Sicherheit und Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Zugriffsl iste.	Um eine Verbindung zum Atlas-Cluster herzustellen, müssen Sie der Zugriffsliste des Projekts einen Eintrag hinzufügen. Atlas verwendet Transport Layer Security (TLS)/Secure Sockets Layer (SSL), um die Verbindun gen zur Virtual Private Cloud (VPC) für Ihre Datenbank zu verschlüsseln. Um die Zugriffsl iste für das Projekt einzurich ten und weitere Informationen zu den Geschichten in diesem Epos zu erhalten, klicken Sie auf die Links im Abschnitt „Verwandte Ressourcen“.	MongoDB DBA
Authentifizieren und autorisie ren Sie Benutzer.	Sie müssen die Datenbank benutzer, die auf die MongoDB Atlas-Cluster zugreifen, erstellen und authentifizieren. Um auf Cluster in einem Projekt zugreifen zu können,	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	müssen Benutzer zu diesem Projekt gehören, und sie können mehreren Projekten angehören.	
Erstellen Sie benutzerdefinierte Rollen.	(Optional) Atlas unterstützt die Erstellung benutzerdefinierter Rollen in Fällen, in denen die integrierten Atlas-Datenbank-Benutzerrechte Ihre gewünschten Rechte nicht abdecken.	MongoDB DBA
Richten Sie VPC-Peering ein.	(Optional) Atlas unterstützt VPC-Peering mit anderen AWS-, Azure- oder Google Cloud Platform (GCP) -VPCs.	MongoDB DBA
Richten Sie einen PrivateLink AWS-Endpunkt ein.	(Optional) Sie können private Endpunkte auf AWS mithilfe von AWS einrichten. PrivateLink	MongoDB DBA
Aktivieren Sie die Zwei-Faktor-Authentifizierung.	(Optional) Atlas unterstützt die Zwei-Faktor-Authentifizierung (2FA), damit Benutzer den Zugriff auf ihre Atlas-Konten kontrollieren können.	MongoDB DBA
Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein.	(Optional) Atlas unterstützt die Benutzerauthentifizierung und -autorisierung mit dem Lightweight Directory Access Protocol (LDAP).	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen einheitlichen AWS-Zugriff ein.	(Optional) Einige Atlas-Funktionen, darunter Atlas Data Lake und Verschlüsselung im Ruhezustand mithilfe der Kundenschlüsselverwaltung, verwenden AWS Identity and Access Management (AWS IAM) -Rollen für die Authentifizierung.	MongoDB DBA
Richten Sie die Verschlüsselung im Ruhezustand mit AWS KMS ein.	(Optional) Atlas unterstützt die Verwendung des AWS Key Management System (AWS KMS) zur Verschlüsselung von Speicher-Engines und Backups von Cloud-Anbietern.	MongoDB DBA
Richten Sie die clientseitige Verschlüsselung auf Feldebene ein.	(Optional) Atlas unterstützt die clientseitige Verschlüsselung auf Feldebene, einschließlich der automatischen Verschlüsselung von Feldern.	MongoDB DBA

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Ihren Zielreplikatsatz in MongoDB Atlas.	Starten Sie Ihren Zielreplikatsatz in MongoDB Atlas. Wählen Sie im Atlas Live Migration Service „Ich bin bereit für die Migration“.	MongoDB DBA
Fügen Sie den Atlas Live Migration Service zur Zugriffsl	Dies hilft, die Quellumgebung für die Verbindung mit dem	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
iste in Ihrem AWS-Quellcluster hinzu.	Atlas-Ziel-Cluster vorzubere iten.	
Bestätigen Sie Ihre AWS-Anmeldeinformationen mit dem Atlas Live Migration Service.	Wählen Sie „Migration starten“. Wenn die Schaltflä che „Prepare to Cutover“ grün wird, führen Sie die Umstellun g durch. Überprüfen Sie die Leistungskennzahlen des Atlas-Clusters.	MongoDB DBA

Konfigurieren Sie die betriebliche Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zum MongoDB Atlas-Cluster her.		Entwickler der Anwendung
Interagieren Sie mit Clusterda ten.		Entwickler von Anwendungen
Überwachen Sie Ihre Cluster.		MongoDB DBA
Clusterdaten sichern und wiederherstellen.		MongoDB DBA

Zugehörige Ressourcen

Leitfaden zur Migration

- Migration von MongoDB zu MongoDB Atlas in der AWS-Cloud

Entdeckung und Bewertung

- Arbeitsspeicher

- Beispiel zur Größenbestimmung mit Atlas-Beispieldatensätzen
- Beispiel zur Größenbestimmung für mobile Anwendungen
- Netzwerkverkehr
- Automatische Cluster-Skalierung
- Vorlage für die Größenbestimmung von Atlas

Konfiguration von Sicherheit und Compliance

- Einträge in der IP-Zugriffsliste konfigurieren
- Datenbankbenutzer konfigurieren
- Atlas-Benutzerzugriff
- Konfigurieren Sie benutzerdefinierte Rollen
- Rechte für Datenbankbenutzer
- Richten Sie eine Netzwerk-Peering-Verbindung ein
- Richten Sie einen privaten Endpunkt ein
- Zwei-Faktor-Authentifizierung
- Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein
- Atlas Data Lake
- Verschlüsselung im Ruhezustand mithilfe von Customer Key Management
- Verwenden von IAM-Rollen
- Clientseitige Verschlüsselung auf Feldebene
- Automatische clientseitige Verschlüsselung auf Feldebene
- MongoDB Atlas-Sicherheit
- MongoDB-Vertrauenszentrum
- Sicherheitsfunktionen und Einrichtung

Einrichtung einer neuen MongoDB Atlas-Umgebung auf AWS

- Cloud-Anbieter und Regionen
- Globale Cluster
- Cluster-Ebene
- Zusätzliche Cluster-Einstellungen

- Fangen Sie mit Atlas an
- Atlas-Benutzerzugriff
- Cluster

Daten migrieren

- Überwachen Sie Ihren Cluster

Integrieren von Abläufen

- Mit einem Cluster verbinden
- Führen Sie CRUD-Operationen in Atlas durch
- Überwachen Sie Ihren Cluster
- Clusterdaten Backup und wiederherstellen

Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS

R-Typ: Replatform	Quelle: Containers	Ziel: Apache Tomcat (ToMEE) auf Amazon ECS
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Container und Mikroservices; Migration
Arbeitslast: Oracle	AWS-Dienste: Amazon ECS	

Übersicht

In diesem Muster werden die Schritte für die Migration eines lokalen Oracle Solaris SPARC-Systems, auf dem Oracle ausgeführt wird, WebLogic zu einer Docker-Container-basierten Installation beschrieben, auf der Apache TomEE (Apache Tomcat mit zusätzlicher Container-Unterstützung) mit Amazon Elastic Container Service (Amazon ECS) ausgeführt wird.

Informationen zur Migration von Datenbanken, die mit den Anwendungen verknüpft sind, die Sie von Oracle WebLogic zu Tomcat migrieren, finden Sie in den Datenbankmigrationsmustern in diesem Katalog.

Bewährte Methoden

Die Schritte für die Migration von Java- und Java Enterprise Edition (Java EE) -Webanwendungen variieren je nach der Anzahl der containerspezifischen Ressourcen, die von der Anwendung verwendet werden. Spring-basierte Anwendungen sind in der Regel einfacher zu migrieren, da sie eine geringe Anzahl von Abhängigkeiten vom Bereitstellungscontainer aufweisen. Im Gegensatz dazu erfordern Java EE-Anwendungen, die Enterprise- JavaBeans (EJBs) und verwaltete Container-Ressourcen wie Thread-Pools, Java Authentication and Authorization Service (JAAS) und Container-Managed Persistence (CMP) verwenden, mehr Aufwand.

Anwendungen, die für Oracle Application Server entwickelt wurden, verwenden häufig die Oracle Identity Management Suite. Kunden, die auf Open-Source-Anwendungsserver migrieren, entscheiden sich häufig dafür, Identitäts- und Zugriffsmanagement mithilfe eines SAML-basierten Verbunds neu zu implementieren. Andere verwenden Oracle HTTP Server Webgate für Fälle, in denen eine Migration von der Oracle Identity Management Suite keine Option ist.

Java- und Java EE-Webanwendungen eignen sich hervorragend für die Bereitstellung auf Docker-basierten AWS-Services wie AWS Fargate und Amazon ECS. Kunden entscheiden sich häufig für ein Docker-Image, auf dem die neueste Version des Zielanwendungsservers (z. B. TomEE) und das Java Development Kit (JDK) vorinstalliert sind. Sie installieren ihre Anwendungen auf dem Basis-Decker-Image, veröffentlichen es in ihrer Amazon Elastic Container Registry (Amazon ECR) -Registrierung und verwenden es für die skalierbare Bereitstellung ihrer Anwendungen auf AWS Fargate oder Amazon ECS.

Im Idealfall ist die Anwendungsbereitstellung elastisch, d. h. die Anzahl der Anwendungsinstanzen skaliert je nach Traffic oder Arbeitslast nach oben oder unten. Das bedeutet, dass Anwendungsinstanzen online gehen oder beendet werden müssen, um die Kapazität an den Bedarf anzupassen.

Wenn Sie eine Java-Anwendung nach AWS verschieben, sollten Sie erwägen, sie zustandslos zu machen. Dies ist ein zentrales Architekturprinzip des AWS Well-Architected Framework, das eine horizontale Skalierung mithilfe von Containerisierung ermöglicht. Beispielsweise speichern die meisten Java-basierten Webanwendungen Benutzersitzungsinformationen lokal. Um die Beendigung der Anwendungsinstanz aufgrund der automatischen Skalierung in Amazon Elastic Compute Cloud (Amazon EC2) oder aus anderen Gründen zu überstehen, sollten Benutzersitzungsinformationen global gespeichert werden, sodass Benutzer von Webanwendungen weiterhin nahtlos und transparent arbeiten können, ohne sich erneut mit einer Webanwendung verbinden oder erneut anmelden zu müssen. Für diesen Ansatz gibt es mehrere Architekturoptionen, darunter Amazon ElastiCache for Redis oder das Speichern des Sitzungsstatus in einer globalen Datenbank. Anwendungsserver wie TomEE verfügen über Plug-ins, die die Speicherung und Verwaltung von Sitzungen über Redis, Datenbanken und andere globale Datenspeicher ermöglichen.

Verwenden Sie ein gemeinsames, zentralisiertes Protokollierungs- und Debugging-Tool, das sich leicht in Amazon CloudWatch und AWS X-Ray integrieren lässt. Die Migration bietet die Möglichkeit, die Funktionen des Anwendungslebenszyklus zu verbessern. Möglicherweise möchten Sie den Erstellungsprozess automatisieren, sodass Änderungen mithilfe einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) problemlos vorgenommen werden können. Dies kann Änderungen an der Anwendung erfordern, sodass sie ohne Ausfallzeiten bereitgestellt werden kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java-Quellcode und JDK

- Mit Oracle erstellte Quellanwendung WebLogic
- Definierte Lösung für Identitäts- und Zugriffsmanagement (SAML oder Oracle Webgate)
- Definierte Lösung für die Verwaltung von Anwendungssitzungen (Umzug like-for-like oder mit Amazon oder Zustandslosigkeit der Anwendung ElastiCache, falls erforderlich)
- Erläuterung, ob das Team J2EE-spezifische Bibliotheken umgestalten muss, um die Portabilität auf Apache ToMEE zu gewährleisten (siehe Status der Implementierung von Java EE 7 auf der Apache-Website)
- Gehärtetes ToMEE-Image auf der Grundlage Ihrer Sicherheitsanforderungen
- Container-Image mit vorinstalliertem Ziel-TomEE
- Vereinbarte und bei Bedarf durchgeführte Anwendungskorrektur (z. B. Protokollierung, Debug-Erstellung, Authentifizierung)

Versionen der Produkte

- Oracle WebLogic OC4J, 9i, 10g
- Tomcat 7 (mit Java 1.6 oder höher)

Architektur

Quelltechnologie-Stack

- Mit Oracle erstellte Webanwendung WebLogic
- Webanwendung, die Oracle Webgate oder SAML-Authentifizierung verwendet
- Webanwendungen, die mit Oracle Database Version 10g und höher verbunden sind

Zieltechnologie-Stack

- ToMee (Apache Tomcat mit zusätzlicher Container-Unterstützung) läuft auf Amazon ECS (siehe auch Bereitstellen von Java-Webanwendungen und Java-Microservices auf Amazon ECS)
- Amazon Relational Database Service (Amazon RDS) für Oracle; Informationen zu Oracle-Versionen, die von Amazon RDS unterstützt werden, finden Sie unter Amazon RDS for Oracle

Zielarchitektur

Tools

Um mit TomEE arbeiten zu können, muss eine Java-Anwendung in eine WAR-Datei neu erstellt werden. In einigen Fällen können Änderungen an der Anwendung erforderlich sein, um die Anwendung auf ToMEE ausführen zu können. Sie sollten überprüfen, ob die erforderlichen Konfigurationsoptionen und Umgebungseigenschaften korrekt definiert sind.

Außerdem sollten JNDI-Lookups (Java Naming and Directory Interface) und JSP-Namespaces (JavaServer Pages) korrekt definiert sein. Erwägen Sie, die von der Anwendung verwendeten Dateinamen zu überprüfen, um Namenskonflikte mit integrierten T-Bibliotheken zu vermeiden. Zum Beispiel ist persistence.xml ein Dateiname, der vom Apache OpenJPA-Framework (das mit OpenEJB in TomEE gebündelt ist) für Konfigurationszwecke verwendet wird. Die Datei persistence.xml in PUI enthält Bean-Deklarationen für das Spring Framework.

ToMee Version 7.0.3 und höher (Tomcat 8.5.7 und höher) gibt eine HTTP 400-Antwort (schlechte Anfrage) für rohe (unkodierte) URLs mit Sonderzeichen zurück. Die Serverantwort wird dem Endbenutzer als leere Seite angezeigt. Frühere Versionen von ToMee und Tomcat erlaubten die Verwendung bestimmter unverschlüsselter Sonderzeichen in URLs. Dies gilt jedoch als unsicher, wie auf der Website CVE-2016-6816 angegeben. Um das Problem mit der URL-Kodierung zu lösen, JavaScript müssen die direkt an den Browser übergebenen URLs mit der Methode encodeURI () codiert werden, anstatt als Rohzeichenfolgen verwendet zu werden.

Nachdem Sie die .war-Datei in ToMEE bereitgestellt haben, überprüfen Sie das Startprotokoll von Linux Cat auf fehlende gemeinsam genutzte Bibliotheken und Oracle-spezifische Erweiterungen, um fehlende Komponenten aus Tomcat-Bibliotheken hinzuzufügen.

Allgemeines Verfahren

- Konfigurieren Sie die Anwendung auf TomEE.
- Identifizieren und rekonfigurieren Sie anwendungsserverspezifische Konfigurationsdateien und Ressourcen vom Quell- bis zum Zielformat.
- Identifizieren und rekonfigurieren Sie JNDI-Ressourcen.
- Passen Sie den EJB-Namespace und die Lookups an das vom Zielanwendungsserver benötigte Format an (falls zutreffend).
- Konfigurieren Sie containerspezifische Sicherheitsrollen und Prinzipalzuordnungen für JAAS-Anwendungen neu (falls zutreffend).

- Package Sie die Anwendung und die gemeinsam genutzten Bibliotheken in eine WAR-Datei.
- Stellen Sie die .war-Datei in TomEE mithilfe des bereitgestellten Docker-Containers bereit.
- Überwachen Sie das Startprotokoll, um alle fehlenden Erweiterungen für gemeinsam genutzte Bibliotheken und Bereitstellungsdeskriptoren zu identifizieren. Wenn welche gefunden wurden, kehren Sie zur ersten Aufgabe zurück.
- Testen Sie die installierte Anwendung anhand der wiederhergestellten Amazon RDS-Datenbank.
- Starten Sie die komplette Architektur mit einem Load Balancer und einem Amazon ECS-Cluster, indem Sie den Anweisungen unter Deploy Docker Containers folgen.
- Aktualisieren Sie die URLs so, dass sie auf den Load Balancer verweisen.
- Aktualisieren Sie die Configuration Management Database (CMDB).

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie eine Anwendung serkennung durch (aktueller Status und Leistungsbasis).		BA, Leiter der Migration
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Validieren Sie das Design der Quell- und Zielanwendung (Identitäts- und Sitzungsm anagement).		DBA, Migrationsingenieur, App-Besitzer
Identifizieren Sie die Hardware- und Speichera nforderungen für die Zielserve rinstanz.		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp auf der Grundlage		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie die Strategie und die Tools für die Anwendungsmigration.		DBA, Leiter der Migration
Füllen Sie das Migration sdesign und den Migration sleitfaden für die Anwendung aus.		Leitung aufbauen, Leitung Migration
Füllen Sie das Runbook zur Anwendungsmigration aus.		Leiter Aufbau, Leiter der Umstellung, Leiter des Tests, Leiter der Migration

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		SysAdmin
Erstellen Sie Sicherhei tsgruppen.		SysAdmin
Konfigurieren und starten Sie die Amazon RDS-DB-In stance.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Amazon ECS-Bereitstellung.		SysAdmin
Package Sie Ihre Anwendung als Docker-Image.		SysAdmin
Übertragen Sie das Image in die Amazon ECR-Regis trierung (oder übersprin gen Sie diesen Schritt und übertragen Sie es in den Amazon ECS-Cluster).		SysAdmin
Konfigurieren Sie die Aufgabendefinition für die Anwendung und die Amazon ECS-Serviceoptionen.		SysAdmin
Konfigurieren Sie Ihren Cluster, überprüfen Sie die Sicherheitseinstellungen und legen Sie AWS Identity and Access Management (IAM) - Rollen fest.		SysAdmin
Starten Sie Ihr Setup und führen Sie Tests gemäß Ihrem Runbook für die Anwendung smigration aus.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich die Erlaubnis Ihres Sicherheitsteams, Produktionsdaten nach AWS zu verschieben.		DBA, Migrationsingenieur, App-Besitzer
Erstellen Sie Endpunkte und erhalten Sie Zugriff auf diese, um Datenbank-Backupdateien abzurufen.		DBA
Verwenden Sie die native Datenbank-Engine oder Tools von Drittanbietern, um Datenbankobjekte und Daten zu migrieren.		DBA
Führen Sie die erforderlichen Tests im Runbook für die Anwendungsmigration aus, um die erfolgreiche Datenmigration zu bestätigen.		DBA, Migrationsingenieur, App-Besitzer

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Änderungsantrag (CR) für die Migration.		Leitung der Umstellung
Besorgen Sie sich die CR-Genehmigung für die Migration.		Übernahme (Leitung)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration aus dem Runbook zur Anwendung smigration.		DBA, Migrationsingenieur, App-Besitzer
Aktualisieren Sie die Anwendung (falls erforderlich).		DBA, Migrationsingenieur, App-Besitzer
Führen Sie funktionale und nichtfunktionale Tests sowie Datenvalidierungs-, SLA- und Leistungstests durch.		Testleiter, App-Besitzer, App-Nutzer

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lassen Sie sich vom Antrag oder Geschäftsinhaber unterschreiben.		Übernahme (Leitung)
Führen Sie eine Übung mit einem Tabellenthema durch, in der Sie alle Schritte des Cutover-Runbooks durchgehe n.		DBA, Migrationsingenieur, App-Besitzer
Wechseln Sie zu den Anwendungsclients auf die neue Infrastruktur.		DBA, Migrationsingenieur, App-Besitzer

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Migrationsingenieur, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		Leiter der Migration
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Änderungen im Vergleich zu Tools, zu Kosteneinsparungen usw.		Leiter der Migration
Schließen Sie das Projekt ab und geben Sie Feedback.		Leiter der Migration, Inhaber der App

Zugehörige Ressourcen

Referenzen

- Dokumentation zu Apache Tomcat 7.0
- Installationsanleitung für Apache Tomcat 7.0
- Apache Tomcat JNDI-Dokumentation
- Apache TomEE-Dokumentation
- Amazon RDS für Oracle
- Amazon-RDS-Preise
- Oracle und AWS
- Dokumentation zu Oracle auf Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen
- Erste Schritte mit Amazon ECS
- Erste Schritte mit Amazon RDS

Tutorials und Videos

- Bewährte Methoden für den Betrieb von Oracle-Datenbanken auf Amazon RDS (Präsentation re:Invent 2018)

Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle

R-Typ: Replatform	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for Oracle
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: Oracle	AWS-Dienste: Amazon EC2; Amazon RDS	

Übersicht

Dieses Muster beschreibt die Schritte zur Migration einer Oracle-Datenbank auf Amazon Elastic Compute Cloud (Amazon EC2) zu Amazon Relational Database Service (Amazon RDS) für Oracle mithilfe von AWS Database Migration Service (AWS DMS). Das Muster verwendet auch Oracle SQL Developer oder SQL *Plus, um eine Verbindung zu Ihrer Oracle-DB-Instance herzustellen, und beinhaltet eine CloudFormation AWS-Vorlage, die einige der Aufgaben automatisiert.

Durch die Migration zu Amazon RDS for Oracle können Sie sich auf Ihr Geschäft und Ihre Anwendungen konzentrieren, während Amazon RDS sich um Datenbankverwaltungsaufgaben wie die Bereitstellung von Datenbanken, Sicherung und Wiederherstellung, Sicherheitspatches, Versions-Upgrades und Speichermanagement kümmert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Machine Image (AMI) für Oracle Database auf Amazon EC2

Produktversionen

- AWS DMS unterstützt die Oracle-Versionen 11g (Version 11.2.0.3.v1 und höher), 12c und 18c für Amazon RDS-Instance-Datenbanken für die Editionen Enterprise, Standard, Standard One und Standard Two. Aktuelle Informationen zu unterstützten Versionen finden Sie in der AWS-

Dokumentation unter Using an Oracle Database as a Target for AWS DMS. (Die angehängten CloudFormation AWS-Vorlagen verwenden Oracle Version 12c als Quelldatenbank.)

- Oracle SQL Developer 4.0.3

Architektur

Quellarchitektur

- Oracle-Datenbank auf Amazon EC2

Zielarchitektur

- Amazon RDS für Oracle

Migrationsarchitektur

Tools

- AWS DMS — Mit dem AWS Database Migration Service (AWS DMS) können Sie Datenbanken schnell und sicher zu AWS migrieren. Es unterstützt sowohl homogene als auch heterogene Migrationen. Informationen zu den unterstützten Oracle-Datenbankversionen und -Editionen finden Sie in der AWS-Dokumentation unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer Oracle-Datenbank als Ziel für AWS DMS.
- Oracle SQL Developer oder SQL *Plus — Mit diesen Tools können Sie eine Verbindung zur Amazon RDS for Oracle Oracle-DB-Instance herstellen.

Epen

Richten Sie Ihre Zieldatenbank ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS for Oracle Oracle-DB-Instance.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	RDS-Konsole unter https://console.aws.amazon.com/rds/. Erstellen Sie eine Oracle-DB-Instance, indem Sie die entsprechende Engine, Vorlage, Einstellung für Datenbankanmeldedaten, Instance-Typ, Speicher, Multi-AZ-Einstellungen, Virtual Private Cloud (VPC) und Konfiguration, Anmeldeinformationen und zusätzliche Einstellungen für die Oracle-Datenbank auswählen. Anweisungen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“. Oder verwenden Sie die CloudFormation AWS-Vorlage (create_rds.YAML) im Anhang, um die Amazon RDS for Oracle Oracle-DB-Instance zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zu Amazon RDS her und gewähren Sie dem Oracle-Benutzer Rechte.	Ändern Sie die Sicherheitsgruppe, um die entsprechenden Ports für die Verbindung vom lokalen Computer und der AWS DMS-Replikationsinstanz aus zu öffnen. Stellen Sie bei der Konfiguration der Konnektivität sicher, dass die Option „Öffentlich zugänglich“ ausgewählt ist, damit Sie von außerhalb der VPC eine Verbindung zur Datenbank herstellen können. Stellen Sie mit Oracle SQL Developer oder SQL *Plus mithilfe der Anmeldeinformationen eine Connect zu Amazon RDS her, erstellen Sie einen AWS DMS-Benutzer und gewähren Sie dem AWS DMS-Benutzer die erforderlichen Rechte, um die Datenbank zu ändern.	Developer

Konfigurieren Sie die Sicherheitsgruppe der Quell-EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Prüfen Sie, ob die Oracle-Datenbank läuft.	Verwenden Sie Secure Shell (SSH), um eine Verbindung zur EC2-Instance herzustellen, und versuchen Sie, mithilfe von SQL *Plus eine Verbindung zur Oracle-Datenbank herzustellen.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Sicherhei tsgruppe.	Ändern Sie die Sicherhei tsgruppe der EC2-Instance, um die entsprechenden Ports zu öffnen, sodass Sie von Ihrem lokalen Computer und der AWS DMS-Replikationsin stanz aus eine Verbindung herstellen können.	Developer

AWS DMS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Erstellen Sie in AWS DMS eine Replikationsinstanz in derselben VPC wie Ihre Amazon RDS for Oracle DB-Instance. Geben Sie den Namen und die Beschreibung für die Replikationsinstanz an, wählen Sie die Instance-Klasse und die Version der Replication Engine (verwende n Sie die Standardversion), wählen Sie die VPC aus, in der Sie die Amazon RDS-DB-Instance erstellt haben, legen Sie bei Bedarf Multi-AZ-Einstellungen fest, weisen Sie Speicher zu, geben Sie die Availability Zone an und konfigurieren Sie zusätzliche Einstellungen. Alternativ können Sie die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudFormation AWS-Vorlage (dms.YAML) im Anhang verwenden, um diesen Schritt zu implementieren.	
Connect zu den Quell- und Zieldatenbank-Endpunkten her.	Erstellen Sie die Quell- und Zieldatenbankendpunkte, indem Sie die Endpunkt-ID, die Engine, den Server, den Port, die Anmeldeinformationen und zusätzliche Verbindungsattribute angeben. Verwenden Sie für den Quellserver den öffentlichen DNS der EC2-Instance, die die Oracle-Datenbank hostet. Verwenden Sie für den Zielserver den Endpunkt von Amazon RDS for Oracle. Führen Sie einen Test durch, um zu überprüfen, ob die Quell- und Zielverbindungen funktionieren. Alternativ können Sie die CloudFormation AWS-Vorlage (dms.YAML) im Anhang verwenden, um diesen Schritt zu implementieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe.	Erstellen Sie eine AWS DMS-Aufgabe, um Daten vom Quellendpunkt zum Zielendpunkt zu migrieren, um die Replikation zwischen dem Quell- und Zielendpunkt oder beiden einzurichten. Geben Sie bei der Erstellung der AWS DMS-Aufgabe die Replikationsinstanz, den Quellendpunkt, den Zielendpunkt, den Migrationstyp (nur Daten, nur Replikation oder beides), die Tabellenzuordnung und den Filter an. Führen Sie die AWS DMS-Aufgabe aus, überwachen Sie die Aufgabe, überprüfen Sie die Tabellenstatistiken und überprüfen Sie die Protokolle in Amazon CloudWatch. Alternativ können Sie die CloudFormation AWS-Vorlage (dms.YAML) im Anhang verwenden, um diesen Schritt zu implementieren.	DBA

Zugehörige Ressourcen

- Eine Amazon RDS-DB-Instance erstellen
- Eine Verbindung zu einer DB-Instance aufbauen, die mit der Oracle-Datenbank-Engine ausgeführt wird
- AWS DMS-Dokumentation

- Schrittweise Anleitungen zu AWS DMS
- Migration von Oracle-Datenbanken in die AWS-Cloud

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren einer lokalen Oracle-Datenbank zu Amazon OpenSearch Service mit Logstash

Erstellt von Aditya Goteti (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Oracle Database	Ziel: Amazon OpenSearch Service
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon OpenSearch Service		

Übersicht

Dieses Muster beschreibt, wie Daten mithilfe von Logstash von einer On-Premises-Oracle-Datenbank zu Amazon OpenSearch Service verschoben werden. Sie enthält Überlegungen zur Architektur sowie einige erforderliche Fähigkeiten und Empfehlungen. Die Daten können aus einer einzelnen Tabelle oder aus mehreren Tabellen stammen, in denen eine Volltextsuche durchgeführt werden muss.

OpenSearch Der Service kann in einer Virtual Private Cloud (VPC) konfiguriert oder mit IP-basierten Einschränkungen öffentlich platziert werden. Dieses Muster beschreibt ein Szenario, in dem OpenSearch Service innerhalb einer VPC konfiguriert ist. Logstash wird verwendet, um die Daten aus der Oracle-Datenbank zu sammeln, sie im JSON-Format zu analysieren und dann die Daten in den OpenSearch Service zu laden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java 8 (erforderlich für Logstash 6.4.3)
- Konnektivität zwischen den On-Premises-Datenbankservern und Amazon Elastic Compute Cloud (Amazon EC2)-Instances in einer VPC, die mit AWS Virtual Private Network (AWS VPN) hergestellt wurden

- Eine Abfrage zum Abrufen der erforderlichen Daten, die aus der Datenbank an den OpenSearch Service übertragen werden sollen
- Oracle Java Database Connectivity (JDBC)-Treiber

Einschränkungen

- Logstash kann keine Datensätze identifizieren, die aus der Datenbank fest gelöscht wurden

Produktversionen

- Oracle Datenbank 12c
- OpenSearch Service 6.3
- Logstash 6.4.3

Architektur

Quelltechnologie-Stack

- On-Premises Oracle-Datenbank
- On-Premises-AWS VPN

Zieltechnologie-Stack

- VPC
- EC2-Instance
- OpenSearch Service
- Logstash
- NAT Gateway (für Betriebssystem-Updates auf EC2-Instances und zur Installation von Java 8-, Logstash- und Plugins)

Datenmigrationsarchitektur

Tools

- Logstash 6.4.3
- JDBC-Eingabe-Plugin (Download und weitere Informationen)
- Logstash-Ausgabe-Plugin (logstash-output-amazon_es)
- Oracle-JDBC-Treiber

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Größe der Quelldaten.	Die Größe der Quelldaten ist einer der Parameter, mit denen Sie die Anzahl der Shards bestimmen, die in einem Index konfiguriert werden sollen.	DBA, Datenbankentwickler
Analysieren Sie die Datentypen jeder Spalte und die entsprechenden Daten.	OpenSearch Der Service ordnet den Datentyp dynamisch zu, wenn im Dokument ein zuvor unerkanntes Feld gefunden wird. Wenn es bestimmte Datentypen oder Formate (z. B. Datumsfelder) gibt, die explizit deklariert werden müssen, identifizieren Sie die Felder und definieren Sie die Zuordnung für diese Felder während der Indexerstellung.	App-Eigentümer, Entwickler, Datenbankentwickler
Stellen Sie fest, ob es Spalten mit Primär- oder eindeutigen Schlüsseln gibt.	Um zu vermeiden, dass Datensätze in Amazon OpenSearch Service während	App-Besitzer, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Updates oder Einfügungen dupliziert werden, müssen Sie die `document_id` Einstellung im Ausgabeabschnitt des `amazon_es` Plugins konfigurieren (z. B. `document_id => "%{customer_id}"` wobei ein Primärschlüssel `customer_id` ist).	
Analysieren Sie die Anzahl und Häufigkeit der hinzugefügten Datensätze. Überprüfen Sie, wie oft die Datensätze gelöscht werden.	Diese Aufgabe ist erforderlich, um die Wachstumsrate der Quelldaten zu verstehen. Wenn Daten intensiv gelesen werden und Einfügungen selten sind, können Sie einen einzigen Index haben. Wenn neue Datensätze häufig eingefügt werden und es keine Löschungen gibt, kann die Shard-Größe die empfohlene maximale Größe von 50 GB leicht überschreiten. In diesem Fall können Sie einen Index dynamisch erstellen, indem Sie Indexmuster in Logstash und in dem Code konfigurieren, in dem Sie mithilfe eines Alias darauf zugreifen können.	App-Besitzer, Entwickler
Bestimmen Sie, wie viele Replikate erforderlich sind.		App-Besitzer, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie die Anzahl der Shards, die für den Index konfiguriert werden sollen.		App-Besitzer, Entwickler
Identifizieren Sie die Instance-Typen für dedizierte Hauptknoten, Datenknoten und die EC2-Instance.	Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	App-Besitzer, Entwickler
Bestimmen Sie die Anzahl der benötigten dedizierten Hauptknoten und Datenknoten.	Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten einer EC2-Instance.	Starten Sie eine EC2-Instance innerhalb der VPC, mit der AWS VPN verbunden ist.	Amazon VPC-Konstrukte, AWS VPN
Installieren Sie Logstash auf der EC2-Instance.		Developer
Installieren Sie die Logstash-Plugins.	Installieren Sie die erforderlichen Logstash-Plugins `jdbc-input` und `logstash-output-amazon_es` .	Developer
Konfigurieren Sie Logstash.	Erstellen Sie den Logstash-Keystore, um vertrauliche Informationen wie AWS Secrets Manager-Schlüssel und Datenbankanmeldein	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	formationen zu speichern, und speichern Sie die Referenze n dann in einer Logstash-Konfigurationsdatei.	
Konfigurieren Sie die Warteschlange für unzustell bare Nachrichten und die persistente Warteschlange.	Wenn Logstash auf ein Ereignis stößt, das es nicht verarbeiten kann, weil die Daten einen Zuordnung sfehler oder ein anderes Problem enthalten, hängt die Logstash-Pipeline das erfolglose Ereignis entweder fest oder löscht es. Um sich vor Datenverlust in dieser Situation zu schützen, können Sie Logstash so konfigurieren, dass erfolglose Ereignisse in eine Warteschlange für unzustellbare Nachrichten geschrieben werden, anstatt sie zu löschen. Zum Schutz vor Datenverlust während einer abnormalen Beendigun g verfügt Logstash über eine persistente Warteschl angenfunktion, die die Nachrichtenwarteschlange auf der Festplatte speichert. Persistente Warteschlangen bieten die Datenbeständigkeit in Logstash.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon OpenSearch -Service-Domain.	Erstellen Sie die Amazon OpenSearch -Service-Domäne mit einer Zugriffsrichtlinie, für die keine Anforderungen mit AWS Identity and Access Management (IAM)-Anmeldeinformationen signiert werden müssen. Die Amazon OpenSearch -Service-Domain muss innerhalb derselben VPC erstellt werden. Sie sollten auch die Instance-Typen auswählen und die Anzahl der dedizierten und Master-Knoten basierend auf Ihrer Analyse festlegen.	Developer
Konfigurieren Sie die erforderlichen Amazon OpenSearch -Service-Protokolle.	Weitere Informationen finden Sie in der OpenSearch Service-Dokumentation.	
Erstellen Sie den Index.		Developer
Starten Sie Logstash.	Führen Sie Logstash als Hintergrundservice aus. Logstash führt die konfigurierte SQL-Abfrage aus, ruft die Daten ab, konvertiert sie in das JSON-Format und speist sie in OpenSearch Service. Konfigurieren Sie für den ersten Ladevorgang den Scheduler nicht in der Logstash-Konfigurationsdatei.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie -Dokumente.	Überprüfen Sie die Anzahl der Dokumente im Index und ob alle Dokumente in der Quelldatenbank vorhanden sind. Während des ersten Ladevorgangs werden sie dem Index hinzugefügt und zum Stoppen von Logstash verwendet. Ändern Sie die Logstash-Konfiguration, um einen Scheduler hinzuzufügen, der je nach Client-Anforderung en in einem festen Intervall ausgeführt wird, und starten Sie Logstash neu. Logstash wählt nur die Datensätze aus, die nach der letzten Ausführun g aktualisiert oder hinzugefü gt wurden, und der Zeitstemp el der letzten Ausführung wird in der Datei gespeiche rt, die mit der Eigenschaft `last_run_metadata_ path => “/usr/sha re/logstash/.logst ash_jdbc_last_run”` in der Logstash-Konfigura tionsdatei konfiguriert ist.	Developer

Zugehörige Ressourcen

- Empfohlene CloudWatch Alarme

- Dedizierte Amazon- OpenSearch Service-Master-Knoten
- Dimensionierung von Amazon- OpenSearch Service-Domains
- Logstash-Dokumentation
- JDBC-Eingabe-Plugin
- Logstash-Ausgabe-Plugin
- Amazon OpenSearch -Service-Website

Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle

Erstellt von Baji Shaik (AWS) und Pavan Pusuluri (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for Oracle
R-Typ: Replatform	Arbeitslast: Oracle	Technologien: Migration; Datenbanken
AWS-Dienste: Amazon RDS; AWS DMS		

Übersicht

Dieses Muster beschreibt die Schritte für die Migration von lokalen Oracle-Datenbanken zu Amazon Relational Database Service (Amazon RDS) für Oracle. Im Rahmen des Migrationsprozesses erstellen Sie einen Migrationsplan und berücksichtigen wichtige Faktoren in Bezug auf Ihre Zieldatenbankinfrastruktur auf der Grundlage Ihrer Quelldatenbank. Sie können je nach Ihren Geschäftsanforderungen und Ihrem Anwendungsfall eine von zwei Migrationsoptionen wählen:

1. AWS Database Migration Service (AWS DMS) — Mit AWS DMS können Sie Datenbanken schnell und sicher in die AWS-Cloud migrieren. Ihre Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch die Ausfallzeiten von Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. Sie können die Migrationszeit reduzieren, indem Sie mit AWS DMS eine Aufgabe erstellen, die laufende Änderungen erfasst, nachdem Sie eine erste Volllastmigration über einen Prozess namens Change Data Capture (CDC) abgeschlossen haben. Weitere Informationen finden Sie in der AWS-Dokumentation unter Migrieren von Oracle zu Amazon RDS mit AWS DMS.
2. Systemeigene Oracle-Tools — Sie können Datenbanken mithilfe systemeigener Oracle-Tools wie Oracle und Data Pump Export und Data Pump Import with Oracle GoldenGate for CDC migrieren. Sie können auch native Oracle-Tools wie das ursprüngliche Export-Hilfsprogramm und das ursprüngliche Import-Hilfsprogramm verwenden, um die Vollladezeit zu reduzieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine lokale Oracle-Datenbank
- Eine Amazon RDS-Oracle-Datenbank-Instance (DB)

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Oracle-Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen und Editionen finden Sie in der AWS-Dokumentation unter Amazon RDS for Oracle. Informationen zu Oracle-Versionen, die von AWS DMS unterstützt werden, finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbanken

Zieltechnologie-Stack

- Amazon RDS für Oracle

Quell- und Zielarchitektur

Das folgende Diagramm zeigt, wie eine lokale Oracle-Datenbank mithilfe von AWS DMS zu Amazon RDS for Oracle migriert wird.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen oder verwenden Sie einen vorhandenen Datenbankbenutzer, gewähren Sie diesem Benutzer die erforderlichen AWS DMS-Berechtigungen, aktivieren Sie den ARCHIVELOG-Modus und richten Sie dann die zusätzliche Protokollierung ein.

2. Konfigurieren Sie das Internet-Gateway zwischen dem lokalen Netzwerk und dem AWS-Netzwerk.
3. Konfigurieren Sie Quell- und Zielendpunkte für AWS DMS.
4. Konfigurieren Sie AWS DMS-Replikationsaufgaben, um die Daten von der Quelldatenbank zur Zieldatenbank zu migrieren.
5. Schließen Sie die Aktivitäten nach der Migration in der Zieldatenbank ab.

Das folgende Diagramm zeigt, wie eine lokale Oracle-Datenbank mithilfe nativer Oracle-Tools zu Amazon RDS for Oracle migriert wird.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen oder verwenden Sie einen vorhandenen Datenbankbenutzer und gewähren Sie die erforderlichen Berechtigungen zum Sichern der Oracle-Datenbank mithilfe der Oracle-Dienstprogramme Export (`exp`) und Import (`imp`).
2. Konfigurieren Sie das Internet-Gateway zwischen dem lokalen Netzwerk und dem AWS-Netzwerk.
3. Konfigurieren Sie den Oracle-Client auf dem Bastion-Host so, dass er die Backup-Datenbank verwendet.
4. Laden Sie die Backup-Datenbank in einen Amazon Simple Storage Service (Amazon S3) -Bucket hoch.
5. Stellen Sie die Datenbanksicherung von Amazon S3 in einer Amazon RDS for Oracle Oracle-Datenbank wieder her.
6. Konfigurieren Sie Oracle GoldenGate für CDC.
7. Schließen Sie die Aktivitäten nach der Migration in der Zieldatenbank ab.

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Native Oracle-Tools helfen Ihnen bei der Durchführung einer homogenen Migration. Sie können Oracle Data Pump verwenden, um Daten zwischen Ihren Quell- und Zieldatenbanken zu migrieren. Dieses Muster verwendet Oracle Data Pump, um den vollen Ladevorgang von der Quelldatenbank in die Zieldatenbank durchzuführen.

- Oracle GoldenGate unterstützt Sie bei der logischen Replikation zwischen zwei oder mehr Datenbanken. Dieses Muster wird verwendet GoldenGate , um die Delta-Änderungen nach dem ersten Laden mithilfe von Oracle Data Pump zu replizieren.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Projektdokumente und zeichnen Sie Datenbankdetails auf.	1. Dokumentieren Sie Ihre Migrationsziele, Migrationsanforderungen, wichtige Projektbeteiligte, Projektmeilensteine, Projektfristen, wichtige Kennzahlen, Migrationsrisiken und Pläne zur Risikominderung. 2. Dokumentieren Sie wichtige Informationen über Ihre Quelldatenbank, einschließlich RAM, IOPS und CPUs. Sie werden diese Informationen später verwenden, um die geeignete Ziel-DB-Instance zu ermitteln. 3. Überprüfen Sie die Versionen Ihrer Quell- und Zieldatenbanken.	DBA
Identifizieren Sie die Speicheranforderungen.	Identifizieren und dokumentieren Sie Ihre Speicheranforderungen, einschließlich der folgenden:	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Berechnen Sie den für die Quell-DB-Instance zugewiesenen Speicher. 2. Sammeln Sie die historischen Wachstumskennzahlen aus der Quell-DB-Instance. 3. Forecast Sie das future Wachstum für die Ziel-DB-Instance. Hinweis: Für Allzweck-SSD-Volumes (GP2) erhalten Sie drei IOPS pro 1 GB Speicher. Ordnen Sie Speicherplatz zu, indem Sie die Gesamtzahl der Lese- und Schreib-IOPS in der Quelldatenbank berechnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instanztyp basierend auf den Rechenanforderungen aus.	1. Ermitteln Sie die Rechenanforderungen der Ziel-DB-Instance. 2. Identifizieren Sie Leistungsprobleme. 3. Berücksichtigen Sie die Faktoren bei der Bestimmung des geeigneten Instance-Typs: • CPU-Auslastung der Quell-DB-Instance • IOPS (Lesen und Schreiben) für die Quell-DB-Instance • Speicherbedarf auf der Quell-DB-Instance	SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff.	1. Identifizieren und dokumentieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für Ihre Quell- und Zieldatenbanken. 2. Konfigurieren Sie die entsprechenden Sicherheitsgruppen, damit die Anwendung mit der Datenbank kommunizieren kann.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.	1. Ermitteln und dokumentieren Sie die Strategie zur Umstellung der Migration. 2. Ermitteln und dokumentieren Sie das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für Ihre Anwendung und planen Sie dann die Umstellung entsprechend.	DBA, Besitzer der App SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Migration srisiken.	Beurteilen Sie die Datenbank und dokumentieren Sie migrationsspezifische Risiken und Abhilfemaßnahmen. Beispielsweise: • Identifizieren Sie Tabellen, die keine Protokollierung erfordern, und heben Sie das Risiko eines Datenverlusts im Falle einer Wiederherstellung hervor. • Extrahieren Sie die Benutzer und Rechte der Quelldatenbank und heben Sie die Konflikte mit den Amazon RDS-Rechten hervor. • Überprüfen Sie das Alert-Protokoll auf Oracle-spezifische Fehler und Warnungen. • Identifizieren Sie die unterstützten und nicht unterstützten Funktionen der Ziel-DB-Instance. • Überprüfen Sie die veraltete n Funktionen der Engine der Ziel-DB-Version.	DBA

Konfiguration der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie eine neue Amazon Virtual Private Cloud (Amazon VPC) für die Ziel-DB-Instance.	SysAdmin
Erstellen Sie Sicherheitsgruppen.	Erstellen Sie eine Sicherheitsgruppe in Ihrer neuen VPC, um eingehende Verbindungen zur DB-Instance zuzulassen.	SysAdmin
Erstellen Sie eine Amazon RDS for Oracle Oracle-DB-Instance.	Erstellen Sie die Ziel-DB-Instance mit der neuen VPC und der neuen Sicherheitsgruppe und starten Sie dann die Instance.	SysAdmin

(Option 1) Verwenden Sie native Tools von Oracle oder Drittanbietern, um Daten zu migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbank vor.	1. Erstellen Sie ein Data Pump-Verzeichnis oder verwenden Sie ein vorhandenes. 2. Erstellen Sie einen Migrationsbenutzer und gewähren Sie ihm Berechtigungen zur Durchführung des Data Pump-Extrakts. 3. Extrahieren Sie Rollen, Benutzer und Tablespaces	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus der Quelldatenbank als SQL-Skript. 4. Übertragen Sie den extrahierten Data Pump-Dump in das Ziel-DB-Instance-Verzeichnis. `data pump`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Zieldatenbank vor.	1. Vergewissern Sie sich, dass alle Datenbankoptionen (z. B. Text und Java) auf der Ziel-DB-Instance von Amazon RDS for Oracle installiert oder aktiviert sind. 2. Erstellen Sie ein Data Pump-Verzeichnis oder verwenden Sie ein vorhandenes. 3. Erstellen Sie einen Migrationsbenutzer und gewähren Sie ihm Berechtigungen zur Durchführung des Data Pump-Imports. 4. Erstellen Sie die erforderlichen Tablespaces, Benutzer und Rollen auf der Ziel-DB-Instance. 5. Importieren Sie den übertragenen Data Pump-Export-Dump in die Zieldatenbank. 6. Erstellen Sie alle Indizes, die beim Import oder bei der Objekterstellung ausgeschlossen wurden. 7. Erstellen Sie alle Einschränkungen, die beim Import ausgeschlossen wurden. 8. Validieren oder kompilieren Sie ungültige Objekte neu.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Erstellen Sie die ungültigen Indizes neu. 10. Überprüfen Sie die Anzahl der Datenbankobjekte zwischen der Quell- und der Zieldatenbank. 11. Beheben Sie alle festgestellten Diskrepanzen zwischen der Objektanzahl.	

(Option 2) Verwenden Sie AWS DMS, um Daten zu migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Daten vor.	1. Bereinigen Sie die Daten in der Quelldatenbank. 2. Erstellen Sie eine Replikationsinstanz. 3. Erstellen Sie einen Quellendpunkt und einen Zielendpunkt. 4. Identifizieren Sie die Anzahl der Tabellen und Objekte, die migriert werden sollen.	DBA
Migrieren Sie die Daten.	1. Löschen Sie Fremdschlüsseleinschränkungen und Auslöser in der Zieldatenbank. 2. Löschen Sie sekundäre Indizes in der Zieldatenbank.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Konfigurieren Sie die Einstellungen für AWS DMS-Vollladeaufgaben von der Quelldatenbank zur Zieldatenbank. 4. Aktivieren Sie Fremdschl üssel. 5. Ermöglichen Sie AWS DMS CDC, um laufende Änderungen zu replizieren. 6. Aktivieren Sie Auslöser. 7. Aktualisieren Sie die Sequenzen. 8. Überprüfen Sie die Quell- und Zieldaten.	

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.	1. Stoppen Sie alle Anwendungsdienste und Client-Verbindungen, die auf Oracle verweisen. 2. Führen Sie die AWS DMS-Aufgaben aus. 3. Richten Sie eine Rollback-Aufgabe ein (z. B. CDC von der Amazon RDS-Daten bank in die lokale Oracle-Datenbank rückgängig machen). 4. Validieren Sie die Daten.	DBA SysAdmin, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Starten Sie die Anwendungsdienste in der neuen Zieldatenbank, indem Sie Amazon Route 53 für die neue Amazon RDS for Oracle Oracle-DB-Instance konfigurieren. 6. Fügen Sie Amazon CloudWatch Monitoring zu Ihrer neuen Amazon RDS for Oracle DB-Instance hinzu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie Ihren Rollback-Plan.	1. Beenden Sie alle Anwendungsdienste, die auf die Amazon RDS for Oracle Oracle-DB-Instance verweisen. 2. Führen Sie mithilfe einer AWS DMS-Aufgabe ein Rollback der Änderungen an der lokalen Oracle-Qu elldatenbank durch. 3. Beenden Sie die AWS-DMS-Aufgaben, die von der lokalen Oracle-Datenbank zur Amazon RDS for Oracle Oracle-Datenbank ausgeführt werden. 4. Konfigurieren Sie die Anwendungen wieder in der Oracle-Quelldatenbank. 5. Vergewissern Sie sich, dass die Rollback-Bereitstellung abgeschlossen ist.	DBA, Besitzer der App

Schließen Sie das Migrationsprojekt ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen bereinigen.	Fahren Sie die temporären AWS-Ressourcen herunter oder entfernen Sie sie, z. B. die AWS DMS-Replikationsin stanz und den S3-Bucket.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Projektdokumente.	Überprüfen Sie Ihre Dokumente und Ziele zur Migrationsplanung und stellen Sie dann sicher, dass Sie alle erforderlichen Migrationsschritte abgeschlossen haben.	DBA SysAdmin, Besitzer der App
Sammeln Sie Metriken.	Erfassen Sie wichtige Migrationskennzahlen, wie lange es gedauert hat, bis die Migration abgeschlossen ist, wie viel Prozent manuelle Aufgaben im Vergleich zu toolbasierten Aufgaben haben, Kosteneinsparungen und andere relevante Kennzahlen.	DBA, Besitzer der SysAdmin App
Schließt das Projekt ab.	Schließen Sie das Migrationsprojekt ab und holen Sie sich Feedback zu den Bemühungen.	DBA SysAdmin, Besitzer der App

Zugehörige Ressourcen

Referenzen

- Strategien für die Migration von Oracle-Datenbanken zu AWS (AWS-Whitepaper)
- AWS Database Migration Service (AWS DMS-Dokumentation)
- Amazon RDS-Preise (Amazon RDS-Dokumentation)

Tutorials und Videos

- Erste Schritte mit AWS Database Migration Service (AWS DMS-Dokumentation)

- Amazon RDS-Ressourcen (Amazon RDS-Dokumentation)
- AWS Database Migration Service (DMS) (YouTube)

Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle Data Pump

Erstellt von Mohan Annam (AWS) und Brian Motzer (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS für Oracle
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster beschreibt, wie eine Oracle-Datenbank mithilfe von Oracle Data Pump von einem On-Premises-Rechenzentrum zu einer Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance migriert wird.

Das Muster umfasst das Erstellen einer Datenabbilddatei aus der Quelldatenbank, das Speichern der Datei in einem Amazon Simple Storage Service (Amazon S3)-Bucket und das anschließende Wiederherstellen der Daten in einer DB-Instance von Amazon RDS für Oracle. Dieses Muster ist nützlich, wenn Sie bei der Verwendung von AWS Database Migration Service (AWS DMS) für die Migration auf Einschränkungen stoßen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die erforderlichen Berechtigungen zum Erstellen von Rollen in AWS Identity and Access Management (IAM) und für einen mehrteiligen Amazon S3-Upload
- Die erforderlichen Berechtigungen zum Exportieren von Daten aus der Quelldatenbank
- AWS Command Line Interface (AWS CLI) installiert und konfiguriert

Produktversionen

- Oracle Data Pump ist nur für Oracle Database 10g Release 1 (10.1) und höhere Versionen verfügbar.

Architektur

Quelltechnologie-Stack

- On-Premises-Oracle-Datenbanken

Zieltechnologie-Stack

- Amazon RDS für Oracle
- SQL-Client (Oracle SQL Developer)
- Ein S3-Bucket

Quell- und Zielarchitektur

Tools

AWS-Services

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist. In diesem Muster wird IAM verwendet, um die Rollen und Richtlinien zu erstellen, die für die Migration von Daten von Amazon S3 zu Amazon RDS für Oracle erforderlich sind.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hohen Geschwindigkeiten von einer Datenbank in eine andere verschieben. In diesem Muster wird Oracle Data Pump verwendet, um die Datenabbilddatei (.dmp) auf den Oracle-Server zu exportieren und sie in Amazon RDS für

Oracle zu importieren. Weitere Informationen finden Sie unter Importieren von Daten in Oracle in Amazon RDS in der Amazon-RDS-Dokumentation.

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht. Es interagiert sowohl mit der lokalen Oracle-Datenbank als auch mit Amazon RDS für Oracle, um die SQL-Befehle auszuführen, die für den Export und Import von Daten erforderlich sind.

Polen

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Bucket.	Um den S3-Bucket zu erstellen, folgen Sie den Anweisungen in der AWS-Dokumentation.	AWS-Systemadministrator

Erstellen der IAM-Rolle und Zuweisen von Richtlinien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM-Berechtigungen.	Um Berechtigungen zu konfigurieren, folgen Sie den Anweisungen in der AWS-Dokumentation.	AWS-Systemadministrator

Erstellen Sie die Ziel-DB-Instance von Amazon RDS für Oracle und ordnen Sie die Amazon S3-Integrationsrolle zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Ziel-DB-Instance von Amazon RDS für Oracle.	Um die Amazon RDS for Oracle-Instance zu erstellen, folgen Sie den Anweisungen in der AWS-Dokumentation .	AWS-Systemadministrator
Ordnen Sie die Rolle der DB-Instance zu.	Um die Rolle der Instance zuzuordnen, folgen Sie den Anweisungen in der AWS-Dokumentation .	DBA

Erstellen des Datenbankbenutzers in der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Benutzer.	Stellen Sie von Oracle SQL Developer oder SQL*Plus aus eine Verbindung zur Zieldatenbank von Amazon RDS für Oracle her und führen Sie den folgenden SQL-Befehl aus, um den Benutzer zu erstellen , in den das Schema importiert werden soll.
	`create user SAMPLE_SCHEMA identified by <PASSWORD>;`
	`grant create session, resource to <USER NAME>;`
	`alter user <USER NAME> quota 100M on users;`
		DBA

Erstellen der Exportdatei aus der Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Datenabbildatei.	Verwenden Sie das folgende Skript, um eine Dump-Datei mit dem Namen `sample.dmp` im `DATA_PUMP_DIR` Verzeichnis für den Export des `SAMPLE_SCHEMA` Benutzers zu erstellen.
	`DECLARE`
	`hdnl NUMBER;`
	`BEGIN`
	`hdnl := dbms_datapump.open(operation => 'EXPORT',`
	`job_mode => 'SCHEMA',`
	`job_name => NULL);`
	`dbms_datapump.add_file( handle => hdnl,`
	`filename => 'sample.dmp',`
	`directory => 'DATA_PUMP_DIR',`
	`filetype => dbms_datapump.ku$_file_type_dump_file);`
	`dbms_datapump.add_file(handle => hdnl,`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>filename => 'export.log',
	directory => 'DATA_PUMP_DIR',
	filetype => dbms_datapump.ku$_file_type_log_file);
	dbms_datapump.metadata_filter(hdnl, 'SCHEMA_EXPR', 'IN ('''SAMPLE_SCHEMA''')');
	dbms_datapump.start_job(hdnl);
	END;
	/</pre>
	Überprüfen Sie die Exportdetails, indem Sie die `export.log` Datei in Ihrem lokalen `DATA_PUMP_DIR` Verzeichnis überprüfen.	

Hochladen der Dump-Datei in den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Datenabbildatei aus der Quelle in den S3-Bucket hoch.	Führen Sie mit AWS CLI den folgenden Befehl aus.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws s3 cp sample.dmp s3://<bucket_created_epic_1>/`	

Herunterladen der Exportdatei aus dem S3-Bucket in die RDS-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Herunterladen der Datenabbilddatei zu Amazon RDS	Führen Sie den folgenden SQL-Befehl aus, um die Dump-Datei `sample.dmp` aus dem S3-Bucket in die Datenbank von Amazon RDS für Oracle zu kopieren. In diesem Beispiel wird die `sample.dmp` Datei aus dem S3-Bucket `my-s3-integration1` in das Oracle-Verzeichnis heruntergeladen`DATA_PUMP_DIR` . Stellen Sie sicher, dass Ihrer RDS-Instance genügend Speicherplatz zugewiesen ist, um sowohl die Datenbank als auch die Exportdatei zu berücksichtigen.
	`-- If you want to download all the files in the S3 bucket remove the p_s3_prefix line.`
	
	`SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>p_bucket_name
	=> 'my-s3-in
	tegration',
	p_s3_prefix =>
	'sample.dmp',
	p_directory_name
	=> 'DATA_PUMP_DIR')
	AS TASK_ID FROM DUAL;</pre>
	Der vorherige Befehl gibt eine Aufgaben-ID aus. Führen Sie den folgenden Befehl aus, um den Status des Downloads zu überprüfen, indem Sie die Daten in der Aufgaben-ID überprüfen.
	<pre>SELECT text FROM
	table(rdsadmin.rds
	_file_util.read_te
	xt_file('BDUMP','d
	btask-<task_id>.lo
	g'));</pre>
	Führen Sie den folgenden Befehl aus, um die Dateien im DATA_PUMP_DIR Verzeichnis anzuzeigen.
	<pre>SELECT filename,
	type,filesize/1024
	/1024 size_megs
	,to_char(mtime,'DD
	-MON-YY HH24:MI:SS')
	timestamp
	FROM TABLE(rdsadmin.rds
	_file_util.listdir	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(p_directory => upper('DATA_PUMP_D IR'))) order by 4;	

Importieren der Dump-Datei in die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Schema und die Daten in Amazon RDS wieder her.	Um die Dump-Datei in das `sample_schema` Datenbankschema zu importieren, führen Sie den folgenden SQL-Befehl von SQL Developer oder SQL*Plus aus. DECLARE hdnl NUMBER; BEGIN hdnl := DBMS_DATA PUMP.OPEN(operation => 'IMPORT', job_mode => 'SCHEMA', job_name= >null); DBMS_DATAPUMP.ADD_ FILE(handle => hdnl, filename => 'sample.d mp', directory => 'DATA_PUMP_DIR', filetype => dbms_data pump.ku$_file_type _dump_file); DBMS_DATAPUMP.ADD_FILE (handle => hdnl, filename => 'import.l og', directory =>	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_log_file);`
	
	`DBMS_DATAPUMP.METADATA_FILTER(hdnl,'SCHEMA_EXPR','IN (''SAMPLE_SCHEMA'')');`
	
	`DBMS_DATAPUMP.START_JOB(hdnl);`
	
	`END;`
	`/`
	
	Führen Sie den folgenden Befehl aus, um die Protokolldatei aus dem Import anzuzeigen.
	
	`SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('DATA_PUMP_DIR','import.log'));`	

Entfernen Sie die Dump-Datei aus dem Verzeichnis DATA_PUMP_DIR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Listen Sie die Exportdateien auf und bereinigen Sie sie.	Listen Sie die Exportdateien im `DATA_PUMP_DIR` Verzeichnis auf und entfernen Sie sie. Führen Sie die folgenden Befehle aus.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`-- List the files`
	`SELECT filename,`
	`type,filesize/1024`
	`/1024 size_megs`
	`,to_char(mtime,'DD`
	`-MON-YY HH24:MI:S`
	`S') timestamp FROM`
	` TABLE(rdsadmin.rds`
	`_file_util.listdir`
	`(p_directory =>`
	` upper('DATA_PUMP_D`
	`IR'))) order by 4;`
	
	`-- Remove the files`
	`EXEC UTL_FILE.`
	`FREMOVE('DATA_PUMP`
	`_DIR','sample.dmp');`
	`EXEC UTL_FILE.FREMOVE('`
	`DATA_PUMP_DIR','im`
	`port.log');`	

Zugehörige Ressourcen

- Amazon S3-Integration
- Erstellen einer DB-Instance
- Importieren von Daten in Oracle in Amazon RDS
- Amazon S3-Dokumentation
- IAM-Dokumentation
- Dokumentation zu Amazon RDS
- Oracle Data Pump-Dokumentation
- Oracle SQL Developer

Migrieren von PostgreSQL auf Amazon EC2 zu Amazon RDS für PostgreSQL mit pglogical

Erstellt von Rajesh Madiwale (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Amazon EC2	Ziel: Amazon RDS für PostgreSQL
R-Typ: Plattformwechsel	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster beschreibt die Schritte zur Migration einer PostgreSQL-Datenbank (Version 9.5 und höher) von Amazon Elastic Compute Cloud (Amazon EC2) zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL mithilfe der PostgreSQL-Erweiterung pglogical. Amazon RDS unterstützt jetzt die Erweiterung pglogical für PostgreSQL Version 10.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Wählen Sie den richtigen Typ der Amazon-RDS-Instance aus. Weitere Informationen finden Sie unter Amazon-RDS-Instance-Typen.
- Stellen Sie sicher, dass die Quell- und Zielversionen von PostgreSQL identisch sind.
- Installieren und integrieren Sie die pglogical-Erweiterung in PostgreSQL auf Amazon EC2.

Produktversionen

- PostgreSQL Version 10 und höher auf Amazon RDS mit den in Amazon RDS unterstützten Funktionen (siehe PostgreSQL auf Amazon RDS in der AWS-Dokumentation). Dieses Muster wurde durch die Migration von PostgreSQL 9.5 zu PostgreSQL Version 10 auf Amazon RDS getestet, gilt aber auch für spätere Versionen von PostgreSQL auf Amazon RDS.

Architektur

Datenmigrationsarchitektur

Tools

- pglogical-Erweiterung
- Native PostgreSQL-Dienstprogramme: pg_dump und pg_restore

Polen

Migrieren von Daten mithilfe der Erweiterung pglogical

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS PostgreSQL-DB-Instance.	Richten Sie eine PostgreSQL-DB-Instance in Amazon RDS ein. Anweisungen finden Sie in der Dokumentation zu Amazon RDS für PostgreSQL.	DBA
Rufen Sie einen Schema-Dump aus der PostgreSQL-Quelldatenbank ab und stellen Sie ihn in der PostgreSQL-Zieldatenbank wieder her.	1. Verwenden Sie das Dienstprogramm pg_dump mit der `-s` Option , um eine Schemadatei aus der Quelldatenbank zu generieren. 2. Verwenden Sie das Dienstprogramm psql mit der `-f` Option , um das Schema in die Zieldatenbank zu laden.	DBA
Aktivieren Sie die logische Dekodierung.	Legen Sie in der DB-Parametergruppe von Amazon RDS den `rds.logical_replic`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ation` statischen Parameter auf 1 fest. Anweisungen finden Sie in der Amazon-RDS-Dokumentation.	

Erstellen Sie die Erweiterung pglogical in den Quell- und Zieldatenbanken.	1. Erstellen Sie die `pglogical` Erweiterung in der PostgreSQL-Quelldatenbank:
	`psql -h <amazon-ec2-endpoint> -d target-dbname -U target-dbuser -c "create extension pglogical ;"`
	2. Erstellen Sie die `pglogical` Erweiterung in der PostgreSQL-Zieldatenbank:
	`psql -h <amazon-rds-endpoint> -d source-dbname -U source-dbuser -c "create extension pglogical ;"`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Herausgeber in der PostgreSQL-Quelldatenbank.	Um einen Herausgeber zu erstellen, führen Sie Folgendes aus: `psql -d dbname -p 5432 <<EOF SELECT pglogical .create_node( node_name := 'provider1', dsn := 'host=<ec2-endpoint> port=5432 dbname=source-dbname user=source-dbuser' ); EOF`	DBA
Erstellen Sie einen Replikationssatz und fügen Sie Tabellen und Sequenzen hinzu.	Um einen Replikationssatz in der PostgreSQL-Quelldatenbank zu erstellen und dem Replikationssatz Tabellen und Sequenzen hinzuzufügen, führen Sie aus: `psql -d dbname -p 5432 <<EOF SELECT pglogical .replication_set_add_all_tables('default', '{public}'::text[],synchronize_data := true); EOF`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Abonnenten.	Um einen Abonnenten in der PostgreSQL-Zieldatenbank zu erstellen, führen Sie Folgendes aus: `psql -h <rds-endpoint> -d target-dbname -U target-dbuser <<EOF SELECT pglogical.create_node( node_name := 'subscriber1', dsn := 'host=<rds-endpoint> port=5432 dbname=target-dbname password=postgres user=target-dbuser' ); EOF`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Abonnement.	Um ein Abonnement für die PostgreSQL-Zieldatenbank zu erstellen, führen Sie Folgendes aus: `psql -h <rds-endpoint> -d target -U postgres <<EOF SELECT pglogical.create_subscription( subscription_name := 'subscription1', replication_sets := array['default'], provider_dsn := 'host=<ec2-endpoint> port=5432 dbname=<source-dbname> password=<password> user=source-dbuser' );`	DBA

Validieren Ihrer Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie Quell- und Zieldatenbanken.	Überprüfen Sie die Quell- und Zieldatenbanken, um sicherzustellen, dass die Daten erfolgreich repliziert werden. Sie können eine grundlegende Validierung durchführen, indem Sie `select count(1)` aus den Quell- und Zieltabellen verwenden.	DBA

Zugehörige Ressourcen

- Amazon RDS
- Logische Replikation für PostgreSQL in Amazon RDS (Amazon-RDS-Dokumentation)
- pglogical (GitHub Repository)
- Einschränkungen von pglogical (GitHub Repository-README-Datei)
- Migrieren von PostgreSQL von On-Premises oder Amazon EC2 zu Amazon RDS mithilfe der logischen Replikation (AWS Database Blog)

Migrieren einer On-Premises-PostgreSQL-Datenbank zu Aurora PostgreSQL

Erstellt von Bolji Shaik (AWS) und Jitender Kumar (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises-PostgreSQL-Datenbank	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Plattformwechsel	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora; AWS DMS		

Übersicht

Amazon Aurora PostgreSQL -Compatible Edition kombiniert die Leistung und Verfügbarkeit kommerzieller High-End-Datenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken. Aurora bietet diese Vorteile, indem der Speicher auf drei Availability Zones in derselben AWS-Region skaliert wird, und unterstützt bis zu 15 Lesereplikat-Instances, um Lese-Workloads zu skalieren und eine hohe Verfügbarkeit innerhalb einer einzelnen Region zu gewährleisten. Durch die Verwendung einer globalen Aurora-Datenbank können Sie PostgreSQL-Datenbanken in bis zu fünf Regionen replizieren, um im Falle eines Regionsausfalls Remote-Lesezugriff und Notfallwiederherstellung zu erhalten. Dieses Muster beschreibt die Schritte zum Migrieren einer On-Premises-PostgreSQL-Quelldatenbank zu einer Aurora-PostgreSQL-kompatiblen Datenbank. Das Muster umfasst zwei Migrationsoptionen: die Verwendung von AWS Data Migration Service (AWS DMS) oder der Verwendung nativer PostgreSQL-Tools (z. B.pg_dump ,pg_restore undpsql) oder Tools von Drittanbietern.

Die in diesem Muster beschriebenen Schritte gelten auch für PostgreSQL-Zieldatenbanken auf Amazon Relational Database Service (Amazon RDS)- und Amazon Elastic Compute Cloud (Amazon EC2)-Instances.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine PostgreSQL-Quelldatenbank in einem On-Premises-Rechenzentrum
- Eine mit Aurora PostgreSQL kompatible DB-Instance oder eine DB-Instance von Amazon RDS für PostgreSQL

Einschränkungen

- Die Beschränkungen der Datenbankgröße liegen bei 64 TB für Amazon RDS for PostgreSQL und 128 TB für Aurora PostgreSQL – kompatibel.
- Wenn Sie die AWS DMS-Migrationsoption verwenden, überprüfen Sie die AWS DMS-Einschränkungen für die Verwendung einer PostgreSQL-Datenbank als Quelle.

Produktversionen

- Informationen zur Unterstützung von Haupt- und Nebenversionen von PostgreSQL in Amazon RDS finden Sie unter Updates von Amazon RDS für PostgreSQL in der Amazon-RDS-Dokumentation.
- Informationen zur PostgreSQL-Unterstützung in Aurora finden Sie unter Updates für Amazon Aurora PostgreSQL in der Aurora-Dokumentation.
- Wenn Sie die AWS DMS-Migrationsoption verwenden, finden Sie weitere Informationen unter Unterstützte PostgreSQL-Versionen in der AWS DMS-Dokumentation.

Architektur

Quelltechnologie-Stack

- On-PremisesPostgreSQL-Datenbank

Zieltechnologie-Stack

- Aurora PostgreSQL – Kompatible DB-Instance

Quellarchitektur

Zielarchitektur

Datenmigrationsarchitektur

Verwenden von AWS DMS

Verwenden nativer PostgreSQL-Tools

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und On-Premises-Konfigurationen. Dieser Service unterstützt verschiedene Quellen und Zieldatenbanken. Informationen zum Validieren der PostgreSQL-Quell- und Zieldatenbankversionen und -editionen, die für die Verwendung mit AWS DMS unterstützt werden, finden Sie unter Verwenden einer PostgreSQL-Datenbank als AWS DMS-Quelle. Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden.
- Zu den nativen PostgreSQL-Tools gehörenpg_dump ,pg_restore undpsql .

Polen

Analysieren der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.	Wenn Sie AWS DMS verwenden, stellen Sie sicher, dass Sie eine unterstützte Version von PostgreSQL verwenden.	DBA
Identifizieren Sie den Speichertyp und die Kapazitätsanforderungen.	1. Berechnen Sie den Speicherplatz, der der Quelldatenbank-Instance zugewiesen ist.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erfassen Sie die historischen Wachstumsmetriken für die Quelldatenbank-Instance. 3. Erwarten Sie die zukünftige Wachstumsprognose für die Zieldatenbank-Instance. 4. Weisen Sie Speicher zu, indem Sie die Gesamtzahl der Lese- und Schreib-IOPS in der Quelldatenbank berechnen. Ein Allzweck-SSD-Volume (gp2) stellt 3 IOPS für jede 1 GB Speicher bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instance-Typ, die Kapazität , die Speicherfunktionen und die Netzwerkfunktionen aus.	Bestimmen Sie die Rechenanf orderungen der Zieldaten bank-Instance. Überprüfen Sie bekannte Leistungsprobleme, die möglicherweise zusätzlic he Aufmerksamkeit erfordern . Berücksichtigen Sie die folgenden Faktoren, um den entsprechenden Instance-Typ zu ermitteln: • CPU-Auslastung der Quelldatenbank-Instance • IOPS (Lese- und Schreibvo rgänge) für die Quelldate nbank-Instance • Speicherbedarf auf der Quelldatenbank-Instance Weitere Informationen finden Sie unter Aurora-DB-Instance -Klassen in der Aurora-Do kumentation.	DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	Bestimmen Sie die entsprech enden Sicherheitsgruppen, die es der Anwendung ermöglich en würden, mit der Datenbank zu kommunizieren.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.	• Bestimmen Sie die Strategie für den Migrations-Cutover basierend auf der Komplexität Ihrer Anwendung. • Bestimmen Sie das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für die Anwendung und planen Sie den Cutover entsprechend.	DBA, App-Besitzer, Systemadministrator

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie eine neue Virtual Private Cloud (VPC) für die Zieldatenbank-Instance.	Systemadministrator
Erstellen Sie Sicherheitsgruppen.	Erstellen Sie eine Sicherheitsgruppe innerhalb der VPC (wie im vorherigen Epi festgelegt), um eingehende Verbindungen zur Datenbank-Instance zuzulassen.	Systemadministrator
Konfigurieren und starten Sie den Aurora-DB-Cluster.	Erstellen Sie die Zieldatenbank-Instance mit der neuen VPC und Sicherheitsgruppe und starten Sie die Instance.	Systemadministrator

Migrieren von Daten Option 1 (mit AWS DMS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Schritte vor der Migration aus.	1. Bereinigen Sie die Daten in der Quelldatenbank. 2. Erstellen Sie eine Replikations-Instance. 3. Erstellen Sie Quell- und Zielendpunkte. 4. Identifizieren Sie die Anzahl der verfügbaren Tabellen und Objekte, die migriert werden sollen.	DBA
Führen Sie die Migrationsschritte aus.	1. Löschen Sie Fremdschlüsseleinschränkungen und Auslöser in der Zieldatenbank. 2. Löschen Sie sekundäre Indizes in der Zieldatenbank. 3. Verwenden Sie eine Volllastaufgabe, um Daten von der Quelle zur Zieldatenbank zu migrieren. 4. Aktivieren Sie Fremdschlüssel. 5. Wenn Sie Flash-Cut-Migration verwenden und Ihre Anwendung nur minimale Ausfallzeiten erfordert, aktivieren Sie Change Data Capture (CDC), um laufende Änderungen zu replizieren	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Aktivieren Sie Auslöser. 7. Sequenzen aktualisieren. 8. Validieren Sie die Quell- und Zieldaten.	
Validieren von Daten.	Um sicherzustellen, dass Ihre Daten korrekt von der Quelle zum Ziel migriert wurden, befolgen Sie die Schritte zur Datenvalidierung in der AWS DMS-Dokumentation.	DBA

Migrieren von Daten Option 2 (mit pg_dump und pg_restore)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbank vor.	1. Erstellen Sie ein Verzeichnis zum Speichern der pg_dump-Sicherung, falls sie noch nicht vorhanden ist. 2. Erstellen Sie einen Migrationsbenutzer, der über Berechtigungen zum Ausführen von pg_dump für Datenbankobjekte verfügt. 3. Stellen Sie eine Verbindung mit der EC2-Instance her und führen Sie pg_dump-Backup aus. Weitere Informationen finden Sie in der pg_dump-Dokument	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ation und der Anleitung in der AWS DMS-Dokumentation.	
Bereiten Sie die Zieldatenbank vor.	1. Erstellen Sie einen Migrationsbenutzer, der über Berechtigungen zur Verwendung von pg_restore für Datenbankobjekte verfügt. 2. Importieren Sie den Datenbank-Dump mithilfe von pg_restore. Weitere Informationen finden Sie in der pg_restore-Dokumentation und der Anleitung in der AWS DMS-Dokumentation.	DBA
Validieren von Daten.	1. Vergleichen Sie die Anzahl der Datenbankobjekte zwischen der Quell- und der Zieldatenbank. 2. Beheben Sie alle Abweichungen zwischen den Objektanzahlen.	DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.	Implementieren Sie die Strategie zur Anwendung	DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	smigration, die Sie im ersten Epic erstellt haben.	

Umstellung auf die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.	1. Halten Sie alle Anwendung sservices und Clientver bindungen an, die auf die On-Premises-PostgreSQL-Datenbank verweisen. 2. Führen Sie die AWS DMS-Aufgaben aus. 3. Richten Sie bei Bedarf eine Rollback-Aufgabe ein (CDC von Aurora PostgreSQ L rückgängig machen – kompatibel mit der On-Premises-PostgreSQL-Date nbank). 4. Validieren von Daten . 5. Starten Sie die Anwendung sservices auf dem neuen Ziel, indem Sie Amazon Route 53 für die neue mit Aurora PostgreSQL kompatible DB-Instance konfigurieren. PostgreSQL 6. Fügen Sie die Überwachu ng von Amazon CloudWatc h und Performance Insights auf Ihrer neuen mit Aurora	DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PostgreSQL kompatiblen DB-Instance hinzu.	
Wenn Sie die Migration rückgängig machen müssen.	1. Halten Sie alle Anwendungsservices an, die auf die Aurora-PostgreSQL-kompatible Datenbank verweisen. 2. Setzen Sie die Änderungen an der On-Premises-PostgreSQL-Quelldatenbank mithilfe der AWS DMS-Aufgabe zurück, die Sie in der vorherigen Geschichte erstellt haben. 3. Halten Sie die AWS DMS-Aufgaben an, die von der On-Premises-PostgreSQL-Datenbank zur Aurora PostgreSQL-kompatiblen Datenbank ausgeführt werden. 4. Konfigurieren Sie die Anwendung so, dass sie auf die On-Premises-PostgreSQL-Quelldatenbank zurückweist. 5. Vergewissern Sie sich, dass die gesamte Rollback-Bereitstellung abgeschlossen ist.	DBA, App-Besitzer

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie Ressourcen herunter.	Fahren Sie die temporären AWS-Ressourcen herunter.	DBA, Systemadministrator
Validieren Sie Dokumente.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer, Systemadministrator
Erfassen Sie Metriken.	Erfassen Sie Metriken zur Zeit der Migration, zum Prozentsatz der manuellen Kostenein sparungen im Vergleich zu Tools usw.	DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt.	Schließen Sie das Projekt und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- AWS Data Migration Service
- VPCs und Amazon Aurora
- Amazon-Aurora-Preise
- Verwenden einer PostgreSQL-Datenbank als AWS DMS-Quelle
- So erstellen Sie eine AWS DMS-Replikations-Instance
- So erstellen Sie Quell- und Zielendpunkte mit AWS DMS

Weitere Ressourcen

- Erste Schritte mit AWS DMS
- step-by-step Walkthroughs zur Datenmigration
- Amazon-Aurora-Ressourcen

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux

Erstellt von Tirumala Dasari (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon EC2 Linux mit Microsoft SQL Server
R-Typ: Replatform	Arbeitslast: Microsoft	Technologien: Migration; Datenbanken
AWS-Dienste: Amazon EC2		

Übersicht

Dieses Muster beschreibt, wie Sie mithilfe von Sicherungs- und Wiederherstellungsdienstprogrammen von einer lokalen Microsoft SQL Server-Datenbank, die unter Microsoft Windows ausgeführt wird, zu Microsoft SQL Server auf einer Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instance migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon EC2 Linux AMI (Amazon Machine Image) mit Microsoft SQL Server
- AWS Direct Connect zwischen lokalem Windows und Microsoft SQL Server auf der Linux EC2-Instance

Architektur

Quelltechnologie-Stack

- Lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Linux EC2-Instanz mit einer Microsoft SQL Server-Datenbank

Architektur der Datenbankmigration

Tools

- WinSCP - Dieses Tool ermöglicht es Windows-Benutzern, Dateien einfach mit Linux-Benutzern zu teilen.
- Sqlcmd — Mit diesem Befehlszeilenprogramm können Sie T-SQL-Anweisungen oder Batches an lokale und Remoteinstanzen von SQL Server senden. Das Hilfsprogramm ist äußerst nützlich für sich wiederholende Datenbankaufgaben wie Batchverarbeitung oder Komponententests.

Epen

Bereiten Sie die EC2-Linux-Instanz mit SQL Server vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein AMI aus, das das Linux-Betriebssystem bereitstellt und Microsoft SQL Server enthält.		Systemadministrator
Konfigurieren Sie das AMI, um eine EC2-Instance zu erstellen .		Sysadmin
Erstellen Sie Regeln für eingehenden und ausgehend en Datenverkehr für Sicherhei tsgruppen.		Sysadmin
Konfigurieren Sie die Linux EC2-Instanz für eine Microsoft SQL Server-Datenbank.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Benutzer und gewähren Sie Berechtigungen wie in der Quelldatenbank.		Appowner, DBA
Installieren Sie die SQL Server-Tools und das Hilfsprogramm sqlcmd auf der Linux EC2-Instanz.		DBA

Sichern Sie die Datenbank und verschieben Sie die Sicherungsdatei auf die Linux EC2-Instanz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sichern Sie die lokale SQL Server-Datenbank.		DBA
Installieren Sie WinSCP auf Microsoft SQL Server.		DBA
Verschieben Sie die Sicherungsdatei auf die Linux EC2-Instanz, auf der Microsoft SQL Server ausgeführt wird.		DBA

Stellen Sie die Datenbank auf einer Linux EC2-Instanz wieder her, auf der SQL Server ausgeführt wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Datenbank mithilfe des Dienstprogramms sqlcmd aus der Datenbank-Backup-Datei wieder her.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbank objekte und -daten.		Entwickler, Testingenieur

Wechseln Sie auf einer Linux EC2-Instanz von Windows SQL Server zu Windows SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbank objekte und -daten.		Entwickler, Testingenieur
Wechseln Sie von der lokalen Microsoft SQL Server-Da tenbank zur Linux EC2-Insta nz, auf der Microsoft SQL Server ausgeführt wird.		DBA

Zugehörige Ressourcen

- So konfigurieren Sie SQL Server 2017 auf Amazon Linux 2- und Ubuntu-AMIs
- Installation von SQL-Tools auf einer Linux-Instance
- Backup und Wiederherstellung von einer lokalen Microsoft SQL Server-Datenbank auf Microsoft SQL Server auf einer Linux EC2-Instanz

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server

R-Typ: Replatform	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for Microsoft SQL Server
Erstellt von: AWS	Umgebung: Produktion	Technologien: Datenbanken; Migration
Arbeitslast: Microsoft	AWS-Dienste: Amazon RDS	

Übersicht

Verbindungsserver ermöglichen es Microsoft SQL Server, SQL-Anweisungen auf anderen Instanzen von Datenbankservern auszuführen. Dieses Muster beschreibt, wie Sie Ihre lokale Microsoft SQL Server-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server migrieren können, um geringere Kosten und höhere Verfügbarkeit zu erzielen. Derzeit unterstützt Amazon RDS for Microsoft SQL Server keine Verbindungen außerhalb eines Amazon Virtual Private Cloud (Amazon VPC) -Netzwerks.

Sie können dieses Muster verwenden, um die folgenden Ziele zu erreichen:

- Um Microsoft SQL Server auf Amazon RDS for Microsoft SQL Server zu migrieren, ohne die Funktionen des Verbindungsservers zu beeinträchtigen.
- Um verknüpfte Microsoft SQL Server in verschiedenen Wellen zu priorisieren und zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Prüfen Sie, ob Microsoft SQL Server auf Amazon RDS die von Ihnen benötigten Funktionen unterstützt.
- Stellen Sie sicher, dass Sie entweder Amazon RDS for Microsoft SQL Server mit Standardsortierungen oder Sortierungen auf Datenbankebene verwenden können.

Architektur

Quelltechnologie-Stack

- Lokale Datenbanken (Microsoft SQL Server)

Zieltechnologie-Stack

- Amazon RDS für SQL Server

Architektur des Quellzustands

Architektur des Zielzustands

Im Zielstatus migrieren Sie Microsoft SQL Server mithilfe von Verbindungsservern zu Amazon RDS for Microsoft SQL Server. Diese Architektur verwendet einen Network Load Balancer, um den Datenverkehr von Amazon RDS for Microsoft SQL Server an lokale Server weiterzuleiten, auf denen Microsoft SQL Server ausgeführt wird. Das folgende Diagramm zeigt die Reverse-Proxy-Fähigkeit für den Network Load Balancer.

Tools

- AWS CloudFormation
- Network Load Balancer
- Amazon RDS for SQL Server in mehreren Availability Zones (Multi-AZs)
- AWS Database Migration Service (AWS DMS)

Epen

Eine Landingzone-VPC erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CIDR-Zute ilung.		AWS SysAdmin
Erstellen einer Virtual Private Cloud (VPC).		AWS SysAdmin
Erstellen Sie die VPC-Subne tze.		AWS SysAdmin
Erstellen Sie die Subnetz-Z ugriffskontrolllisten (ACLs).		AWS SysAdmin
Erstellen Sie die Subnetz-R outing-Tabellen.		AWS SysAdmin
Stellen Sie eine Verbindung mit AWS Direct Connect oder AWS Virtual Private Network (VPN) her.		AWS SysAdmin

Migrieren Sie die Datenbank zu Amazon RDS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS for Microsoft SQL Server Server-DB-Instance.		AWS SysAdmin
Erstellen Sie eine AWS DMS-Replikations-Instance.		AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quell- und Zieldatenbank-Endpunkte in AWS DMS.		AWS SysAdmin
Erstellen Sie die Migration saufgabe und setzen Sie die kontinuierliche Replikation nach einer Volllast auf ON.		AWS SysAdmin
Fordern Sie eine Firewall-Änderung an, damit Amazon RDS for Microsoft SQL Server auf die lokalen SQL Server-Da tenbanken zugreifen kann.		AWS SysAdmin
Erstellen Sie einen Network Load Balancer.		AWS SysAdmin
Erstellen Sie eine Zielgruppe, die auf die Datenbankserver in Ihrem Rechenzentrum abzielt	Wir empfehlen, Hostnamen in der Zielkonfiguration zu verwenden, um Failover-Ereignisse im Rechenzentrum (DC) einzubeziehen.	AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die SQL-Anweisung für die Einrichtung des Verbindungsservers aus.	Führen Sie die SQL-Anweisungen zum Hinzufügen eines Verbindungsservers mithilfe des Microsoft SQL-Managementtools für die Amazon RDS for Microsoft SQL Server-DB-Instance aus. Legen Sie in der SQL-Anweisung @datasrc fest, um den Network Load Balancer Balancer-Hostnamen zu verwenden. Fügen Sie Anmeldeinformationen für verknüpfte Server hinzu, indem Sie das Microsoft SQL-Management-Tool für die Amazon RDS for Microsoft SQL Server-DB-Instance verwenden.	AWS SysAdmin
Testen und validieren Sie die SQL Server-Funktionen.		AWS SysAdmin
Erstellen Sie eine Umstellung.		AWS SysAdmin

Zugehörige Ressourcen

- Allgemeine Verwaltungsaufgaben für Microsoft SQL Server auf Amazon RDS
- Sortierungen und Zeichensätze für Microsoft SQL Server
- Dokumentation zum Network Load Balancer
- Implementieren von Verbindungsservern mit Amazon RDS for Microsoft SQL Server (Blogbeitrag)

Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server mithilfe nativer Sicherungs- und Wiederherstellungsmethoden

Erstellt von Tirumala Dasari (AWS), David Queiroz (AWS) und Vishal Singh (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premises SQL Server-Datenbank	Ziel: Amazon RDS für SQL Server
R-Typ: Plattformwechsel	Workload: Microsoft	Technologien: Migration ; Datenbanken; Betriebssysteme
AWS-Services: Amazon RDS; Amazon S3		

Übersicht

Dieses Muster beschreibt, wie Sie eine lokale Microsoft SQL Server-Datenbank zu einer Amazon Relational Database Service (Amazon RDS) für SQL Server-DB-Instance migrieren (homogene Migration). Der Migrationsprozess basiert auf nativen SQL Server-Backup- und Wiederherstellungsmethoden. Es verwendet SQL Server Management Studio (SSMS), um eine Datenbank-Sicherungsdatei zu erstellen, und einen Amazon Simple Storage Service (Amazon S3)-Bucket, um die Sicherungsdatei zu speichern, bevor sie in Amazon RDS für SQL Server wiederhergestellt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Identity and Access Management (IAM)-Rollenrichtlinien für den Zugriff auf den S3-Bucket und die Amazon RDS for SQL Server-DB-Instance.

Einschränkungen

- Der in diesem Muster beschriebene Prozess migriert nur die Datenbank. SQL-Anmeldungen oder Datenbankbenutzer, einschließlich SQL Server Agent-Aufträgen, werden nicht migriert, da sie zusätzliche Schritte erfordern.

Produktversionen

- SQL Server 2012-2017. Die neueste Liste der unterstützten Versionen und Funktionen finden Sie unter Microsoft SQL Server in Amazon RDS in der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- DB-Instance von Amazon RDS für SQL Server

Datenmigrationsarchitektur

Tools

- Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung der SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Polen

Erstellen einer DB-Instance von Amazon RDS für SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie SQL Server als Datenbank-Engine in Amazon RDS für SQL Server aus.		DBA
Wählen Sie die SQL Server Express Edition aus.		DBA
Geben Sie Datenbankdetails an.	Weitere Informationen zum Erstellen einer DB-Instance finden Sie in der Amazon-RDS-Dokumentation.	DBA, App-Besitzer

Erstellen einer Sicherungsdatei aus der lokalen SQL Server-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über SSMS eine Verbindung mit der lokalen SQL Server-Datenbank her.		DBA
Erstellen Sie eine Sicherung der Datenbank.	Anweisungen finden Sie in der SSMS-Dokumentation.	DBA, App-Besitzer

Hochladen der Sicherungsdatei in Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Buckets in Amazon S3.	Weitere Informationen finden Sie in der Amazon S3-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Sicherungsdatei in den S3-Bucket hoch.	Weitere Informationen finden Sie in der Amazon S3-Dokumentation.	SysOps Administrator

Wiederherstellen der Datenbank in Amazon RDS für SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Optionsgruppe zu Amazon RDS hinzu.	1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/. 2. Wählen Sie im Navigationsbereich Optionsgruppen, Gruppe erstellen aus. 3. Geben Sie die Informationen für die Optionsgruppe ein und wählen Sie dann Erstellen aus. 4. Fügen Sie die `SQLSERVER_BACKUP_RESTORE` Option der Optionsgruppe hinzu und wählen Sie dann Option hinzufügen aus. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	SysOps Administrator
Stellen Sie die Datenbank wieder her.	1. Stellen Sie über SSMS eine Verbindung zu Amazon RDS für SQL Server her.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Rufen Sie die `msdb.dbo.rds_restore_database` gespeicherte Prozedur auf, um die Datenbank wiederherzustellen.	

Validieren der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Objekte und Daten.	Validieren Sie die Objekte und Daten zwischen der Quelldatenbank und Amazon RDS for SQL Server. Hinweis: Diese Aufgabe migriert nur die Datenbank. Anmeldungen und Aufträge werden nicht migriert.	App-Eigentümer, DBA

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Leiten Sie den Anwendungsdatenverkehr um.	Leiten Sie nach der Validierung den Anwendungsdatenverkehr an die DB-Instance von Amazon RDS für SQL Server um.	App-Eigentümer, DBA

Zugehörige Ressourcen

- Amazon S3-Dokumentation

- Dokumentation zu Amazon RDS für SQL Server
- Optionen für die Microsoft SQL Server Database Engine

Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL

R-Typ: Replatform	Quelle: Datenbanken: Relational	Ziel: Amazon Aurora MySQL
Erstellt von: AWS	Umgebung: PoC oder Pilot	Technologien: Datenbanken; Migration
Arbeitslast: Microsoft	AWS-Dienste: Amazon Aurora	

Übersicht

Dieses Muster beschreibt, wie eine Microsoft SQL Server-Datenbank, die sich entweder lokal oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance befindet, zu Amazon Aurora MySQL migriert wird. Das Muster verwendet AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT) für die Datenmigration und Schemakonvertierung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum oder auf einer EC2-Instanz
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Konnektoren, installiert entweder auf einem lokalen Computer oder einer EC2-Instance, auf der AWS SCT installiert ist

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016 und 2017 für die Enterprise, Standard, Workgroup und Developer Editionen. Die Web- und Express-Editionen werden von AWS DMS

nicht unterstützt. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Microsoft SQL Server-Versionen finden Sie in der AWS SCT-Dokumentation.

- MySQL-Versionen 5.5, 5.6 und 5.7. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Microsoft SQL Server-Datenbank
- Eine Microsoft SQL Server-Datenbank auf einer EC2-Instanz

Zieltechnologie-Stack

- Aurora MySQL

Architektur der Datenmigration

- Aus einer Microsoft SQL Server-Datenbank, die in der AWS-Cloud läuft

- Aus einer Microsoft SQL Server-Datenbank, die in einem lokalen Rechenzentrum läuft

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) unterstützt Sie bei der Migration Ihrer Daten zu und von weit verbreiteten kommerziellen und Open-Source-Datenbanken, darunter Oracle, SQL Server, MySQL und PostgreSQL. Sie können AWS DMS verwenden, um Ihre Daten

in die AWS Cloud, zwischen lokalen Instances (über eine AWS Cloud-Einrichtung) oder zwischen Kombinationen aus Cloud und lokalen Einrichtungen zu migrieren.

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) vereinfacht heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Erstellen Sie eine Sicherheitsgruppe für ausgehende Nachrichten für die Quell- und Zieldatenbanken.		SysAdmin
Erstellen und konfigurieren Sie bei Bedarf eine EC2-Instance für AWS SCT.		DBA
Laden Sie die neueste Version von AWS SCT und die zugehörigen Treiber herunter.		DBA
Fügen Sie die erforderlichen Benutzer und Berechtigungen in der Quelldatenbank hinzu und validieren Sie sie.		DBA
Erstellen Sie ein AWS SCT-Projekt für den Workload und		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
stellen Sie eine Verbindung zur Quelldatenbank her.		
Erstellen Sie einen Bewertungsbericht und bewerten Sie die Machbarkeit.		DBA

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS-DB-Zielinstanz mit Amazon Aurora als Datenbank-Engine.		DBA
Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Quelle.		DBA
Ordnen Sie die vorhandenen Datenbankbenutzer den neuen Datenbankbenutzern zu.		Besitzer der App
Erstellen Sie Benutzer in der Zieldatenbank.		DBA
Wenden Sie Rollen aus dem vorherigen Schritt auf die Zieldatenbank an.		DBA
Überprüfen Sie die Datenbankoptionen, Parameter, Netzwerkdateien und		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Datenbank-Links in der Quelldatenbank und bewerten Sie dann deren Anwendbarkeit auf die Zieldatenbank.		
Wenden Sie alle relevanten Einstellungen auf das Ziel an.		DBA

Objekte übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS SCT-Konnektivität zur Zieldatenbank.		DBA
Konvertieren Sie das Schema mit AWS SCT.	AWS SCT konvertiert das Quelldatenbankschema und den größten Teil des benutzerdefinierten Codes automatisch in ein Format, das mit der Zieldatenbank kompatibel ist. Jeder Code, den das Tool nicht automatisch konvertieren kann, ist deutlich gekennzeichnet, sodass Sie ihn selbst konvertieren können.	DBA
Überprüfen Sie den generierten SQL-Bericht und speichern Sie alle Fehler und Warnungen.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie automatische Schemaänderungen auf das Ziel an oder speichern Sie sie als .sql-Datei.		DBA
Überprüfen Sie, ob AWS SCT die Objekte auf dem Ziel erstellt hat.		DBA
Alle Elemente, die nicht automatisch konvertiert werden konnten, können manuell neu geschrieben, zurückgewiesen oder neu gestaltet werden.		DBA
Wenden Sie die generiert en Rollen- und Benutzerb erechtigungen an und überprüfen Sie alle Ausnahmen.		DBA

Migrieren Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Migration smethode.		DBA
Erstellen Sie eine Replikati onsinstanz von der AWS DMS-Konsole aus.	Detaillierte Informationen zur Verwendung von AWS DMS finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quell- und Zielendpunkte.		DBA
Erstellen Sie eine Replikati onsaufgabe.		DBA
Starten Sie die Replikati onsaufgabe und überwachen Sie die Protokolle.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS SCT, um die SQL-Elemente im Anwendungscode zu analysier en und zu konvertieren.	Wenn Sie Ihr Datenbank schema von einer Engine in eine andere konvertieren, müssen Sie auch den SQL-Code in Ihren Anwendungen aktualisieren, damit diese mit der neuen Datenbank-Engine anstelle der alten interagieren. Sie können den konvertierten SQL-Code anzeigen, analysier en, bearbeiten und speichern . Detaillierte Informationen zur Verwendung von AWS SCT finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	Besitzer der App
Erstellen Sie die neuen Anwendungsserver auf AWS.		Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie den Anwendung scode auf die neuen Server.		Besitzer der App
Konfigurieren Sie den Anwendungsserver für die Zieldatenbank und die Treiber.		Besitzer der App
Korrigieren Sie jeglichen Code, der für die Quelldate nbank-Engine in der Anwendung spezifisch ist.		Besitzer der App
Optimieren Sie den Anwendungscode für die Ziel-Engine.		Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie alle neuen Benutzer, Zuschüsse und Codeänderungen auf das Ziel an.		DBA
Sperren Sie die Anwendung für alle Änderungen.		Besitzer der App
Stellen Sie sicher, dass alle Änderungen an die Zieldaten bank weitergegeben wurden.		DBA
Verweisen Sie den neuen Anwendungsserver auf die Zieldatenbank.		Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfe alles noch einmal.		Besitzer der App
Geh live.		Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter (AWS DMS-Replikationsinstanz und EC2-Instance, die für AWS SCT verwendet werden).		DBA, Besitzer der App
Aktualisieren Sie das Feedback zum AWS DMS-Prozess für interne Teams.		DBA, Besitzer der App
Überarbeiten Sie den AWS-DMS-Prozess und verbessern Sie gegebenenfalls die Vorlage.		DBA, Besitzer der App
Überprüfen und validieren Sie die Projektdokumente.		DBA, Besitzer der App
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparungen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.		DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie das Projekt und geben Sie Feedback.		DBA, Besitzer der App

Zugehörige Ressourcen

Referenzen

- AWS DMS-Benutzerhandbuch
- AWS SCT-Benutzerhandbuch
- Amazon Aurora Aurora-Preise

Tutorials und Videos

- Erste Schritte mit dem AWS Database Migration Service
- Erste Schritte mit dem AWS Schema Conversion Tool
- Amazon RDS-Ressourcen
- Schrittweise Anleitungen zu AWS DMS

Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB

Erstellt von Shyam Sunder Rakhecha (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Datenbanken: Relational	Ziel: Amazon RDS for MariaDB
R-Typ: Replatform	Arbeitslast: Open Source	Technologien: Migration; Datenbanken

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen MariaDB-Datenbank zu Amazon Relational Database Service (Amazon RDS) für MariaDB mithilfe nativer Tools. Wenn Sie MySQL-Tools installiert haben, können Sie mysql und mysqldump verwenden. Wenn Sie MariaDB-Tools installiert haben, können Sie Mariadb und Mariadb-dump verwenden. MySQL- und MariaDB-Tools haben denselben Ursprung, aber es gibt geringfügige Unterschiede in MariaDB-Version 10.6 und höher.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine MariaDB-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- MariaDB-Versionen 10.0-10.6 (die aktuelle Liste der unterstützten Versionen finden Sie unter MariaDB on Amazon RDS in der AWS-Dokumentation)

Architektur

Quelltechnologie-Stack

- MariaDB-Datenbank in einem lokalen Rechenzentrum

Zieltechnologie-Stack

- Amazon RDS for MariaDB MariaDB-DB-Instance

Zielarchitektur

Architektur der Datenmigration

Tools

- Native MySQL-Tools: mysql und mysqldump
- Native MariaDB-Tools: Mariadb und Mariadb-Dump

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA, Systemadministrator
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		Systemadministrator
Erstellen Sie Sicherhei tsgruppen.		Systemadministrator
Konfigurieren und starten Sie eine Amazon RDS-DB-Instance, auf der MariaDB ausgeführt wird.		Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native Tools, um Datenbankobjekte und Daten zu migrieren.	Verwenden Sie in der Quelldatenbank mysqldump oder mariadb-dump, um eine Ausgabedatei zu erstellen , die Datenbankobjekte und Daten enthält. Verwenden Sie in der Zieldatenbank mysql oder mariadb, um die Daten wiederherzustellen.	DBA
Validieren Sie die Daten.	Überprüfen Sie die Quell- und Zieldatenbanken, um sicherzustellen, dass die Datenmigration erfolgreich war.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA, Besitzer der App, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Sammeln Sie Kennzahlen zum Zeitpunkt der Migration, zu den durch Tools erzielten Kosteneinsparungen usw.		DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Amazon RDS-Referenzen

- Amazon RDS für MariaDB
- Amazon Virtual Private Cloud VPCs und Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen
- Amazon RDS — Preisgestaltung

MySQL- und MariaDB-Referenzen

- mariadb-dump/mysqldump
- mysql-Befehlszeilenclient

Anleitungen und Videos

- Erste Schritte mit Amazon RDS

Migrieren einer On-Premises-MySQL-Datenbank zu Aurora MySQL

Erstellt von Vinod Kumar Sadu (AWS) und Igor Obradovic (AWS)

Umgebung: Produktion	Quelle: On-Premises-MySQL-Datenbank	Ziel: Amazon Aurora MySQL – Kompatible Edition
R-Typ: Plattformwechsel	Workload: Open-Source	Technologien: Migration; Datenbanken
AWS-Services: AWS DMS		

Übersicht

Dieses Muster erklärt, wie Sie eine lokale MySQL-Quelldatenbank zu Amazon Aurora MySQL -kompatible Edition migrieren. Es werden zwei Optionen für die Migration beschrieben: die Verwendung von AWS Database Migration Service (AWS DMS) oder die Verwendung nativer MySQL-Tools wie mysqldbcopy undmysqldump .

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine MySQL-Quelldatenbank in einem On-Premises-Rechenzentrum

Einschränkungen

- Datenbankgrößenbeschränkung: 64 TB

Produktversionen

- MySQL-Versionen 5.7 und 8.0. Die neueste Liste der unterstützten Versionen finden Sie unter Amazon-Aurora-Versionen in der -AWSDokumentation. Wenn Sie verwendenAWS DMS, finden Sie weitere Informationen unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS for MySQL-Versionen, die von unterstützt werdenAWS DMS.

Architektur

Quelltechnologie-Stack

- Eine lokale MySQL-Datenbank

Zieltechnologie-Stack

- Amazon Aurora MySQL-Compatible Edition

Zielarchitektur

Datenmigrationsarchitektur

Verwenden von AWS DMS:

Verwenden nativer MySQL-Tools:

Tools

- AWS Database Migration Service (AWS DMS) unterstützt mehrere Quell- und Zieldatenbanken. Informationen zu MySQL-Quell- und Zieldatenbanken, die von unterstützt werdenAWS DMS, finden Sie unter Migrieren von MySQL-kompatiblen Datenbanken zu AWS. Wir empfehlen Ihnen, die neueste Version von AWS DMS für die umfassendste Versions- und Funktionsunterstützung zu verwenden.
- mysqldbcopy ist ein MySQL-Dienstprogramm, das eine MySQL-Datenbank auf einem einzelnen Server oder zwischen Servern kopiert.
- mysqldump ist ein MySQL-Hilfsprogramm, das eine Dump-Datei aus einer MySQL-Datenbank für Backup- oder Migrationszwecke erstellt.

Polen

Planen der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserver-Instance.		DBA, Systemadministrator
Identifizieren Sie Speichera nforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie basierend auf Kapazität, Speicherfunktionen und Netzwerkfunktionen den richtigen Instance-Typ aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA, Systemadministrator
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Konfigurieren der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherheitsgruppen.		Systemadministrator
Konfigurieren und starten Sie einen mit Aurora MySQL kompatiblen DB-Cluster.		Systemadministrator

Daten migrieren – Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbietern, um Datenbankobjekte und -daten zu migrieren.	Anweisungen finden Sie in der Dokumentation für MySQL-Tools wie mysqldbcopy und mysqldump.	DBA

Daten migrieren – Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.	Anweisungen finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Quelle und Verwenden einer MySQL-kompatiblen Datenbank als Ziel in der -AWS DMSDokumentation.	DBA

Migrieren der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie die Anwendung sclients auf die neue Infrastru ktur.		DBA, App-Besitzer, Systemadministrator

Schließen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Erfassen Sie Metriken zur Zeit der Migration, % des manuellen im Vergleich zum Tool, Kosteneinsparungen usw.		DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt ab und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- Migrieren Ihrer Datenbanken zu Amazon Aurora
- AWS DMS-Website
- AWS DMS-Dokumentation
- Amazon Aurora – Preise
- Erstellen und Herstellen einer Verbindung mit einem Aurora MySQL-DB-Cluster
- Amazon Virtual Private Cloud VPCs und Amazon RDS
- Amazon-Aurora-Dokumentation

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon Aurora

Migrieren Sie On-Premises-MySQL-Datenbanken zu Aurora MySQL mit Percona XtraBackup, Amazon EFS und Amazon S3

Erstellt von Rohan Jamadagni (AWS), sajith menon (AWS) und Udayasimha Theepireddy (AWS)

Quelle: On-Premises	Ziel: Aurora MySQL	R-Typ: Plattformwechsel
Umgebung: Produktion	Technologien: Datenbanken; Migration	Workload: Open-Source
AWS-Services: Amazon S3; Amazon Aurora; Amazon EFS		

Übersicht

Dieses Muster beschreibt, wie Sie große, On-Premises-MySQL-Datenbanken mithilfe von Percona effizient zu Amazon Aurora MySQL migrieren XtraBackup. Percona XtraBackup ist ein Open-Source-Backup-Dienstprogramm, das nicht blockierend für MySQL-basierte Server ist. Das Muster zeigt, wie Sie Amazon Elastic File System (Amazon EFS) verwenden, um die Zeit für das Hochladen des Backups in Amazon Simple Storage Service (Amazon S3) zu reduzieren und das Backup in Amazon Aurora MySQL wiederherzustellen. Das Muster enthält auch Details dazu, wie inkrementelle Percona-Backups erstellt werden, um die Anzahl der Binärprotokolle zu minimieren, die auf die Aurora MySQL-Zieldatenbank angewendet werden sollen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Berechtigungen zum Erstellen von AWS Identity and Access Management (IAM)-Rollen und -Richtlinien
- Netzwerkkonnektivität zwischen der On-Premises-MySQL-Datenbank und der Virtual Private Cloud (VPC) in AWS

Einschränkungen

- Bei den Quellservern muss es sich um Linux-basierte Systeme handeln, die einen Network File System (NFS)-Client (nfs-utils/nfs-common) installieren können.
- Der S3-Bucket, der zum Hochladen von Sicherungsdateien verwendet wird, unterstützt nur serverseitige Verschlüsselung (SSE-S3/SSE-KMS).
- Amazon S3 begrenzt die Größe der Sicherungsdateien auf 5 TB. Wenn Ihre Sicherungsdatei 5 TB überschreitet, können Sie sie in mehrere kleinere Dateien aufteilen.
- Die Anzahl der in den S3-Bucket hochgeladenen Quelldateien darf eine Million Dateien nicht überschreiten.
- Das Muster unterstützt nur die XtraBackup vollständige Percona-Sicherung und die inkrementelle Sicherung. Es unterstützt keine teilweisen Backups, die `--tables`, `--tables-exclude`, `--tables-file--databases`, oder verwenden`--databases-exclude--databases-file`.
- Aurora stellt keine Benutzer, Funktionen, gespeicherten Prozeduren oder Zeitzoneninformationen aus der MySQL-Quelldatenbank wieder her.

Produktversionen

- Die Quelldatenbank muss MySQL Version 5.5, 5.6 oder 5.7 sein.
- Für MySQL 5.7 müssen Sie Percona XtraBackup 2.4 verwenden.
- Für MySQL 5.6 und 5.6 müssen Sie Percona XtraBackup 2.3 oder 2.4 verwenden.

Architektur

Quelltechnologie-Stack

- Linux-basiertes Betriebssystem
- MySQL-Server
- Perkona XtraBackup

Zieltechnologie-Stack

- Amazon Aurora
- Amazon S3
- Amazon EFS

Zielarchitektur

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die das Einrichten, Betreiben und Skalieren von MySQL-Bereitstellungen einfach und kostengünstig macht. Aurora MySQL ist ein Drop-In-Ersatz für MySQL .
- Amazon Elastic File System (Amazon EFS) hilft Ihnen beim Erstellen und Konfigurieren freigegebener Dateisysteme in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Percona XtraBackup ist ein Open-Source-Dienstprogramm, das Streaming, komprimierte und inkrementelle Backups von MySQL-Datenbanken durchführt, ohne Ihre Datenbanken zu unterbrechen oder zu blockieren.

Polen

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Sicherheitsgruppe, die Sie mit Amazon-EFS-Mountingzielen verknüpfen möchten.	Erstellen Sie eine Sicherheitsgruppe in der VPC, die mit einer VPN-Anfügung an die On-Premises-Datenbank über AWS Transit Gateway konfiguriert ist. Weitere Informationen zu den in dieser und anderen Artikeln beschriebenen Befehlen und	AWS DevOps/Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schritten finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“ am Ende dieses Musters.	
Bearbeiten Sie die Sicherheitsgruppenregeln.	Fügen Sie eine Regel für eingehenden Datenverkehr hinzu, die den Typ NFS, Port 2049 und den IP-Bereich des On-Premises-Datenbankservers als Quelle verwendet. Standardmäßig lässt die Regel für ausgehenden Datenverkehr zu, dass der gesamte Datenverkehr verlassen wird. Wenn dies nicht der Fall ist, fügen Sie eine Regel für ausgehenden Datenverkehr hinzu, um eine Verbindung für den NFS-Port zu öffnen. Fügen Sie zwei weitere Regeln für eingehenden Datenverkehr hinzu: Port 2049 (Quelle: Sicherheitsgruppen-ID derselben Sicherheitsgruppe) und Port 22 (Quelle: IP-Bereich von wo aus Sie eine Verbindung zu einer EC2-Instance herstellen).	AWS DevOps/Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Dateisystems.	Verwenden Sie in den Mountingzielen die VPC und die Sicherheitsgruppe, die Sie in der vorherigen Geschicht e erstellt haben. Wählen Sie den Durchsatzmodus und die Leistung basierend auf den E/A-Anforderungen der On-Premises-Datenbank aus. Aktivieren Sie optional die Verschlüsselung im Ruhezustand.	AWS DevOps/Datenbankad ministrator

Mounten des Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Insta nce-Profilrolle, die einer EC2-Instance zugeordnet werden soll.	Erstellen Sie eine IAM-Rolle , die über Berechtigungen zum Hochladen und Zugreifen auf Objekte in Amazon S3 verfügt. Wählen Sie den S3-Bucket aus, in dem das Backup als Richtlinienressour ce gespeichert wird.	AWS DevOps
Erstellen Sie eine EC2-Insta nce.	Starten Sie eine Linux-bas ierte EC2-Instance und fügen Sie die IAM-Instance-Profi lrolle an, die Sie im vorherige n Schritt erstellt haben, sowie die Sicherheitsgruppe, die Sie zuvor erstellt haben.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den NFS-Client.	Installieren Sie den NFS-Client auf dem On-Premises-Datenbankserver und auf der EC2-Instance. Installationsanweisungen finden Sie im Abschnitt „Zusätzliche Informationen“.	DevOps
Mounten Sie das Amazon EFS-Dateisystem ein.	Mounten Sie das Amazon-EFS-Dateisystem On-Premises und auf der EC2-Instance. Erstellen Sie auf jedem Server ein Verzeichnis zum Speichern des Backups und mounten Sie das Dateisystem mithilfe des Mountingzielendpunkts. Ein Beispiel finden Sie im Abschnitt „Zusätzliche Informationen“.	DevOps

Erstellen einer Sicherung der MySQL-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Percona XtraBackup.	Installieren Sie Percona XtraBackup 2.3 oder 2.4 (abhängig von der Version Ihrer MySQL-Datenbank) auf dem On-Premises-Datenbankserver. Installationslinks finden Sie im Abschnitt „Verwandte Ressourcen“.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zählen Sie die Schemata und Tabellen in der Quelldatenbank.	Erfassen und notieren Sie die Anzahl der Schemata und Objekte in der MySQL-Quelldatenbank. Sie werden diese Zählungen verwenden, um die Aurora MySQL-Datenbank nach der Migration zu validieren.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Notieren Sie sich die neueste binäre Protokoll sequenz aus der Quelldate nbank.	Führen Sie diesen Schritt aus, wenn Sie eine binäre Protokollreplikation zwischen der Quelldatenbank und Aurora MySQL einrichten möchten, um Ausfallzeiten zu minimieren. log-bin muss aktiviert sein und server_id muss eindeutig sein. Notieren Sie sich die aktuelle binäre Protokollsequenz aus der Quelldatenbank, kurz bevor Sie eine Sicherung initiiere n. Führen Sie diesen Schritt kurz vor dem vollständigen Backup durch, wenn Sie nur das vollständige Backup verwenden möchten. Wenn Sie vorhaben, inkrement elle Backups nach einer vollständigen Sicherung zu erstellen, führen Sie diesen Schritt unmittelbar vor der endgültigen inkrementellen Sicherung durch, die Sie auf der Aurora MySQL-DB-Instance wiederherstellen werden.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine vollständige Sicherung der MySQL-Quelldatenbank.	Erstellen Sie eine vollständige Sicherung der MySQL-Quelldatenbank mit Percona XtraBackup. Beispielbefehle für vollständige und inkrementelle Backups finden Sie im Abschnitt „Zusätzliche Informationen“.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erstellen Sie inkrementelle Backups mit Percona XtraBackup.	Inkrementelle Backups können verwendet werden, um die Menge der Binärprotokolle zu reduzieren, die Sie anwenden müssen, um die Quelldatenbank mit Aurora MySQL zu synchronisieren. Große und transaktionsintensive Datenbanken können während Backups eine große Anzahl von Binärprotokollen generieren. Indem Sie inkrementelle Backups erstellen und diese auf einem gemeinsam genutzten Amazon-EFS-Dateisystem speichern, können Sie die Zeit für das Sichern und Hochladen Ihrer Datenbank erheblich reduzieren. Weitere Informationen finden Sie im Abschnitt „Zusätzliche Informationen“. Fahren Sie mit dem Erstellen inkrementeller Backups fort, bis Sie bereit sind, mit dem Migrationsprozess zu Aurora zu beginnen.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie Backups vor.	In diesem Schritt werden Transaktionsprotokolle für Transaktionen, die während des Backups unterwegs waren, auf das Backup angewendet. Wenden Sie weiterhin Transakti onsprotokolle (--apply-log-only) auf jedes inkrement elle Backup an, um die Backups zusammenzuführen, mit Ausnahme des letzten Backups. Beispiele finden Sie im Abschnitt „Zusätzli che Informationen“. Nach diesem Schritt befindet sich das vollständige, zusammeng eführte Backup in ~/<efs_mo unt_name>/fullbackup.	Datenbankadministrator
Komprimieren und teilen Sie die letzte zusammengeführte Sicherung auf.	Nachdem Sie das endgültig e, zusammengeführte Backup vorbereitet haben, verwenden Sie die Befehle tar, zip und split, um kleinere Zip-Dateien des Backups zu erstellen. Beispiele finden Sie im Abschnitt „Zusätzliche Informationen“.	Datenbankadministrator

Wiederherstellen des Backups in einem Aurora MySQL-DB-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Backup in Amazon S3 hoch.	Das Amazon-EFS-Dateisystem, in dem die Sicherungsdateien gespeichert sind, wird sowohl in der On-Premises-Datenbank als auch in einer EC2-Instance gemountet, sodass die Sicherungsdateien für die EC2-Instance leicht verfügbar sind. Stellen Sie mithilfe von Secure Shell (SSH) eine Verbindung mit der EC2-Instance her und laden Sie die gezippten Sicherungsdateien in einen neuen oder vorhandenen S3-Bucket hoch. Beispiel: aws s3 sync ~/<efs_mount_name>/fullbackup s3://<bucket_name>/fullbackup. Weitere Informationen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	AWS DevOps
Erstellen Sie eine Servicerolle für Aurora, um auf Amazon S3 zuzugreifen.	Erstellen Sie eine IAM-Rolle mit Vertrauensstellung „rds.amazonaws.com“ und einer Richtlinie, die es Aurora ermöglicht, auf den S3-Bucket zuzugreifen, in dem die Sicherungsdateien gespeichert sind. Die erforderlichen Berechtigungen sind	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ListBucket GetObject, und GetObjectVersion.	
Erstellen Sie die Netzwerkkonfiguration für Aurora.	Erstellen Sie eine Cluster-DB-Subnetzgruppe mit mindestens zwei Availability Zones und einer Subnetz-Routing-Tabellenkonfiguration, die ausgehende Konnektivität zur Quelldatenbank ermöglicht. Erstellen Sie eine Sicherheitsgruppe, die ausgehende Verbindungen zur On-Premises-Datenbank zulässt und es Administratoren ermöglicht, eine Verbindung zum Aurora-DB-Cluster herzustellen. Weitere Informationen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	AWS DevOps/Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Backup in einem Aurora MySQL-DB-Cluster wieder her.	Stellen Sie Ihre Daten aus dem Backup wieder her, das Sie in Amazon S3 hochgeladen haben. Geben Sie die MySQL-Version Ihrer Quelldatenbank an, geben Sie den S3-Bucket-Namen und das Ordnerpfadpräfix an, in das Sie die Sicherungsdatei hochgeladen haben (z. B. „vollständiges Backup“ für die Beispiele im Abschnitt „Zusätzliche Informationen“) und stellen Sie die IAM-Rolle bereit, die Sie erstellt haben, um Aurora den Zugriff auf Amazon S3 zu autorisieren.	AWS DevOps/Datenbankadministrator
Validieren Sie die Aurora MySQL-Datenbank.	Validieren Sie die Anzahl der Schemata und Objekte im wiederhergestellten Aurora-DB-Cluster anhand der Anzahl, die Sie aus der Quelldatenbank erhalten haben.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Binlog-Replikation ein.	Verwenden Sie die binäre Protokollsequenz, die Sie zuvor notiert haben, bevor Sie die letzte Sicherung erstellen, die im Aurora-DB-Cluster wiederhergestellt wurde. Erstellen Sie einen Replikationsbenutzer in der Quelldatenbank und folgen Sie den Anweisungen im Abschnitt „Zusätzliche Informationen“, um die entsprechenden Berechtigungen bereitzustellen, die Replikation in Aurora zu aktivieren und zu bestätigen, dass die Replikation synchron ist.	AWS DevOps/Datenbankadministrator

Zugehörige Ressourcen

Erstellen eines Amazon-EFS-Dateisystems

- Erstellen einer Sicherheitsgruppe (Amazon-VPC-Dokumentation)
- Transit-Gateway-VPN-Anfügungen (Amazon-VPC-Dokumentation)
- Skalieren des VPN-Durchsatzes mit AWS Transit Gateway (Blog für Netzwerk und Bereitstellung von Inhalten)
- Erstellen eines Amazon-EFS-Dateisystems (Amazon-EFS-Dokumentation)
- Erstellen von Mount-Zielen (Amazon-EFS-Dokumentation)
- Verschlüsseln von Daten im Ruhezustand (Amazon-EFS-Dokumentation)

Mounten des Dateisystems

- IAM-Rollen für Amazon EC2 (Amazon-EC2-Dokumentation)

- Starten einer Amazon EC2 Linux-Instance (Amazon EC2-Dokumentation)
- Installieren des NFS-Clients (Amazon-EFS-Dokumentation)
- Mounten des Amazon-EFS-Dateisystems auf Ihrem On-Premises-Client (Amazon-EFS-Dokumentation)
- Mounting von EFS-Dateisystemen (Amazon-EFS-Dokumentation)

Erstellen einer Sicherung der MySQL-Quelldatenbank

- Installieren von Percona XtraBackup 2.3 (Percona- XtraBackup Dokumentation)
- Installieren von Percona XtraBackup 2.4 (Percona- XtraBackup Dokumentation)
- Festlegen der Replikationsmasterkonfiguration (MySQL-Dokumentation)
- Migrieren von Daten aus einer externen MySQL-Datenbank zu einem Aurora MySQL-DB-Cluster (Aurora-Dokumentation)
- Inkrementelle Sicherung (Percona- XtraBackup Dokumentation)

Wiederherstellen des Backups in Amazon Aurora MySQL

- Erstellen eines Buckets (Amazon S3-Dokumentation)
- Herstellen einer Verbindung mit Ihrer Linux-Instance über SSH (Amazon-Ec2-Dokumentation)
- Konfigurieren der AWS CLI (AWS CLI-Dokumentation)
- Sync-Befehl (AWS-CLI-Befehlsreferenz)
- Erstellen einer IAM-Richtlinie für den Zugriff auf Amazon S3-Ressourcen (Aurora-Dokumentation)
- Voraussetzungen für DB-Cluster (Aurora-Dokumentation)
- Arbeiten mit DB-Subnetzgruppen (Aurora-Dokumentation)
- Erstellen einer VPC-Sicherheitsgruppe für eine private DB-Instance (Aurora-Dokumentation)
- Wiederherstellen eines Aurora MySQL-DB-Clusters aus einem S3-Bucket (Aurora-Dokumentation)
- Einrichten der Replikation mit MySQL oder einem anderen Aurora-DB-Cluster (Aurora-Dokumentation)
- mysql.rds_set_external_master-Prozedur (MySQL auf Amazon RDS SQL-Referenz)
- mysql.rds_start_replication-Prozedur (MySQL in Amazon RDS SQL-Referenz)

Zusätzliche Referenzen

- Migrieren von Daten aus einer externen MySQL-Datenbank zu einem Aurora MySQL-DB-Cluster (Aurora-Dokumentation)
- MySQL-Server-Downloads (Oracle-Website)

Tutorials und Videos

- Migrieren von MySQL-Daten zu einem Aurora MySQL-DB-Cluster mit Amazon S3 (AWS Knowledge Center)
- Einrichten und Mounten von Amazon EFS (Video)

Zusätzliche Informationen

Installieren eines NFS-Clients

- Wenn Sie Red Hat oder ein ähnliches Linux-Betriebssystem verwenden, verwenden Sie den Befehl :

```
$ sudo yum -y install nfs-utils
```

- Wenn Sie Ubuntu oder ein ähnliches Linux-Betriebssystem verwenden, verwenden Sie den Befehl :

```
$ sudo apt-get -y install nfs-common
```

Weitere Informationen finden Sie in der Anleitung in der Amazon-EFS-Dokumentation.

Mounten des Amazon-EFS-Dateisystems

Verwenden Sie die -Befehle:

```
mkdir ~/<efs_mount_name>
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ ~/<efs_mount_name>
```

Weitere Informationen finden Sie in der Anleitung und Mounting von EFS-Dateisystemen in der Amazon-EFS-Dokumentation.

Erstellen von Backups der MySQL-Quelldatenbank

Vollständige Backups

Verwenden Sie einen Befehl wie den folgenden, der das Backup aufnimmt, komprimiert und in kleinere Blöcke von jeweils 1 GB aufteilt:

```
xtrabackup --backup --user=dbuser --password=<password> --binlog-info=AUTO --stream=tar
 --target-dir=~/<efs_mount_name>/fullbackup | gzip - | split -d --bytes=1024MB - ~/
<efs_mount_name>/fullbackup/backup.tar.gz &
```

Wenn Sie vorhaben, nachfolgende inkrementelle Backups nach dem vollständigen Backup zu erstellen, komprimieren und teilen Sie das Backup nicht. Verwenden Sie stattdessen einen Befehl ähnlich dem folgenden:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/fullbackup/
```

Inkrementelle Backups

Verwenden Sie den vollständigen Sicherungspfad für den `--incremental-basedir` Parameter, z. B.:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/incremental/backupdate --incremental-basedir=~/<efs_mount_name>/
fullbackup
```

wobei basedir der Pfad zum vollständigen Backup und zur xtrabackup_checkpoints-Datei ist.

Weitere Informationen zum Erstellen von Backups finden Sie unter Migrieren von Daten aus einer externen MySQL-Datenbank zu einem Amazon Aurora MySQL-DB-Cluster in der Aurora-Dokumentation.

Vorbereiten von Backups

So bereiten Sie ein vollständiges Backup vor:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup
```

So bereiten Sie ein inkrementelles Backup vor:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup --
incremental-dir=~/<efs_mount_name>/incremental/06062020
```

So bereiten Sie das endgültige Backup vor:

```
xtrabackup --prepare --target-dir=~/<efs_mount_name>/fullbackup --incremental-dir=~/
<efs_mount_name>/incremental/06072020
```

Weitere Informationen finden Sie unter Inkrementelle Backups in der Percona- XtraBackup Dokumentation.

Komprimieren und Aufteilen des zusammengeführten Backups

So komprimieren Sie das zusammengeführte Backup unter ~/<efs_mount_name>/fullbackup:

```
tar -zcvf <backupfilename.tar.gz> ~/<efs_mount_name>/fullbackup
```

So teilen Sie das Backup auf:

```
split -d -b1024M --verbose  <backupfilename.tar.gz> <backupfilename.tar.gz>
```

Einrichten der Binlog-Replikation

So erstellen Sie einen Replikationsbenutzer in der Quelldatenbank und stellen die entsprechenden Berechtigungen bereit:

```
CREATE USER 'repl_user'@'' IDENTIFIED BY ''; GRANT REPLICATION CLIENT, REPLICATION
 SLAVE ON *.* TO 'repl_user'@'';
```

Um die Replikation auf Aurora zu aktivieren, indem Sie eine Verbindung zum Aurora-DB-Cluster herstellen, aktivieren Sie Binärprotokolle in der DB-Cluster-Parametergruppe. Einstellen `binlog_format = mixed` (Mischmodus wird bevorzugt). Diese Änderung erfordert, dass Sie die Instance neu starten, um das Update anzuwenden.

```
CALL mysql.rds_set_external_master ('sourcedbinstanceIP', sourcedbport, 'repl_user',
 '', 'binlog_file_name', binlog_file_position, 0); CALL mysql.rds_start_replication;
```

So bestätigen Sie, dass die Replikation synchron ist:

```
SHOW Slave Status \G;
```

Das Feld Sekunden hinter Master zeigt an, wie weit Aurora von der On-Premises-Datenbank entfernt ist.

Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS

Quelle: Anwendungen	Ziel: Containerisierte Anwendung, die auf Amazon ECS bereitgestellt wird	R-Typ: Replatform
Umgebung: PoC oder Pilotprojekt	Technologien: Migration; Web- und mobile Apps	Arbeitslast: Open Source
AWS-Services: Amazon EC2 Container Registry; Amazon ECS		

Übersicht

AWS App2Container (A2C) ist ein Befehlszeilentool, das dabei hilft, bestehende Anwendungen, die auf virtuellen Maschinen ausgeführt werden, in Container umzuwandeln, ohne dass Codeänderungen erforderlich sind. A2C erkennt Anwendungen, die auf einem Server laufen, identifiziert Abhängigkeiten und generiert relevante Artefakte für eine reibungslose Bereitstellung in Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Kubernetes Service (Amazon EKS).

Dieses Muster enthält die Schritte für die Remote-Migration von lokalen Java-Anwendungen, die auf einem Anwendungsserver bereitgestellt werden, zu AWS Fargate oder Amazon EKS mithilfe von App2Container über den Worker-Computer.

Der Arbeitscomputer kann in den folgenden Anwendungsfällen verwendet werden:

- Die Docker-Installation ist auf den Anwendungsservern, auf denen die Java-Anwendungen ausgeführt werden, nicht zulässig oder nicht verfügbar.
- Sie müssen die Migration mehrerer Anwendungen verwalten, die auf verschiedenen physischen oder virtuellen Servern bereitgestellt werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Anwendungsserver mit einer Java-Anwendung, die auf einem Linux-Server ausgeführt wird
- Ein Arbeitscomputer mit einem Linux-Betriebssystem
- Ein Arbeitscomputer mit mindestens 20 GB verfügbarem Festplattenspeicher

Einschränkungen

- Nicht alle Anwendungen werden unterstützt. Weitere Informationen finden Sie unter Unterstützte Anwendungen für Linux.

Architektur

Quelltechnologie-Stack

- Java-Anwendungen, die auf einem Linux-Server ausgeführt werden

Zieltechnologie-Stack

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Elastic Container Registry
- AWS Fargate

Zielarchitektur

Tools

Tools

- AWS App2Container — AWS App2Container (A2C) ist ein Befehlszeilentool, mit dem Sie Anwendungen, die in Ihren lokalen Rechenzentren oder auf virtuellen Maschinen ausgeführt werden, so verschieben können, dass sie in Containern ausgeführt werden, die von Amazon ECS oder Amazon EKS verwaltet werden.

- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und produziert Artefakte, die sofort einsatzbereit sind.
- AWS CodeCommit — AWS CodeCommit ist ein von Amazon Web Services gehosteter Service zur Versionskontrolle, mit dem Sie Ressourcen (wie Dokumente, Quellcode und Binärdateien) privat in der Cloud speichern und verwalten können.
- AWS CodePipeline — AWS CodePipeline ist ein Continuous Delivery Service, mit dem Sie die zur Veröffentlichung Ihrer Software erforderlichen Schritte modellieren, visualisieren und automatisieren können.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen.
- AWS Fargate — AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen, ohne Server oder Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Mit Fargate müssen Sie keine Cluster virtueller Maschinen mehr bereitstellen, konfigurieren oder skalieren, um Container auszuführen.

Epen

Richten Sie Anmeldeinformationen ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Geheimnis für den Zugriff auf den Anwendungsserver.	Um vom Arbeitscomputer aus remote auf den Anwendung sserver zuzugreifen, erstellen Sie ein Geheimnis in AWS Secrets Manager. Für Ihr Geheimnis können Sie entweder den privaten SSH-	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schlüssel oder das Zertifikat und den privaten SSH-Schlüssel verwenden. Weitere Informationen finden Sie unter Manage Secrets for AWS App2Container.	

Richten Sie die Arbeitsmaschine ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die TAR-Datei.	Führen Sie `sudo yum install -y tar`.	DevOps, Entwickler
Installieren Sie den AWS CLI.	Führen Sie den Befehl aus, um das Amazon Command Line Interface (AWS CLI) zu installieren`curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip" .` Extrahieren Sie `awscliv2.zip .` Führen Sie `sudo ./aws/install .`	DevOps, Entwickler
Installieren Sie App2Container.	Führen Sie die folgenden Befehle aus: `curl -o AWSApp2Container-installer-linux.tar.gz https://app2contai`	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`ner-release-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/AWSApp2Container-installer-linux.tar.gz`
	
	`sudo tar xvf AWSApp2Container-installer-linux.tar.gz`
	
	`sudo ./install.sh`	

Konfigurieren Sie die Profile.	Führen Sie den Befehl aus, um das AWS-Standardprofil zu konfigurieren`sudo aws configure` . Führen Sie den Befehl aus, um das benannte AWS-Standardprofil zu konfigurieren`sudo aws configure --profile <profile name>`.	DevOps, Entwickler

Docker-Installation.	Führen Sie die folgenden Befehle aus.
	
	`sudo yum install -y docker`
	
	`sudo systemctl enable docker & sudo systemctl restart docker`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie App2Container.	Um App2Container zu initialisieren, benötigen Sie die folgenden Informationen: • `workspace` : Um Artefakte zur Containerisierung von Anwendungen zu speichern . Es wird empfohlen, einen Verzeichnispfad mit mindestens 20 GB freiem Festplattenspeicher anzugeben. • `awsProfile` : Auf dem Server konfiguriertes AWS-Profil. Dies ist erforderlich, um Artefakte auf Amazon S3 hochzuladen, den `containerize` Befehl auszuführen und AWS-Artefakte für die Bereitstellung auf Amazon ECS oder Amazon EKS zu generieren. • `s3Bucket`: Um AWS-Artefakte zu extrahieren und zu speichern. • `metricsReportPermission` : Um gemeldete Metriken zu sammeln und zu speichern. • `dockerContentTrust` : Um das Docker-Image zu signieren.	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie `sudo app2container init .`	

Konfigurieren Sie den Arbeitscomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Arbeitscomputer so, dass er eine Remoteverbindung herstellt und App2Container-Befehle auf dem Anwendungsserver ausführt.	Um den Arbeitscomputer zu konfigurieren, sind die folgenden Informationen erforderlich: • `Server FQDN`: Der vollqualifizierte Domänenname des Anwendungsservers. • `Server IP address`: Die IP-Adresse des Anwendungsservers. Entweder der FQDN oder die IP-Adresse ist ausreichend. • `SecretARN` : Der Amazon-Ressourcenname (ARN) des Secrets, das für die Verbindung mit dem Anwendungsserver verwendet wird und in Secrets Manager gespeichert ist. • `AuthMethod` : Die `cert` Authentifizierungsmethode `key` oder.	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie `sudo app2container remote configure` .	

Entdecken, analysieren und extrahieren Sie Anwendungen auf dem Arbeitscomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entdecken Sie die lokalen Java-Anwendungen.	Führen Sie den folgenden Befehl aus, um per Fernzugriff alle Anwendungen zu ermitteln , die auf dem Anwendungsserver ausgeführt werden. `sudo app2container remote inventory --target <FQDN/IP of App server>` Dieser Befehl generiert eine Liste der bereitgestellten Anwendungen in`inventory.json` .	Entwickler, DevOps
Analysieren Sie die entdeckten Anwendungen.	Führen Sie den folgenden Befehl aus, um jede Anwendung mithilfe der in der Inventarphase erhaltenen Anwendungs-ID remote zu analysieren. `sudo app2container remote analyze --application-id <java-app-id> --target`	Entwickler, DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<FQDN/IP of App Server>` Dadurch wird eine `analysis.json` Datei am Speicherort des Workspace generiert. Nachdem diese Datei generiert wurde, können Sie die Containerisierungsparameter Ihren Bedürfnissen entsprechend ändern.	
Extrahieren Sie die analysierten Anwendungen.	Um ein Anwendungsarchiv für die analysierte Anwendung zu generieren, führen Sie den folgenden Befehl remote aus, der das TAR-Bundle am Workspace-Speicherort generiert. `sudo app2container remote extract --application-id <application id> --target <FQDN/IP of App Server>` Extrahierte Artefakte können auf dem lokalen Arbeitscomputer generiert werden.	Entwickler, DevOps

Containeriere die extrahierten Artefakte auf dem Worker-Computer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Containerisieren Sie die extrahierten Artefakte.	Containerisieren Sie die im vorherigen Schritt extrahier ten Artefakte, indem Sie den folgenden Befehl ausführen. `sudo app2container containerize --input-archive <tar bundle location on worker machine>`	Entwickler, DevOps
Finalisieren Sie das Ziel.	Um das Ziel zu finalisie ren, öffnen Sie es. Es wird erstelltdeployment.json , wenn der container ize Befehl ausgeführt wird. Um AWS Fargate als Ziel anzugeben, legen Sie createEcsArtifacts auf true fest. Um Amazon EKS als Ziel festzulegen, legen Sie den Wert createEks Artifacts auf true fest.	Entwickler, DevOps

Generieren und Bereitstellen von AWS-Artefakten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie AWS-Berei tstellungsartefakte auf dem Arbeitscomputer.	Führen Sie den folgenden Befehl aus, um Bereitste llungsartefakte zu generieren.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sudo app2container generate app-deployment --application-id <application id>` Dadurch wird die `ecs-master.yml` CloudFormation AWS-Vorlage im Workspace generiert.	
Stellen Sie die Artefakte bereit.	Um die generierten Artefakte weiter bereitzustellen, stellen Sie die CloudFormation AWS-Vorlage bereit, indem Sie den folgenden Befehl ausführen. `aws cloudformation deploy --template-file <path to ecs-master.yml> --capabilities CAPABILITY_NAMED_IAM --stack-name <application id>-ECS`	DevOps
Generieren Sie die Pipeline.	Modifizieren Sie`pipeline.json` , was in der vorherigen Geschichte erstellt wurde, basierend auf Ihren Bedürfnissen. Führen Sie dann den `generate pipeline` Befehl aus, um die Artefakte für die Pipeline-Bereitstellung zu generieren.	DevOps

Zugehörige Ressourcen

- Was ist App2Container?
- Blogbeitrag zu AWS App2Container
- Grundlagen der AWS-CLI-Konfiguration
- Docker-Grundlagen für Amazon ECS
- Docker-Befehle

Migrieren gemeinsam genutzter Dateisysteme in einer großen AWS-Migration

Erstellt von Amit Rudraraju (AWS), Sam Apa (AWS), Bheemeswararaoa (AWS), Wally Lu (AWS) und Sanjeev Prakasam (AWS)

Umgebung: Produktion	Quelle: Lokales gemeinsam genutztes Dateisystem	Ziel: Amazon EFS oder Amazon FSx
R-Typ: Plattformwechsel	Workload: Alle anderen Workloads	Technologien: Migration; Speicher und Backup
AWS-Services: AWS DataSync; Amazon EFS ; Amazon FSx für Windows File Server; Amazon FSx für NetApp ONTAP		

Übersicht

Die Migration von 300 oder mehr Servern wird als große Migration betrachtet. Der Zweck einer großen Migration besteht darin, Workloads von ihren vorhandenen On-Premises-Rechenzentren in die AWS Cloud zu migrieren. Diese Projekte konzentrieren sich in der Regel auf Anwendungs- und Datenbank-Workloads. Freigegebene Dateisysteme erfordern jedoch eine gezielte Aufmerksamkeit und einen separaten Migrationsplan. Dieses Muster beschreibt den Migrationsprozess für gemeinsam genutzte Dateisysteme und bietet bewährte Methoden für die erfolgreiche Migration im Rahmen eines großen Migrationsprojekts.

Ein gemeinsam genutztes Dateisystem (SFS), auch bekannt als Netzwerk- oder Cluster-Dateisystem, ist eine Dateifreigabe, die auf mehreren Servern bereitgestellt wird. Auf freigegebene Dateisysteme kann über Protokolle wie Network File System (NFS), Common Internet File System (CIFS) oder Server Message Block (SMB) zugegriffen werden.

Diese Systeme werden nicht mit Standard-Migrationstools wie AWS Application Migration Service migriert, da sie weder für den Host bestimmt sind, der migriert wird, noch als Blockgerät dargestellt werden. Obwohl die meisten Hostabhängigkeiten transparent migriert werden, muss die Koordination und Verwaltung der abhängigen Dateisysteme separat erfolgen.

Sie migrieren freigegebene Dateisysteme in den folgenden Phasen: Erkennen, Planen, Vorbereiten, Cutover und Validieren. Mit diesem Muster und den angehängten Arbeitsmappen migrieren Sie Ihr freigegebenes Dateisystem zu einem AWS-Speicherservice wie Amazon Elastic File System (Amazon EFS), Amazon FSx für NetApp ONTAP oder Amazon FSx für Windows File Server. Um das Dateisystem zu übertragen, können Sie AWS DataSync oder ein Tool eines Drittanbieters verwenden, z. B. NetApp SnapMirror.

Hinweis: Dieses Muster ist Teil einer AWS Prescriptive Guidance-Serie zu großen Migrationen in die AWS Cloud . Dieses Muster enthält bewährte Methoden und Anweisungen für die Einbindun g von SFSs in Ihre Wave-Pläne für Server. Wenn Sie ein oder mehrere gemeinsam genutzte Dateisysteme außerhalb eines großen Migrationsprojekts migrieren, lesen Sie die Datenüber tragungsanweisungen in der AWS-Dokumentation für Amazon EFS , Amazon FSx for Windows File Server und Amazon FSx for NetApp ONTAP .

Voraussetzungen und Einschränkungen

Voraussetzungen

Die Voraussetzungen können je nach Quell- und Zieldateisystem und Anwendungsfall variieren. Die folgenden sind am häufigsten:

- Ein aktives AWS-Konto.
- Sie haben die Erkennung des Anwendungsportfolios für Ihr großes Migrationsprojekt abgeschlossen und mit der Entwicklung von Wave-Plänen begonnen. Weitere Informationen finden Sie unter Portfolio-Playbook für große AWS-Migrationen.
- Virtual Private Clouds (VPCs) und Sicherheitsgruppen, die eingehenden und ausgehenden Datenverkehr zwischen dem On-Premises-Rechenzentrum und Ihrer AWS-Umgebung zulassen. Weitere Informationen finden Sie unter Konnektivitätsoptionen von Netzwerk zu Amazon VPC und AWS- DataSync Netzwerkanforderungen.
- Berechtigungen zum Erstellen von AWS- CloudFormation Stacks oder Berechtigungen zum Erstellen von Amazon EFS- oder Amazon FSx-Ressourcen. Weitere Informationen finden Sie in der CloudFormation Dokumentation , der Amazon-EFS-Dokumentation oder der Amazon-FSx-Dokumentation .
- Wenn Sie AWS DataSync zur Durchführung der Migration verwenden, benötigen Sie die folgenden Berechtigungen:

- Berechtigungen für AWS DataSync zum Senden von Protokollen an eine AWS CloudWatch Logs-Protokollgruppe. Weitere Informationen finden Sie unter Erlauben DataSync des Hochladens von Protokollen in CloudWatch Protokollgruppen.
- Berechtigungen für den Zugriff auf die CloudWatch Logs-Protokollgruppe. Weitere Informationen finden Sie unter Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihre CloudWatch Logs-Ressourcen.
- Berechtigungen zum Erstellen von Agenten und Aufgaben in DataSync. Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen für die Verwendung von AWS DataSync.

Einschränkungen

- Dieses Muster ist darauf ausgelegt, SFSs im Rahmen eines großen Migrationsprojekts zu migrieren. Es enthält bewährte Methoden und Anweisungen für die Einbindung von SFSs in Ihre Wave-Pläne für die Migration von Anwendungen. Wenn Sie ein oder mehrere gemeinsam genutzte Dateisysteme außerhalb eines großen Migrationsprojekts migrieren, lesen Sie die Datenübertragungsanweisungen in der AWS-Dokumentation für Amazon EFS , Amazon FSx for Windows File Server und Amazon FSx for NetApp ONTAP .
- Dieses Muster basiert auf häufig verwendeten Architekturen, Services und Migrationsmustern. Große Migrationsprojekte und Strategien können jedoch zwischen Organisationen variieren. Möglicherweise müssen Sie diese Lösung oder die bereitgestellten Arbeitsmappen an Ihre Anforderungen anpassen.

Architektur

Quelltechnologie-Stack

Eine oder mehrere der folgenden Optionen:

- Linux (NFS)-Dateiserver
- Windows (SMB)-Dateiserver
- NetApp -Speicher-Array
- Dell EMC Isilon-Speicher-Array

Zieltechnologie-Stack

Eine oder mehrere der folgenden Optionen:

- Amazon Elastic File System
- Amazon FSx für NetApp ONTAP
- Amazon FSx für Windows File Server

Zielarchitektur

Das Diagramm zeigt den folgenden Prozess:

1. Sie stellen eine Verbindung zwischen dem On-Premises-Rechenzentrum und der AWS Cloud her, indem Sie einen AWS-Service wie AWS Direct Connect oder AWS Site-to-Site VPN verwenden.
2. Sie installieren den DataSync Agenten im On-Premises-Rechenzentrum.
3. Laut Ihrem Wave-Plan verwenden Sie , DataSync um Daten aus dem gemeinsam genutzten Quelldateisystem in die gemeinsame Nutzung der AWS-Zieldatei zu replizieren.

Migrationsphasen

Die folgende Abbildung zeigt die Phasen und allgemeinen Schritte für die Migration eines SFS in einem großen Migrationsprojekt.

Der Abschnitt „Epics“ dieses Musters enthält detaillierte Anweisungen zum Abschluss der Migration und zur Verwendung der angehängten Arbeitsmappen. Im Folgenden finden Sie einen allgemeinen Überblick über die Schritte in diesem schrittweisen Ansatz.

Phase	Schritte
Erkennen	1. Mit einem Erkennungstool sammeln Sie Daten über das gemeinsam genutzte Dateisystem, einschließlich Servern, Mountingpunkten und IP-Adressen. 2. Mithilfe einer Konfigurationsverwaltungsdatenbank (CMDB) oder Ihres Migrationstools erfassen Sie Details zum Server, einschließlich Informationen über die Migrationswellen, die

	Umgebung, den Anwendungsbesitzer, den Namen des IT Service Management (ITSM)-Service, die Organisationseinheit und die Anwendungs-ID.
Plan	3. Erstellen Sie anhand der gesammelten Informationen über die SFSs und die Server den SFS-Wellenplan. 4. Wählen Sie anhand der Informationen in der Build-Arbeitsmappe für jedes SFS einen Ziel-AWS-Service und ein Migrationstool aus.
Vorbereitung	5. Richten Sie die Zielinfrastruktur in Amazon EFS , Amazon FSx für NetApp ONTAP oder Amazon FSx für Windows File Server ein. 6. Richten Sie den Datenübertragungsservice ein, z. B. DataSync, und starten Sie dann die erste Datenübertragung. Wenn die erste Synchronisierung abgeschlossen ist, können Sie wiederkehrende Synchronisierungen so einrichten, dass sie nach einem Zeitplan ausgeführt werden. 7. Aktualisieren Sie den SFS-Wellenplan mit Informationen über die gemeinsame Nutzung der Zieldatei, z. B. die IP-Adresse oder den Pfad.

Cutover	8. Stoppen Sie Anwendungen, die aktiv auf das Quell-SFS zugreifen. 9. Führen Sie im -Datenübertragungsservice eine endgültige Datenübertragung durch. 10. Wenn die Synchronisierung abgeschlossen ist, überprüfen Sie, ob sie vollständig erfolgreich war, indem Sie die Protokolldaten in - CloudWatch Protokolle überprüfen.
Validieren	11. Ändern Sie auf den Servern den Mountingpunkt in den neuen SFS-Pfad. 12. Starten und validieren Sie die Anwendungen neu.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, damit Sie sie überwachen und sicher archivieren können.
- AWS DataSync ist ein Online-Service zur Datenübertragung und -erkennung, mit dem Sie Dateien oder Objektdaten in, von und zwischen AWS-Speicherservices verschieben können.
- Amazon Elastic File System (Amazon EFS)hilft Ihnen beim Erstellen und Konfigurieren freigegebener Dateisysteme in der AWS Cloud.
- Amazon FSx bietet Dateisysteme, die branchenübliche Konnektivitätsprotokolle unterstützen und eine hohe Verfügbarkeit und Replikation über AWS-Regionen hinweg bieten.

Andere Tools

- SnapMirror ist ein NetApp Datenreplikationstool, das Daten von bestimmten Quell-Volumes oder Qtrees auf Ziel-Volumes bzw. Qtrees repliziert. Sie können dieses Tool verwenden, um ein NetApp Quelldateisystem zu Amazon FSx für ONTAP zu migrieren.

- Robocopy , die für Robust File Copy kurz ist, ist ein Befehlszeilenverzeichnis und ein Befehl für Windows. Sie können dieses Tool verwenden, um ein Windows-Quelldateisystem zu Amazon FSx for Windows File Server zu migrieren.

Bewährte Methoden

Wave-Planungsansätze

Berücksichtigen Sie bei der Planung von Wellen für Ihr großes Migrationsprojekt die Latenz und die Anwendungsleistung. Wenn das SFS und die abhängigen Anwendungen an verschiedenen Standorten ausgeführt werden, z. B. an einem in der Cloud und an einem im On-Premises-Rechenzentrum, kann dies die Latenz erhöhen und die Anwendungsleistung beeinträchtigen. Die folgenden Optionen sind beim Erstellen von Wave-Plänen verfügbar:

1. Migrieren Sie das SFS und alle abhängigen Server innerhalb derselben Welle – Dieser Ansatz verhindert Leistungsprobleme und minimiert Neuarbeiten, z. B. die mehrfache Neukonfiguration von Mount-Punkten. Es wird empfohlen, wenn zwischen der Anwendung und dem SFS eine sehr geringe Latenz erforderlich ist. Die Wave-Planung ist jedoch komplex, und das Ziel besteht in der Regel darin, Variablen aus Abhängigkeitsgruppierungen zu entfernen und ihnen nicht hinzuzufügen. Darüber hinaus wird dieser Ansatz nicht empfohlen, wenn viele Server auf dasselbe SFS zugreifen, da er die Welle zu groß macht.
2. Migrieren Sie das SFS, nachdem der letzte abhängige Server migriert wurde – Wenn beispielsweise von mehreren Servern auf ein SFS zugegriffen wird und diese Server für die Migration in den Waves 4, 6 und 7 geplant sind, planen Sie das SFS für die Migration in Wave 7 ein.

   Dieser Ansatz ist oft der logischste für große Migrationen und wird für latenzempfindliche Anwendungen empfohlen. Es reduziert die mit der Datenübertragung verbundenen Kosten. Es minimiert auch die Latenzzeit zwischen dem SFS und Anwendungen mit höherer Stufe (z. B. Produktion), da Anwendungen mit höherer Stufe in der Regel nach Entwicklungs- und QA-Anwendungen als letzte migriert werden sollen.

   Dieser Ansatz erfordert jedoch weiterhin Entdeckung, Planung und Agilität. Möglicherweise müssen Sie das SFS in einer früheren Welle migrieren. Vergewissern Sie sich, dass die Anwendungen der zusätzlichen Latenz für den Zeitraum zwischen der ersten abhängigen Welle und der Welle, die das SFS enthält, standhalten können. Führen Sie eine Erkennungssitzung mit den Anwendungsbesitzern durch und migrieren Sie die Anwendung in derselben Welle zur latenzempfindlichsten Anwendung. Wenn nach der Migration einer abhängigen Anwendung

Leistungsprobleme auftreten, bereiten Sie sich darauf vor, schnell zu pivotieren, um das SFS so schnell wie möglich zu migrieren.

3. Migrieren des SFS am Ende des großen Migrationsprojekts – Dieser Ansatz wird empfohlen, wenn die Latenz kein Faktor ist, z. B. wenn selten auf die Daten im SFS zugegriffen wird oder sie nicht entscheidend für die Anwendungsleistung sind. Dieser Ansatz optimiert die Migration und vereinfacht die Cutover-Aufgaben.

Sie können diese Ansätze basierend auf der Latenzsensibilität der Anwendung mischen. Sie können beispielsweise latenzempfindliche SFSs mithilfe der Ansätze 1 oder 2 und dann die restlichen SFSs mithilfe von Ansatz 3 migrieren.

Auswählen eines AWS-Dateisystemservices

AWS bietet mehrere Cloud-Services für die Dateispeicherung. Jedes bietet unterschiedliche Vorteile und Einschränkungen in Bezug auf Leistung, Größe, Zugänglichkeit, Integration, Compliance und Kostenoptimierung. Es gibt einige logische Standardoptionen. Wenn Ihr aktuelles On-Premises-Dateisystem beispielsweise Windows Server ausführt, ist Amazon FSx for Windows File Server die Standardauswahl. Oder wenn das On-Premises-Dateisystem NetApp ONTAP ausführt, ist Amazon FSx für NetApp ONTAP die Standardauswahl. Sie können jedoch einen Zielservice wählen, der auf den Anforderungen Ihrer Anwendung basiert oder andere Cloud-Betriebsvorteile nutzt. Weitere Informationen finden Sie unter Auswählen des richtigen AWS-Dateispeicherservices für Ihre Bereitstellung (AWS Summit-Präsentation).

Auswählen eines Migrationstools

Amazon EFS und Amazon FSx unterstützen die Verwendung von AWS DataSync für die Migration gemeinsam genutzter Dateisysteme in die AWS Cloud. Weitere Informationen zu unterstützten Speichersystemen und -services, Vorteilen und Anwendungsfällen finden Sie unter Was ist AWS? DataSync. Eine Übersicht über die Verwendung von DataSync zum Übertragen Ihrer Dateien finden Sie unter Funktionsweise von AWS- DataSync Übertragungen.

Es gibt auch mehrere Tools von Drittanbietern, die verfügbar sind, darunter die folgenden:

- Wenn Sie Amazon FSx für NetApp ONTAP wählen, können Sie verwenden, NetApp SnapMirror um die Dateien vom On-Premises-Rechenzentrum in die Cloud zu migrieren. SnapMirror verwendet die Replikation auf Blockebene, was schneller sein kann als DataSync und die Dauer des Datenübertragungsprozesses reduzieren kann. Weitere Informationen finden Sie unter Migrieren zu FSx für ONTAP mit NetApp SnapMirror.

- Wenn Sie Amazon FSx für Windows File Server wählen, können Sie Robocopy verwenden, um Dateien in die Cloud zu migrieren. Weitere Informationen finden Sie unter Migrieren vorhandener Dateien zu FSx für Windows File Server mit Robocopy.

Polen

Erkennen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das SFS-Discovery-Workbook vor.	1. Laden Sie die Arbeitsmappen im Abschnitt Anhänge dieses Musters herunter. Dies enthält zwei Dateien, SFS-Discovery-Workbook.xlsx und SFS-Wave-Plan-Workbook.xlsx. 2. Öffnen Sie die SFS-Discovery-Workbook-Datei in Microsoft Excel. 3. Gehen Sie auf dem Dashboard wie folgt vor: • Aktualisieren Sie in Spalte A den Umgebungsnamen. • Aktualisieren Sie in Spalte B die Reihenfolge der Umgebungen, um sie in der Reihenfolge der niedrigsten (1) Priorität auf die höchste Priorität zu setzen. • Aktualisieren Sie in den Spalten D–E den Wave-Zeitplan.	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Aktualisieren Sie in den Spalten C und K die AWS-Kontonamen. • Aktualisieren Sie in Spalte L die VPC-IDs . • Aktualisieren Sie in den Spalten M–O die Subnetz-IDs . 4. Überprüfen Sie den Rest der Workbook-Vorlage und aktualisieren Sie alle anderen Werte, die für Ihre Organisation oder Ihren Anwendungsfall erforderlich sind. 5. Speichern Sie das Arbeitsbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen über das Quell-SFS.	1. Identifizieren Sie mit Ihrem bevorzugten Erkennung stool alle SFS-Mounts auf allen entsprechenden Speichergeräten, Linux-Servern und Windows-Servern. In der Regel müssen Sie die folgenden Informationen sammeln: • Client-Geräte • Client-IP-Adresse • SFS-Details • Mountingpunkt Hinweis: Sie können Ihrem Migrations-Runbook Mountingpunktdetails hinzufügen, um das SFS nach der Migration erneut zu mounten. 2. Öffnen Sie die Datei SFS-Discovery-Workbook. 3. Gehen Sie auf dem Wave-Sheet-Arbeitsplan wie folgt vor: • Vergewissern Sie sich in der Spalte Serverstandort (D) in der Formel, dass das Format des CIDR-Bereichs für die On-Premises-Quelle für Ihren Bereich funktioni	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ert. Wenn Ihr CIDR-Bereich beispielsweise lautet`10.0.0.0/8` , geben Sie ein`10.*.*.*`. • Vergewissern Sie sich in der Spalte SFS location (E) in der Formel, dass das Format des CIDR-Bereichs für die Ziel-VPC für Ihren Bereich funktioniert. Wenn Ihr CIDR-Bereich beispiels weise lautet`176.16.0.0/16` , geben Sie ein`176.16.*.*` . 4. Gehen Sie auf dem SFS-Datenkollisor wie folgt vor: • Geben Sie in der Spalte Servername (A) den Namen des Servers ein, auf dem das SFS gemountet ist. • Geben Sie in der Spalte SFS-Pfad (B) den Namen des SFS ein. • Geben Sie in der Spalte IP-Adresse (C) die IP-Adresse des Servers ein. • Fügen Sie weitere relevante Informati onen hinzu, die Sie während der Erkennung gesammelt haben, z. B. den Mountingpunkt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und die SFS-Größe. Sie können diese Daten später verwenden, um die Berechnungen der Wave-Planung zu ändern. 5. Speichern Sie das Arbeitsbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen über die Server.	1. Identifizieren Sie mithilfe Ihrer CMDB oder der in Ihrem Migrationstool aufgezeichneten Daten alle folgenden Informationen zu den Servern mit SFS-Mounts: • Server name • IP-Adresse • Wave • Organisationseinheit (OU) • Serverumgebung, z. B. `DEVQA`, oder `PROD` • Anwendungsname • Anwendungseigentümer und Kontaktinformationen 2. Öffnen Sie die Datei SFS-Discovery-Workbook. 3. Geben Sie im Feld Server-Daten-Strahl in den Spalten A bis H die Informationen ein, die Sie über die Quellserver gesammelt haben. Beachten Sie Folgendes: • Geben Sie in der Spalte Wave #(C) den Wave-Namen (z. B. `Wave1`), out-of-scope (`OOS`) oder ein`Retire`.	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wenn die Spalte Kontakt des App-Besitzers (H) korrekt ist, überprüfen Sie, ob die E-Mail-Adresse korrekt ist. Diese E-Mail-Adresse wird automatisch auf der Grundlage des Namens generiert, den Sie in der Spalte App-Eigentümer (G) angegeben haben. Aktualisieren Sie bei Bedarf den Wert manuell, um die richtige E-Mail-Adresse widerzuspiegeln. • Ändern Sie nicht die Spalten I–J , die Formeln enthalten. 4. Speichern Sie das Arbeitsbuch.	

Plan

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SFS-Wellenplan.	1. Öffnen Sie die Datei SFS-Discovery-Workbook. 2. Überprüfen Sie, ob alle in der Erkennungsphase erfassten Informationen korrekt und aktuell sind. 3. Filtern Sie im Wave-Sheet-Koordinatenbereich die	Build-Verantwortlicher, Cutover-Verantwortlicher, Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Spalte SFS Wave (K) nach dem Wert 1. Dies ist eine Liste aller SFSs in der ersten Welle. Hinweis: Ein Wert von `0` in dieser Spalte gibt an, dass das SFS außerhalb des Umfangs der Migration liegt. Dies kann daran liegen, dass das SFS bereits auf AWS gehostet wird oder dass die Server, die auf die Freigabe zugreifen, nicht im Rahmen der Migration liegen. 4. Stellen Sie sicher, dass Sie diese SFSs in dieser Welle migrieren möchten. Weitere Informationen zum Zuweisen von SFSs zu Wellen finden Sie unter Wave-Planungsansätze im Abschnitt Bewährte Methoden. 5. Wählen Sie die Zellen aus, die die gefilterten Werte enthalten, und kopieren Sie sie. Kopieren Sie nicht die Kopfzeile, die die Spaltenti tel enthält. 6. Öffnen Sie die Datei SFS-Wave-Plan-Workbook, die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie zuvor heruntergeladen haben. 7. Wählen Sie im Abschnitt Exportieren aus Erkennung die Option Zelle A2 aus. 8. Fügen Sie die kopierten Daten ein. 9. Speichern Sie die Dateien SFS-Discovery-Workbook und SFS-Wave-Plan-Workbook.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den AWS-Ziels ervice und das Migrationstool aus.	1. Wählen Sie in der SFS-Wave-Plan-Workbook-Datei unter dem Ged-from-Discovery-Coordinate die Werte in der Spalte Alter Pfad (C) aus und kopieren Sie sie. 2. Wählen Sie in der Wave-Koordinate die Option cellA2 aus. 3. Fügen Sie die kopierten Daten ein. Die Spalten B–M in diesem Bildschir m werden automatisch aktualisiert, um andere Daten widerzuspiegeln, die diesem Pfad zugeordnet sind. 4. Entfernen Sie alle duplizier ten Werte in SpalteA . Anweisungen finden Sie unter Doppelte Werte entfernen (Microsoft Support-Website). 5. Überprüfen Sie in der Spalte Zielmuster oder Service (F) den empfohlen en AWS-Zielservice und aktualisieren Sie ihn nach Bedarf. Weitere Informati onen finden Sie unter Auswählen eines AWS-Dateisystemservices	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Abschnitt Bewährte Methoden dieses Musters. 6. Überprüfen Sie in der Spalte Migrationsmethode (G) das empfohlene Migrationstool und aktualisieren Sie es nach Bedarf. Weitere Informationen finden Sie unter Auswählen eines Migrationstools im Abschnitt Bewährte Methoden dieses Musters. 7. Speichern Sie die Datei SFS-Discovery-Workbook. Sie haben die Erstellung eines Wave-Plans für diese Wave abgeschlossen. 8. Wiederholen Sie diese Anweisungen, um einen Wave-Plan für jede Wave vorzubereiten. Da sich Wave-Pläne während der Migration ändern können, empfehlen wir Ihnen, nicht mehr als 5 Waves im Voraus zu planen.	

Vorbereitung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Zieldateisystem ein.	Richten Sie gemäß den in Ihrem Wave-Plan aufgezeichneten Details die Zieldatei	Migrationsingenieur, Migrationsleiter, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	systeme im AWS-Zielk onto, in der VPC und in den Subnetzen ein. Anweisungen finden Sie in der folgenden AWS-Dokumentation: • Amazon EFS • Amazon FSx für NetApp ONTAP • Amazon FSx für Windows File Server	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Migrationstool ein und übertragen Sie Daten.	1. Wenn Sie AWS verwenden DataSync, konfigurieren Sie die Protokollierung für DataSync Aufgaben. Anweisungen finden Sie unter Protokollieren Ihrer AWS- DataSync Aufgabenaktivitäten. 2. Richten Sie das Migration stool ein und führen Sie eine erste Datenübertragung gemäß den Anweisungen für das von Ihnen ausgewählte Tool durch: • Informationen zu Amazon EFS finden Sie hier: • Übertragen von Dateien zu Amazon EFS mit AWS DataSync • Informationen zu Amazon FSx für ONTAP finden Sie im Folgenden: • Migrieren zu FSx für ONTAP mit NetApp SnapMirror • Migrieren zu FSx für ONTAP mit AWS DataSync • Weitere Informationen zu Amazon FSx for Windows	AWS-Administrator, Cloud-Administrator, Migration singenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	File Server finden Sie im Folgenden: • Migrieren vorhandener Dateien zu FSx for Windows File Server mit AWS DataSync • Migrieren vorhandener Dateien zu FSx for Windows File Server mit Robocopy 3. Änderungen am Quell-SFS können während oder nach der ersten Übertragung auftreten. Richten Sie wiederkehrende Datenübertragungen zwischen dem Quell- und dem Zieldateisystem ein, um die Daten synchronisiert zu halten: • Wenn Sie verwenden DataSync, finden Sie weitere Informationen unter Planen Ihrer AWS-DataSync Aufgabe. DataSync überträgt nur die geänderten oder neuen Dateien im Quell-SFS. • Wenn Sie ein Drittanbieter-Tool verwenden, finden Sie weitere Informationen in der Dokumentation zu dem	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von Ihnen ausgewählten Tool.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den Wave-Plan.	1. Öffnen Sie die Datei SFS-Wave-Plan-Workbook für die aktuelle Welle. 2. Geben Sie in der Spalte Neue Pfad-IP-Adresse (N) in der Spalte Build-Wave-Coordinate die IP-Adresse des Zieldateisystems ein. Gehen Sie wie folgt vor, um die IP-Adresse zu finden: • Wählen Sie für FSx for Windows File Server in der Amazon-FSx-Konsole Dateisysteme aus, wählen Sie Ihr Dateisystem aus und zeigen Sie dann den Abschnitt Netzwerk und Sicherheit an. • Informationen zu FSx für ONTAP finden Sie unter Mounting von Volumes. • Informationen zu Amazon EFS finden Sie unter Mounting mit einer IP-Adresse . 3. Geben Sie in der Spalte Neuer Pfad (O) den neuen Mount-Pfad ein. Der Mount-Pfad ist der DNS-Name des Dateisystems. Führen Sie einen der folgenden Schritte	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus, um den Mount-Pfad zu finden: • Wählen Sie für FSx for Windows File Server in der Amazon-FSx-Konsole Dateisysteme, wählen Sie Ihr Dateisystem und dann Anfügen aus. • Informationen zu FSx für ONTAP finden Sie auf der Seite Dateisyst emdetails. Anweisungen finden Sie unter Mounting von Volumes. • Informationen zu Amazon EFS finden Sie unter Informationen sammeln. 4. Vergewissern Sie sich, dass die Spalten Neuer Pfad (C) und Neue Pfad-IP-Adresse (D) auf der Seite Remount-Summary die aktualisierten Werte widerspiegeln. 5. Vergewissern Sie sich, dass Ihre Organisation Runbooks für das erneute Mounten der Linux- und Windows-Dateisysteme nach dem Cutover vorbereitet hat. Allgemeine Anweisungen finden Sie hier: • Mounting von EFS-Dateisystemen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Zugreifen auf FSx for Windows File Server-Dateifreigaben • Mounten von FSx-für-ONTAP-Volumes 6. Wenn abhängige Server nicht in dieser Welle enthalten sind, notieren Sie sie im App-Team-Communication-Vorgang. Informieren Sie die jeweiligen Anwendungs- oder Serverbesitzer, da sie möglicherweise nicht in der Standard-Wave-Kommunikation enthalten sind. 7. Wenn SFSs nach Abschluss des Wave-Plans aus der Wave entfernt werden, verfolgen Sie diese auf dem GitLab.	

Cutover

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie Anwendungen.	Wenn Anwendungen oder Clients aktiv Lese- und Schreibvorgänge im Quell-SFS ausführen, halten Sie sie an, bevor Sie die endgültige Datensynchronisierung durchführen. Anweisungen	App-Besitzer, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der Anwendungsdokumentation oder Ihren internen Prozessen zum Stoppen von Lese- und Schreibaktivitäten. Weitere Informationen finden Sie unter Starten oder Stoppen des Webservers (IIS 8) (Microsoft-Dokumentation) oder Verwalten von Systemservices mit systemctl (Red-Hat-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die endgültige Datenübertragung durch.	1. Führen Sie im Migration stool manuell eine abschließende Datenüber tragungsaufgabe oder einen abschließenden Auftrag aus, um das Zieldatei system mit dem Quell-SFS zu synchronisieren. Anweisungen finden Sie unter Starten Ihrer DataSync Aufgabe oder in der Dokumentation zu Ihrem ausgewählten Drittanbieter-Migrationstool. 2. Warten Sie, bis die Datenübertragungsa ufgabe abgeschlossen ist. Weitere Informationen finden Sie unter AWS Überwachung der AWS-DataSync Aktivität mit Amazon CloudWatch und Überwachung Ihrer DataSync Aufgabe über die Befehlszeile .	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Datenübertragung.	Wenn Sie AWS verwenden DataSync, gehen Sie wie folgt vor, um zu überprüfen, ob die endgültige Datenübertragung erfolgreich abgeschlossen wurde: 1. Notieren Sie sich in der AWS- DataSync Konsole die Aufgaben- und Ausführungs-ID, z. B. `task-0000-exec-1111` . 2. Navigieren Sie zum Abschnitt Aufgabenprotokollierung der DataSync Aufgabe. 3. Wählen Sie den Link für die CloudWatch Protokollgruppe aus. 4. Suchen Sie in den Protokollen nach der Aufgaben- und Ausführungs-ID. 5. Notieren Sie sich alle Übertragungsfehler. Weitere Informationen finden Sie unter Häufige Fehler in der - DataSync Dokumentation. 6. Validieren Sie Folgendes: • Vergleichen Sie die Dateilisten aus den Quell- und Ziel-SFSs, um zu	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bestätigen, dass alle Daten übertragen wurden • Vergleichen Sie die Dateizugriffsberec htigungen zwischen den Quell- und Ziel-SFSs. Wenn Sie ein Drittanbieter-Tool verwenden, lesen Sie die Anweisungen zur Validieru ng der Datenübertragung in der Dokumentation für das ausgewählte Migrationstool.	

Validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Mounten Sie das Dateisyst em neu und überprüfen Sie die Anwendungsfunktion und -leistung.	1. Wenn abhängige Server in dieser Welle migriert wurden, geben Sie in der SFS-Wave-Plan-Work book-Datei im Remount-Summary-Remount-Summary-Wissenscha ftsprogramm die neue IP-Adresse des Servers in der Spalte Neue Server-IP-Adresse (F) ein. 2. Aktualisieren Sie auf allen Servern den Mountingp unkt für das Dateisyst em vom alten zum neuen Pfad. Verwenden Sie das	AWS-Systemadministrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Runbook Ihrer Organisation für das erneute Mounting, das zuvor in der Vorbereitungsphase besprochen wurde. 3. Vergewissern Sie sich, dass das Dateisystem ordnungsgemäß gemountet und zugänglich ist, indem Sie die Mounts überprüfen und überprüfen, ob Dateien vorhanden sind. Das Infrastrukturteam führt diese Aktivitäten in der Regel durch. 4. Starten Sie die Anwendungen neu und bitten Sie die Anwendungsbesitzer oder das QA-Team, Funktions- und Leistungstests für die Anwendung durchzuführen, je nach Bedarf für die Anwendung.	

Fehlerbehebung

Problem	Lösung
Zellenwerte in Microsoft Excel werden nicht aktualisiert.	Kopieren Sie die Formeln in den Beispielzeilen, indem Sie den Füllgriff ziehen. Weitere Informationen finden Sie in den Anweisungen für Windows oder Mac https://support.microsoft.com/en-au/office/copy-a-formula-by-dragging-the-fill-handle-in-excel-for-mac-

Problem	Lösung
	dd928259-622b-473f-9a33-83aa1a63e218 (Microsoft Support Website).

Zugehörige Ressourcen

AWS-Dokumentation

- AWS- DataSync Dokumentation
- Amazon-EFS-Dokumentation
- Amazon-FSx-Dokumentation
- Große Migrationen zur AWS Cloud
  - Leitfaden für große AWS-Migrationen
  - Portfolio-Playbook für große AWS-Migrationen

Fehlersuche

- Fehlerbehebung bei AWS- DataSync Problemen
- Fehlerbehebung bei Amazon EFS
- Fehlerbehebung bei Amazon FSx for Windows File Server
- Fehlerbehebung bei Amazon FSx für NetApp ONTAP

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren einer Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle GoldenGate Flat File Adaptern

Erstellt von Dhairya Jindani (AWS) und Bolji Shaik (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Eine Oracle-Datenbank (lokal oder auf einer EC2-Instance)	Ziel: Amazon RDS für Oracle
R-Typ: Plattformwechsel	Workload: Oracle	Technologien: Migration; Analytik; Datenbanken
AWS-Services: Amazon RDS		

Übersicht

Oracle GoldenGate ist ein Service zur Datenerfassung und Replikation in Echtzeit für heterogene Datenbanken und IT-Umgebungen. Dieser Service unterstützt jedoch derzeit nicht Amazon Relational Database Service (Amazon RDS) für Oracle. Eine Liste der unterstützten Datenbanken finden Sie unter Oracle GoldenGate für heterogene Datenbanken (Oracle-Dokumentation). Dieses Muster beschreibt, wie Sie flache Oracle- GoldenGate und Oracle- GoldenGate Dateiadapter verwenden, um flache Dateien aus der Oracle-Quelldatenbank zu generieren, die On-Premises oder auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance sein können. Anschließend können Sie diese flachen Dateien in eine Datenbank-Instance von Amazon RDS für Oracle importieren.

In diesem Muster verwenden Sie Oracle, GoldenGate um die Trail-Dateien aus Ihrer Oracle-Quelldatenbank zu extrahieren. Die Datenkopie kopiert die Trail-Dateien auf einen Integrationsserver, bei dem es sich um eine EC2-Instance handelt. Auf dem Integrationsserver GoldenGate verwendet Oracle den flachen Dateiadapter, um eine Reihe sequenzieller flacher Dateien basierend auf der transationalen Datenerfassung der Trail-Dateien zu generieren. Oracle GoldenGate formatiert die Daten entweder als durch Trennzeichen getrennte Werte oder als durch Längen getrennte Werte. Anschließend verwenden Sie Oracle SQL*Loader, um die flachen Dateien in die Zieldatenbank-Instance von Amazon RDS für Oracle zu importieren.

Zielgruppe

Dieses Muster richtet sich an diejenigen, die Erfahrung mit und Kenntnisse der GoldenGateGrundbausteine eines Oracle- haben. Weitere Informationen finden Sie unter Übersicht über die Oracle- GoldenGate Architektur (Oracle-Dokumentation).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto.
- Eine Oracle- GoldenGate Lizenz.
- Eine separate Lizenz für einen Oracle- GoldenGate Adapter.
- Eine Oracle-Quelldatenbank, die entweder On-Premises oder auf einer EC2-Instance ausgeführt wird.
- Eine EC2-Linux-Instance, die als Integrationsserver verwendet wird. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2-Linux-Instances (Amazon EC2Dokumentation).
- Eine Ziel-Datenbank-Instance von Amazon RDS für Oracle. Weitere Informationen finden Sie unter Erstellen einer Oracle-DB-Instance (Amazon-RDS-Dokumentation).

Produktversionen

- Oracle Database Enterprise Edition Version 10g, 11g, 12c oder höher
- Oracle GoldenGate Version 12.2.0.1.1 oder höher

Architektur

Quelltechnologie-Stack

Eine Oracle-Datenbank (lokal oder auf einer EC2-Instance)

Zieltechnologie-Stack

Amazon RDS für Oracle

Quell- und Zielarchitektur

1. Oracle GoldenGate extrahiert Trails aus den Quelldatenbankprotokollen.

2. Der Datenstrom extrahiert die Trails und migriert sie zu einem Integrationsserver.
3. Der GoldenGate flache Oracle-Dateiadapter liest die Trails, Quelldefinitionen und extrahiert Parameter.
4. Sie beenden die Extraktion, wodurch eine Kontrolldatei und flache Datendateien generiert werden.
5. Sie migrieren die flachen Datendateien zu einer Datenbank-Instance von Amazon RDS für Oracle in der AWS Cloud.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) for Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS Cloud.

Andere -Services

- Oracle GoldenGate ist ein Service, der Ihnen hilft, Daten von einer Datenbank in eine andere heterogene Datenbank oder in eine andere Zieltopologie wie flache Dateien zu replizieren, zu filtern und umzuwandeln.
- Mit Oracle- GoldenGate Anwendungsadaptern kann Oracle eine Reihe von sequenziellen flachen Dateien GoldenGate erstellen und Dateien aus Transaktionsdaten steuern, die in den Trail-Dateien einer Quelldatenbank erfasst wurden. Diese Adapter werden häufig für ETL-Operationen (Extract, Transform, Load) in Data-Warehouse-Anwendungen und proprietären oder Legacy-Anwendungen verwendet. Oracle GoldenGate führt diese Erfassung durch und wendet sie nahezu in Echtzeit auf heterogene Datenbanken, Plattformen und Betriebssysteme an. Die Adapter unterstützen verschiedene Formate für die Ausgabedateien, z. B. CSV oder Apache Parquet. Sie können diese generierten Dateien laden, um die Daten in verschiedene heterogene Datenbanken zu laden.

Polen

Einrichten von Oracle GoldenGate auf dem Quelldatenbankserver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Oracle herunter GoldenGate.	Laden Sie auf dem Quelldatenbankserver Oracle GoldenGate Version 12.2.0.1.1 oder höher herunter. Anweisungen finden Sie unter Herunterladen von Oracle GoldenGate (Oracle-Dokumentation).	DBA
Installieren Sie Oracle GoldenGate.	Anweisungen finden Sie unter Installieren von Oracle GoldenGate (Oracle-Dokumentation).	DBA
Richten Sie Oracle ein GoldenGate.	Anweisungen finden Sie unter Vorbereiten der Datenbank für Oracle GoldenGate (Oracle-Dokumentation).	DBA

Einrichten von Oracle GoldenGate auf dem Integrationsserver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Oracle herunter GoldenGate.	Laden Sie auf dem Integrationsserver Oracle GoldenGate Version 12.2.0.1.1 oder höher herunter. Anweisungen finden Sie unter Herunterladen von Oracle GoldenGate (Oracle-Dokumentation).	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle GoldenGate.	Erstellen Sie Verzeichnisse, richten Sie den Managerprozess ein und erstellen Sie die `defgen` Datei für eine heterogene Umgebung. Anweisungen finden Sie unter Installieren von Oracle GoldenGate (Oracle-Dokumentation).	DBA

Ändern der Oracle- GoldenGate Datenerfassungskonfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Oracle-GoldenGate Adapter vor.	Richten Sie auf dem Integrationsserver die Oracle-GoldenGate Adaptersoftware ein. Gehen Sie wie folgt vor: 1. Laden Sie von Oracle Software Delivery Cloud ggs_Adapters_Linux_x64.zip herunter. 2. Entpacken Sie ggs_Adapters_Linux_x64.zip . 3. Führen Sie den folgenden Befehl aus, um die Adapter zu installieren. `tar -xvf ggs_Adapters_Linux_x64.tar`	DBA
Konfigurieren Sie die Datenmenge.	Konfigurieren Sie auf dem Quellserver den Datenstro	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	m, um die Trail-Datei vom Quellserver auf den Integrati onsserver zu übertragen. Erstellen Sie das Dateiverz eichnis für die Parameter datei und die Trails-Datei. Anweisungen finden Sie unter Konfigurieren des Flat File Adapters (Oracle-Dokumentat ion).	

Generieren und Migrieren der flachen Dateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die flachen Dateien.	Erstellen Sie die Extract-D atei und die Control-Datei und starten Sie dann den Extraktio nsprozess auf dem Integrati onsserver. Dadurch werden die Datenbankänderungen extrahiert und die Quelldate nbank in die flachen Dateien geschrieben. Anweisungen finden Sie unter Verwenden des Flat File Adapters (Oracle-Dokumentation).	DBA
Laden Sie die flachen Dateien in die Zieldatenbank.	Laden Sie die flachen Dateien in die Zieldatenbank-Instance von Amazon RDS für Oracle. Weitere Informationen finden Sie unter Importieren mit	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Oracle SQL*Loader (Amazon-RDS-Dokumentation).	

Fehlerbehebung

Problem	Lösung
Der GoldenGate flache Oracle-Dateiadapter generiert einen Fehler.	Eine Beschreibung der Adapterfehler finden Sie unter Auffinden von Fehlermeldungen (Oracle-Dokumentation). Anweisungen zur Fehlerbeh ebung finden Sie unter Fehlerbehebung beim Flat File Adapter (Oracle-Dokumentation).

Zugehörige Ressourcen

- Installieren von Oracle GoldenGate (Oracle-Dokumentation)
- Konfigurieren von Oracle GoldenGate (Oracle-Dokumentation)
- Grundlegendes zu Oracle GoldenGate Adapters (Oracle-Dokumentation)
- Konfigurieren des Flat File Adapters (Oracle-Dokumentation)

Ändern von Python- und Perl-Anwendungen zur Unterstützung der Datenbankmigration von Microsoft SQL Server zu Amazon Aurora PostgreSQL – Kompatible Edition

Erstellt von Dwarika Patra (AWS) und Deepesh Jaya Prakash (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: SQL Server	Ziel: Aurora PostgreSQL – kompatibel
R-Typ: Plattformwechsel	Workload: Microsoft; Open-Source	Technologien: Migration; Datenbanken
AWS-Services: Amazon Aurora		

Übersicht

Dieses Muster beschreibt Änderungen an Anwendungs-Repositorys, die möglicherweise erforderlich sind, wenn Sie Datenbanken von Microsoft SQL Server zu Amazon Aurora PostgreSQL -kompatible Edition migrieren. Das Muster geht davon aus, dass diese Anwendungen Python- oder Perl-basiert sind, und enthält separate Anweisungen für diese Skriptsprachen.

Die Migration von SQL Server-Datenbanken zu Aurora PostgreSQL – kompatibel umfasst Schemakonvertierung, Datenbankobjektkonvertierung, Datenmigration und Datenladevorgänge. Aufgrund der Unterschiede zwischen PostgreSQL und SQL Server (in Bezug auf Datentypen, Verbindungsobjekte, Syntax und Logik) besteht die schwierigste Migrationsaufgabe darin, die erforderlichen Änderungen an der Codebasis vorzunehmen, damit sie mit PostgreSQL ordnungsgemäß funktioniert.

Bei einer Python-basierten Anwendung sind Verbindungsobjekte und Klassen im gesamten System verteilt. Außerdem verwendet die Python-Codebasis möglicherweise mehrere Bibliotheken, um eine Verbindung mit der Datenbank herzustellen. Wenn sich die Datenbankverbindungsschnittstelle ändert, erfordern die Objekte, die die Inline-Abfragen der Anwendung ausführen, ebenfalls Änderungen.

Bei einer Perl-basierten Anwendung umfassen Änderungen Verbindungsobjekte, Datenbankverbindungstreiber, statische und dynamische Inline-SQL-Anweisungen und die Art und Weise, wie die Anwendung komplexe dynamische DML-Abfragen und Ergebnissätze verarbeitet.

Wenn Sie Ihre Anwendung migrieren, können Sie auch mögliche Verbesserungen in AWS berücksichtigen, z. B. den FTP-Server durch Amazon Simple Storage Service (Amazon S3)-Zugriff zu ersetzen.

Der Prozess der Anwendungsmigration beinhaltet die folgenden Herausforderungen:

- Verbindungsobjekte. Wenn Verbindungsobjekte im Code mit mehreren Bibliotheken und Funktionsaufrufen verteilt sind, müssen Sie möglicherweise eine verallgemeinerte Möglichkeit finden, sie zur Unterstützung von PostgreSQL zu ändern.
- Fehler- oder Ausnahmebehandlung beim Abrufen oder Aktualisieren von Datensätzen. Wenn Sie über bedingte CRUD-Operationen (Create, Read, Update, Delete) in der Datenbank verfügen, die Variablen, Ergebnissätze oder Datenframes zurückgeben, können Fehler oder Ausnahmen zu Anwendungsfehlern mit kaskadierenden Auswirkungen führen. Diese sollten mit geeigneten Validierungen und Speicherpunkten sorgfältig behandelt werden. Ein solcher Save Point besteht darin, große Inline-SQL-Abfragen oder Datenbankobjekte in `BEGIN...EXCEPTION...END`Blöcken aufzurufen.
- Steuern von Transaktionen und deren Validierung. Dazu gehören manuelle und automatische Commits und Rollbacks. Der PostgreSQL-Treiber für Perl erfordert, dass Sie das Auto-Commit-Attribut immer explizit festlegen.
- Umgang mit dynamischen SQL-Abfragen. Dies erfordert ein starkes Verständnis der Abfragelogik und iterative Tests, um sicherzustellen, dass Abfragen wie erwartet funktionieren.
- Leistung. Sie sollten sicherstellen, dass Codeänderungen nicht zu einer Verschlechterung der Anwendungsleistung führen.

Dieses Muster erklärt den Konvertierungsprozess im Detail.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Funktionierende Kenntnisse der Python- und Perl-Syntax.
- Grundlegende Fähigkeiten in SQL Server und PostgreSQL .
- Grundlegendes zu Ihrer vorhandenen Anwendungsarchitektur.

- Zugriff auf Ihren Anwendungscode, Ihre SQL Server-Datenbank und Ihre PostgreSQL-Datenbank.
- Zugriff auf Windows oder Linux (oder eine andere Unix)-Entwicklungsumgebung mit Anmeldeinformationen für die Entwicklung, das Testen und die Validierung von Anwendungsänderungen.
- Für eine Python-basierte Anwendung Python-Standardbibliotheken, die Ihre Anwendung möglicherweise benötigt, z. B. Pandas zur Verarbeitung von Datenframes und psycopg2 oder SQLAlchemy für Datenbankverbindungen.
- Für eine Perl-basierte Anwendung erforderliche Perl-Pakete mit abhängigen Bibliotheken oder Modulen. Das microSD Perl Archive Network (CPAN)-Modul kann die meisten Anwendungsanforderungen unterstützen.
- Alle erforderlichen abhängigen benutzerdefinierten Bibliotheken oder Module.
- Datenbankanmeldeinformationen für den Lesezugriff auf SQL Server und den Lese-/Schreibzugriff auf Aurora.
- PostgreSQL zum Validieren und Debuggen von Anwendungsänderungen mit -Services und -Benutzern.
- Zugriff auf Entwicklungstools während der Anwendungsmigration wie Visual Studio Code, Sublime Text oder pgAdmin.

Einschränkungen

- Einige Python- oder Perl-Versionen, Module, Bibliotheken und Pakete sind nicht mit der Cloud-Umgebung kompatibel.
- Einige Bibliotheken und Frameworks von Drittanbietern, die für SQL Server verwendet werden, können nicht ersetzt werden, um die PostgreSQL-Migration zu unterstützen.
- Leistungsschwankungen erfordern möglicherweise Änderungen an Ihrer Anwendung, an Inline-Transact-SQL (T-SQL)-Abfragen, Datenbankfunktionen und gespeicherten Prozeduren.
- PostgreSQL unterstützt Kleinbuchstabennamen für Tabellennamen, Spaltennamen und andere Datenbankobjekte.
- Einige Datentypen, wie UUID-Spalten, werden nur in Kleinbuchstaben gespeichert. Python- und Perl-Anwendungen müssen solche Fallunterschiede verarbeiten.
- Unterschiede bei der Zeichenkodierung müssen mit dem richtigen Datentyp für die entsprechenden Textspalten in der PostgreSQL-Datenbank behandelt werden.

Produktversionen

- Python 3.6 oder höher (verwenden Sie die Version, die Ihr Betriebssystem unterstützt)
- Perl 5.8.3 oder höher (verwenden Sie die -Version, die Ihr Betriebssystem unterstützt)
- Aurora PostgreSQL – Kompatible Edition 4.2 oder höher (siehe Details)

Architektur

Quelltechnologie-Stack

- Scripting-Sprache (Anwendungsprogrammierung): Python 2.7 oder höher oder Perl 5.8
- Datenbank: Microsoft SQL Server Version 13
- Betriebssystem: Red Hat Enterprise Linux (RHEL) 7

Zieltechnologie-Stack

- Scripting-Sprache (Anwendungsprogrammierung): Python 3.6 oder höher oder Perl 5.8 oder höher
- Datenbank: Aurora PostgreSQL – kompatibel mit 4.2
- Betriebssystem: RHEL 7

Migrationsarchitektur

Tools

AWS-Services und -Tools

- Aurora PostgreSQL – Compatible Edition ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-kompatible relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Kosteneffizienz von Open-Source-Datenbanken kombiniert. Aurora PostgreSQL ist ein Drop-In-Ersatz für PostgreSQL und erleichtert und kostengünstiger das Einrichten, Betreiben und Skalieren Ihrer neuen und vorhandenen PostgreSQL-Bereitstellungen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere Tools

- Python- und PostgresSQL-Datenbankverbindungsbibliotheken wie psycopg2 und SQLAlchemy
- Perl und seine DBI-Module
- Interaktives PostgreSQL-Terminal (psql)

Polen

Migrieren Ihres Anwendungs-Repositorys zu PostgreSQL – allgemeine Schritte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie wie folgt vor, um Ihre Anwendung zu PostgreSQL zu migrieren.	1. Legen Sie datenbank spezifische ODBC-Trei ber und Bibliotheken für PostgreSQL fest. Sie können beispielsweise eines der CPAN-Modu le für Perl und Pyodbc , psycopg2 oder SQLAlchem y für Python verwenden. 2. Konvertieren Sie Datenbank objekte, indem Sie diese Bibliotheken verwenden , um eine Verbindung zu Aurora PostgreSQL herzustellen – kompatibel. 3. Wenden Sie Codeänder ungen in vorhandenen Anwendungsmodulen an, um kompatible T-SQL-Anw eisungen abzurufen. 4. Schreiben Sie datenbank spezifische Funktions aufrufe und gespeicherte Prozeduren in Anwendung scode um.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Behandeln Sie Änderungen an den Variablen Ihrer Anwendung und ihren Datentypen, die für Inline-SQL-Abfragen verwendet werden. 6. Verarbeiten Sie inkompatible datenbankspezifische Funktionen. 7. Schließen Sie den end-to-end Test des konvertierten Anwendungscodes für die Datenbankmigration ab. 8. Vergleichen Sie die Ergebnisse von Microsoft SQL Server mit der Anwendung, die Sie zu PostgreSQL migriert haben. 9. Führen Sie Benchmarking der Anwendungsleistung zwischen Microsoft SQL Server und PostgreSQL durch. 10. Überarbeiten Sie gespeicherte Prozeduren oder Inline-T-SQL-Anweisungen, die von der Anwendung aufgerufen werden, um die Leistung zu verbessern. Die folgenden Abschnitte enthalten detaillierte Anweisungen für einige dieser	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konvertierungsaufgaben für Python- und Perl-Anwendungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie für jeden Schritt der Migration eine Checkliste.	Fügen Sie Ihrer Checkliste für jeden Schritt der Anwendung smigration, einschließlich des letzten Schritts, Folgendes hinzu: • Lesen Sie die PostgreSQ L-Dokumentation, um sicherzustellen, dass alle Ihre Änderungen mit dem PostgreSQL-Standard kompatibel sind. • Suchen Sie nach Ganzzahl- und Gleitkommawerten für Spalten. • Identifizieren Sie die Anzahl der eingefügten, aktualisi erten und extrahierten Zeilen zusammen mit den Spaltennamen und Datums-/Uhrzeitstempeln. Sie können ein Diff-Dien stprogramm verwenden oder ein Skript schreiben , um diese Prüfungen zu automatisieren. • Führen Sie Leistungs prüfungen für große Inline-SQL-Anweisungen durch und überprüfen Sie die Gesamtleistung der Anwendung. • Überprüfen Sie, ob die Fehlerbehandlung für	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datenbankoperationen korrekt ist und ob das Programm ordnungsgemäß beendet wurde, indem Sie mehrere Try/Catch-Blöcke verwenden. • Überprüfen Sie, ob die richtigen Protokollierungspr ozesse vorhanden sind.	

Analysieren und Aktualisieren Ihrer Anwendung – Python-Codebasis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Ihre vorhandene Python-Co debasis.	Ihre Analyse sollte Folgendes beinhalten, um den Prozess der Anwendungsmigration zu erleichtern: • Identifizieren Sie alle Verbindungsobjekte im Code. • Identifizieren Sie alle inkompatiblen Inline-SQL-Abfragen (wie T-SQL-Anw eisungen und gespeicherte Prozeduren) und analysier en Sie die erforderlichen Änderungen. • Lesen Sie die Dokumenta tion für Ihren Code und verfolgen Sie den Kontrolla blauf, um die Code-Funk tionalität zu verstehen. Dies	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird später hilfreich sein, wenn Sie die Anwendung auf Leistungs- oder Lastvergleiche testen. • Machen Sie sich mit dem Zweck der Anwendung vertraut, damit Sie sie nach der Datenbank konvertierung effektiv testen können. Die meisten Python-Anwendungen, die für die Konvertierung mit Datenbankmigration en in Frage kommen, sind entweder Feeds, die Daten aus anderen Quellen in Datenbanktabellen laden, oder Extraktoren, die Daten aus den Tabellen abrufen und sie in verschied ene Ausgabeformate umwandeln (z. B. CSV-, JSON- oder flache Dateien), die für die Erstellung von Berichten oder für API-Aufrufe zur Durchführung von Validierungen geeignet sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konvertieren Sie Ihre Datenbankverbindungen zur Unterstützung von PostgreSQL .	Die meisten Python-Anwendungen verwenden die Pyodbc-Bibliothek, um wie folgt eine Verbindung zu SQL Server-Datenbanken herzustellen.
	
	`import pyodbc`
	`....`
	`try:`
	`conn_string = "Driver=ODBC Driver 17 for SQL Server;UID={};PWD={};Server={};Database={}".format (conn_user, conn_password, conn_server, conn_database)`
	`conn = pyodbc.connect(conn_string)`
	`cur = conn.cursor()`
	`result = cur.execute(query_string)`
	`for row in result:`
	`print (row)`
	`except Exception as e:`
	`print(str(e))`
	
	Konvertieren Sie die Datenbankverbindung wie folgt, um PostgreSQL zu unterstützen.
	
	`import pyodbc`
	`import psycopg2`
	`....`
	`try:`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> conn_string =
	 'postgresql+psycop
	g2://'+
	    conn_user+':'+conn
	_password+'@'+conn
	_server+'/'+conn_d
	atabase
	    conn = pyodbc.co
	nnect(conn_string,
	 connect_args={'opt
	ions':'-csearch_pa
	th=dbo'})
	    cur = conn.cursor()
	    result = cur.execu
	te(query_string)
	    for row in result:
	    print (row)
	except Exception as e:
	    print(str(e))</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie Inline-SQL-Abfragen in PostgreSQL .	Konvertieren Sie Ihre Inline-SQL-Abfragen in ein PostgreSQL-kompatibles Format. Die folgende SQL Server-Abfrage ruft beispiels weise eine Zeichenfolge aus einer Tabelle ab. `dtype = “type1” stm = ‘“SELECT TOP 1 searchcode FROM TypesTable (NOLOCK) WHERE code=”’ + “’” + str(dtype) + “’” # For Microsoft SQL Server Database Connection engine = create_en gine(‘mssql+pyodbc :///?odbc_connect=%s’ % urllib.parse.quote _plus(conn_string) , connect_args={‘con nect_timeout’:logi n_timeout}) conn = engine_connect() rs = conn.execute(stm) for row in rs: print(row)`  Nach der Konvertierung sieht die PostgreSQL-kompatible Inline-SQL-Abfrage wie folgt aus.  `dtype = “type1”`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`stm = '"SELECT searchcode FROM TypesTable WHERE code="' + "'" + str(dtype) + "' LIMIT 1"`
	`# For PostgreSQL Database Connection`
	`engine = create_engine('postgres+psycopg2://%s' %conn_string, connect_args={'connect_timeout':login_timeout})`
	`conn = engine.connect()`
	`rs = conn.execute(stm)`
	`for row in rs:`
	`  print(row)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Verarbeiten Sie dynamische SQL-Abfragen.	Dynamisches SQL kann in einem Skript oder in mehreren Python-Skripten vorhanden sein. In früheren Beispiele n wurde gezeigt, wie die Zeichenfolgenersetzungsfunk tion von Python verwendet wird, um Variablen zum Erstellen dynamischer SQL-Abfragen einzufügen. Ein alternativer Ansatz besteht darin, die Abfragezeichenfolge gegebenenfalls mit Variablen anzuhängen.
	
	Im folgenden Beispiel wird die Abfragezeichenfolge im laufenden Betrieb basierend auf den von einer Funktion zurückgegebenen Werten erstellt.
	
	`query = '"SELECT id from equity e join issues i on e.permId=i.permId where e.id'"`
	`query += get_id_filter(ids) + " e.id is NOT NULL`
	
	Diese Arten dynamischer Abfragen sind während der Anwendungsmigration sehr häufig. Gehen Sie wie folgt vor, um dynamische Abfragen zu verarbeiten:
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Überprüfen Sie die Gesamtsyntax (z. B. die Syntax für die `SELECT` Anweisung mit einer `JOIN` -Klausel). • Überprüfen Sie alle Variablen oder Spaltennamen, die in der Abfrage verwendet werden, z. B. `i` und `id`. • Überprüfen Sie die Funktionen, Argumente und Rückgabewerte, die in der Abfrage verwendet werden (z. B. `get_id_filter` und ihr Argument `ids`).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Behandlung von Ergebnissätzen, Variablen und Datenframes.	Für Microsoft SQL Server verwenden Sie Python-Methoden wie `fetchone()` oder , `fetchall()` um den Ergebnissatz aus der Datenbank abzurufen. Sie können auch verwenden `fetchmany(size)` und die Anzahl der Datensätze angeben, die aus dem Ergebnissatz zurückgegeben werden sollen. Dazu können Sie das Pyodbc-Verbindungsobjekt verwenden, wie im folgenden Beispiel gezeigt.
	
	pyodbc (Microsoft SQL Server)
	
	`import pyodbc`
	`server = 'tcp:myserver.database.windows.net'`
	`database = 'exampledb'`
	`username = 'exampleusername'`
	`password = 'examplepassword'`
	`conn = pyodbc.connect('DRIVER={ODBC Driver 17 for SQL Server};SERVER='+server+';DATABASE='+database+';UID='+username+';PWD='+ password)`
	`cursor = conn.cursor()`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cursor.execute("SELECT * FROM ITEMS")`
	`row = cursor.fetchone()`
	`while row:`
	`  print(row[0])`
	`  row = cursor.fetchone()`	

	Um in Aurora ähnliche Aufgaben wie das Herstellen einer Verbindung mit PostgreSQL und das Abrufen von Ergebnissätzen auszuführen, können Sie entweder psycopg2 oder SQLAlchemy verwenden. Diese Python-Bibliotheken stellen das Verbindungsmodul und das Cursor-Objekt bereit, die durch die PostgreSQL-Datenbankdatensätze durchquert werden sollen, wie im folgenden Beispiel gezeigt.
	
	psycopg2 (Aurora PostgreSQL – kompatibel)
	
	`import psycopg2`
	`query = "SELECT * FROM ITEMS;"`
	`//Initialize variables`
	`host=dbname=user=password=port=sslmode=connect_timeout=""`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`connstring = "host='{h ost}' dbname='{ dbname}' user='{user}' \ password='{passw ord}'port='{port}' ".format(host=host ,dbname=dbname,\ user=user,password= password,port=port) conn = psycopg2. connect(connstring) cursor = conn.cursor() cursor.execute(query) column_names = [column[0] for column in cursor.description] print("Column Names: ", column_names) print("Column values: " for row in cursor: print("itemid :", row[0]) print("itemdescrpt ion :", row[1]) print("it emprice :", row[3]))`  SQLAlchemy (Aurora PostgreSQL – kompatibel)  `from sqlalchemy import create_engine from pandas import DataFrame conn_string = 'postgres ql://core:database @localhost:5432/ex ampledatabase'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`engine = create_en gine(conn_string) conn = engine.co nnect() dataid = 1001 result = conn.exec ute("SELECT * FROM ITEMS") df = DataFrame (result.fetchall()) df.columns = result.ke ys() df = pd.DataFrame() engine.connect() df = pd.read_sql_query(sql_query, engine, coerce_float=False) print(“df=”, df)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihre Anwendung während und nach der Migration.	Das Testen der migrierten Python-Anwendung ist ein fortlaufender Prozess. Da die Migration Änderunge n an Verbindungsobjekten (psycopg2 oder SQLAlchem y Fehlerbehandlung, neue Features (Datenframes), Inline-SQL-Änderungen, Massenkopierfunktionen (`bcp`anstelle von `COPY`) und ähnliche Änderungen umfasst, muss sie während und nach der Anwendungsmigration sorgfältig getestet werden. Überprüfen Sie Folgendes: • Fehlerbedingungen und Handhabung • Alle Datensatzkonflikte nach der Migration • Aktualisierungen oder Löschungen von Datensätz en • Zeit, die zum Ausführen der Anwendung benötigt wird	App-Developer

Analysieren und Aktualisieren Ihrer Anwendung – Perl-Codebasis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Ihre vorhandene Perl-Codebasis.	Ihre Analyse sollte Folgendes beinhalten, um den Prozess der Anwendungsmigration	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zu erleichtern. Sie sollten Folgendes identifizieren: • INI- oder konfigurationsbasierter Code • Datenbankspezifische Open Database Connectivity (ODBC)-Standardtreiber oder benutzerdefinierte Treiber • Codeänderungen, die für Inline- und T-SQL-Abfragen erforderlich sind • Interaktionen zwischen verschiedenen Perl-Modulen (z. B. ein einzelnes Perl-ODBC-Verbindungsobjekt, das von mehreren Funktionskomponenten aufgerufen oder verwendet wird) • Umgang mit Datensätzen und Ergebnissätzen • Externe, abhängige Perl-Bibliotheken • Alle APIs, die in der Anwendung verwendet werden • Perl-Versions- und Treiberkompatibilität mit Aurora PostgreSQL – kompatibel	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konvertieren Sie die Verbindungen aus der Perl-Anwendung und dem DBI-Modul, um PostgreSQL zu unterstützen.	Perl-basierte Anwendungen verwenden im Allgemeinen das Perl-DBI-Modul, ein Standard-Datenbankzugriffsmodul für die Programmiersprache Perl. Sie können dasselbe DBI-Modul mit unterschiedlichen Treibern für SQL Server und PostgreSQL verwenden.
	
	Weitere Informationen zu erforderlichen Perl-Modulen, Installationen und anderen Anweisungen finden Sie in der DBD::Pg-Dokumentation. Im folgenden Beispiel wird eine Verbindung zu Aurora PostgreSQL hergestellt – kompatibel unter `examplete st-aurorapg-databa se.cluster-samplec lusture.us-east-.r ds.amazonaws.com` .
	
	`#!/usr/bin/perl`
	`use DBI;`
	`use strict;`
	`my $driver = "Pg";`
	`my $hostname = “examplet`
	`est-aurorapg-datab`
	`ase-sampleclusture`
	`.us-east.rds.amazo`
	`naws.com”`
	`my $dsn = "DBI:$driver:`
	` dbname = $hostname`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	;host = 127.0.0.1;port = 5432"; my $username = "postgres"; my $password = "pass123"; $dbh = DBI->connect("dbi:Pg:dbname=$hostname;host=$host;port=$port;options=$options", $username, $password, {AutoCommit => 0, RaiseError => 1, PrintError => 0});	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie Inline-SQL-Abfragen in PostgreSQL .	Ihre Anwendung verfügt möglicherweise über Inline-SQL-Abfragen mit `SELECT`, `DELETEUPDATE`, und ähnlichen Anweisungen, die Abfrageklauseln enthalten, die PostgreSQL nicht unterstüt zt. Abfrageschlüsselwö rter wie `TOP` und `NOLOCK` werden beispielsweise in PostgreSQL nicht unterstüt zt. Die folgenden Beispiele zeigen, wie Sie `TOP-NOLOCK`, - und boolesche Variablen behandeln können.
	
	In SQL Server:
	
	`$sqlStr = $sqlStr . "WHERE a.student _id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_rec ord b WITH (NOLOCK) \ INNER JOIN student_c ontributor c WITH (NOLOCK) on c.contrib utor_id = b.c_st)`
	
	Konvertieren Sie für PostgreSQL in:
	
	`$sqlStr = $sqlStr . "WHERE a.student _id in (SELECT`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	TOP $numofRecords c_student_id \ FROM active_student_rec ord b INNER JOIN student_contributor c \ on c.contributor_id = b.c_student_contr_id WHERE b_current_1 is true \ LIMIT $numofRecords)"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verarbeiten Sie dynamische SQL-Abfragen und Perl-Variablen.	Dynamische SQL-Abfragen sind SQL-Anweisungen, die zur Anwendungslaufzeit erstellt werden. Diese Abfragen werden dynamisch erstellt, wenn die Anwendung ausgeführt wird, abhängig von bestimmten Bedingungen, sodass der vollständige Text der Abfrage erst zur Laufzeit bekannt ist. Ein Beispiel ist eine Finanzanalyseanwendung, die täglich die 10 wichtigsten Anteile analysiert und sich jeden Tag ändert. Die SQL-Tabellen werden auf der Grundlage der Top-Leistungsersteller erstellt, und die Werte sind bis zur Laufzeit nicht bekannt. Angenommen, die Inline-SQL-Abfragen für dieses Beispiel werden an eine Wrapper-Funktion übergeben, um die Ergebnisse in einer Variablen abzurufen, und dann verwendet eine Variable eine Bedingung, um zu bestimmen, ob die Tabelle vorhanden ist: • Wenn die Tabelle vorhanden ist, erstellen Sie sie nicht. Führen Sie eine gewisse Verarbeitung durch.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Wenn die Tabelle nicht vorhanden ist, erstellen Sie die Tabelle und führen Sie auch eine gewisse Verarbeitung durch.
	
	Im Folgenden finden Sie ein Beispiel für die variable Behandlung, gefolgt von den SQL Server- und PostgreSQL-Abfragen für diesen Anwendungsfall.
	
	`my $tableexists = db_read( arg 1, $sql_qry, undef, 'writer'); my $table_already_exists = $tableexists->[0]{table_exists}; if ($table_already_exists){ # do some thing } else { # do something else }`
	
	SQL Server:
	
	`my $sql_qry = “SELECT OBJECT_ID('$backendTable', 'U') table_exists", undef, 'writer') ";`
	
	PostgreSQL:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`my $sql_qry = “SELECT TO_REGCLASS('$backendTable', 'U') table_exists", undef, 'writer')";`
	
	Im folgenden Beispiel wird eine Perl-Variable in Inline-SQL verwendet, die eine -`SELECT`Anweisung mit einem ausführt, `JOIN`um den Primärschlüssel der Tabelle und Position der Schlüssel spalte abzurufen.
	
	SQL Server:
	
	`my $sql_qry = "SELECT column_name', character_maximum_length \ FROM INFORMATION_SCHEMA.COLUMNS \ WHERE TABLE_SCHEMA='$example_scheMaInfo' \ AND TABLE_NAME='$example_table' \ AND DATA_TYPE IN ('varchar','nvarchar');";`
	
	PostgreSQL:
	
	`my $sql_qry = "SELECT c1.column_name, c1.ordinal_position \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`FROM information_schema .key_column_usage AS c LEFT \ JOIN information_schema .table_constraints AS t1 \ ON t1.constraint_name = c1.constraint_name \ WHERE t1.table_name = $example_schemaInf o'.'$example_table' \ AND t1.constraint_type = 'PRIMARY KEY' ;";`	

Nehmen Sie zusätzliche Änderungen an Ihrer Perl-basierten oder Python-basierten Anwendung vor, um PostgreSQL zu unterstützen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie zusätzlic he SQL Server-Konstrukte in PostgreSQL .	Die folgenden Änderungen gelten für alle Anwendung en, unabhängig von der Programmiersprache. • Qualifizieren Sie Datenbank objekte, die Ihre Anwendung verwendet, mit neuen und geeigneten Schemanamen. • Verarbeiten Sie LIKE-Operatoren für den Abgleich unter Berücksichtigung der Groß- und Kleinschreibung mit der Sortierfunktion in PostgreSQL . • Verarbeiten Sie nicht unterstützte datenbank	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	spezifische Funktione n wie `DATEDIFF`, `DATEADD`, `CONVERT`, und `GETDATE-CAST`Operatoren. Entsprechende PostgreSQ L-kompatible Funktionen finden Sie unterNative oder integrierte SQL-Funktionen im Abschnitt Zusätzliche Informationen. • Verarbeiten Sie boolesche Werte in Vergleich sanweisungen. • Verarbeiten Sie Rückgabew erte von Funktionen. Dabei kann es sich um Datensätz e, Datenframes, Variablen und boolesche Werte handeln. Behandeln Sie diese gemäß den Anforderu ngen Ihrer Anwendung und zur Unterstützung von PostgreSQL . • Verarbeiten Sie anonyme Blöcke (z. B. `BEGIN TRAN`) mit neuen, benutzerd efinierten PostgreSQL-Funktionen. • Konvertieren Sie Massenein fügungen für Zeilen. Das PostgreSQL-Äquivalent des Dienstprogramms SQL Server Bulk Copy (`bcp`), das	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	innerhalb der Anwendung aufgerufen wird, ist `COPY`. • Konvertieren Sie Spaltenverkettungsoperatoren. SQL Server verwendet + für die Zeichenfolgeverkettung, PostgreSQL verwendet jedoch `||`.	

Verbessern der Leistung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nutzen Sie AWS-Services, um Leistungsverbesserungen vorzunehmen.	Wenn Sie zur AWS Cloud migrieren, können Sie Ihr Anwendungs- und Datenbankdesign verfeinern, um die Vorteile der AWS-Services zu nutzen. Wenn beispielsweise die Abfragen von Ihrer Python-Anwendung, die mit einem Aurora PostgreSQL kompatiblen Datenbankserver verbunden ist, mehr Zeit in Anspruch nehmen als Ihre ursprünglichen Microsoft SQL Server-Abfragen, könnten Sie erwägen, einen Feed historischer Daten direkt in einen Amazon Simple Storage Service (Amazon S3)-Bucket vom Aurora-Server zu erstellen und Amazon Athena -basierte SQL-Abfragen zu	App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, um Berichte und Analysedatenabfragen für Ihre Benutzer-Dashboards zu generieren.	

Zugehörige Ressourcen

- Perl
- Perl-DBI-Modul
- Python
- psycopg2
- SQLAlchemy
- Massenkopie – PostgreSQL
- Massenkopie – Microsoft SQL Server
- PostgreSQL
- Arbeiten mit Amazon Aurora PostgreSQL

Zusätzliche Informationen

Sowohl Microsoft SQL Server als auch Aurora PostgreSQL – kompatibel sind ANSI-SQL-Beschwerden. Sie sollten jedoch weiterhin alle Inkompatibilitäten in Syntax, Spaltendatentypen, nativen datenbankspezifischen Funktionen, Masseneinfügungen und Groß- und Kleinschreibung beachten, wenn Sie Ihre Python- oder Perl-Anwendung von SQL Server zu PostgreSQL migrieren.

In den folgenden Abschnitten finden Sie weitere Informationen zu möglichen Inkonsistenzen.

Datentypvergleich

Änderungen des Datentyps von SQL Server zu PostgreSQL können zu erheblichen Unterschieden in den resultierenden Daten führen, mit denen Anwendungen arbeiten. Einen Vergleich der Datentypen finden Sie in der Tabelle auf der Sqlines-Website.

Native oder integrierte SQL-Funktionen

Das Verhalten einiger Funktionen unterscheidet sich zwischen SQL Server- und PostgreSQL-Datenbanken. Die folgende Tabelle bietet einen Vergleich.

Microsoft SQL Server	Beschreibung	PostgreSQL
`CAST`	Konvertiert einen Wert von einem Datentyp in einen anderen.	PostgreSQL `type :: operator`
`GETDATE()`	Gibt das aktuelle Datum und die aktuelle Uhrzeit des Datenbanksystems in einem `YYYY-MM-DD hh:mm:ss.mmm` Format zurück.	`CLOCK_TIMESTAMP`
`DATEADD`	Fügt einem Datum ein Zeit-/Datumsintervall hinzu.	`INTERVAL` Ausdruck
`CONVERT`	Konvertiert einen Wert in ein bestimmtes Datenformat.	`TO_CHAR`
`DATEDIFF`	Gibt die Differenz zwischen zwei Daten zurück.	`DATE_PART`
`TOP`	Beschränkt die Anzahl der Zeilen in einem `SELECT`Ergebnissatz.	`LIMIT/FETCH`

Anonyme Blöcke

Eine strukturierte SQL-Abfrage ist in Abschnitte wie Deklaration, ausführbare Dateien und Ausnahmebehandlung unterteilt. In der folgenden Tabelle werden die Microsoft SQL Server- und PostgreSQL-Versionen eines einfachen anonymen Blocks verglichen. Für komplexe anonyme Blöcke empfehlen wir Ihnen, eine benutzerdefinierte Datenbankfunktion innerhalb Ihrer Anwendung aufzurufen.

Microsoft SQL Server	PostgreSQL

```
my $sql_qry1=
my $sql_qry2 =
my $sqlqry = "BEGIN TRAN
$sql_qry1 $sql_qry2
if @\@error !=0 ROLLBACK
TRAN
else COMIT TRAN";
```

```
my $sql_qry1=
my $sql_qry2 =
my $sql_qry = " DO \$\$
BEGIN
$header_sql $content_sql
END
\$\$";
```

Weitere Unterschiede

- Masseneinfügungen von Zeilen: Das PostgreSQL-Äquivalent des Hilfsprogramms Microsoft SQL Server bcp ist COPY .
- Groß- und Kleinschreibung: Bei Spaltennamen wird in PostgreSQL zwischen Groß- und Kleinschreibung unterschieden, sodass Sie Ihre SQL Server-Spaltennamen in Kleinbuchstaben oder Großbuchstaben konvertieren müssen. Dies wird ein Faktor, wenn Sie Daten extrahieren oder vergleichen oder Spaltennamen in Ergebnissätzen oder Variablen platzieren. Im folgenden Beispiel werden Spalten identifiziert, in denen Werte in Groß- oder Kleinbuchstaben gespeichert werden können.

```
my $sql_qry = "SELECT $record_id FROM $exampleTable WHERE LOWER($record_name) =
 \'failed transaction\'";
```

- Verkettung:SQL Server verwendet + als Operator für die Zeichenfolgeverkettung, während PostgreSQL verwendet | | .
- Validierung: Sie sollten Inline-SQL-Abfragen und -Funktionen testen und validieren, bevor Sie sie im Anwendungscode für PostgreSQL verwenden.
- Aufnahme in die ORM-Bibliothek: Sie können auch nach vorhandener Datenbankverbindungsbibliothek suchen oder sie durch Python-ORM-Bibliotheken wie SQLAlchemy und PynomoDB ersetzen. Dies hilft, Daten mithilfe eines objektorientierten Paradigmas einfach aus einer Datenbank abzufragen und zu bearbeiten.

Migrationsmuster nach Arbeitslast

Themen

IBM

- Migrieren einer Db2-Datenbank von Amazon EC2 zu Aurora MySQL – kompatibel mithilfe von AWS DMS
- Migrieren Sie Db2 für LUW zu Amazon EC2, indem Sie den Protokoll-Versand verwenden, um die Ausfallzeit zu reduzieren
- Migrieren Sie Db2 für LUW zu Amazon EC2 mit Notfallwiederherstellung für hohe Verfügbarkeit
- Migrieren von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL – kompatibel mit AWS DMS und AWS SCT
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2

Microsoft

- Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS
- Ändern von Python- und Perl-Anwendungen zur Unterstützung der Datenbankmigration von Microsoft SQL Server zu Amazon Aurora PostgreSQL – Kompatible Edition
- Erstellen von AWS- CloudFormation Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- Exportieren einer Microsoft SQL Server-Datenbank nach Amazon S3 mithilfe von AWS DMS
- Aufnehmen und Migrieren von EC2-Windows-Instances in ein AWS Managed Services-Konto
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server mithilfe nativer Sicherungs- und Wiederherstellungsmethoden
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mit AWS DMS
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten
- ???
- Migrieren von Daten von Microsoft Azure Blob zu Amazon S3 mithilfe von Rclone
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- ???
- Einrichten einer Multi-AZ-Infrastruktur für eine SQL Server Always On FCI mithilfe von Amazon FSx

–

- Erstellen eines Genehmigungsprozesses für Firewall-Anforderungen während einer Hostwechsel-Migration zu AWS

Open-Source-Software

- Erstellen von Anwendungsbenutzern und -rollen in Aurora PostgreSQL – kompatibel
- ???
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Migrieren einer On-Premises-MySQL-Datenbank zu Amazon RDS für MySQL
- Migrieren einer On-Premises-MySQL-Datenbank zu Aurora MySQL
- Migrieren einer On-Premises-PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren von PostgreSQL auf Amazon EC2 zu Amazon RDS für PostgreSQL mit pglogical
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie On-Premises-MySQL-Datenbanken zu Aurora MySQL mit Percona XtraBackup, Amazon EFS und Amazon S3
- Migrieren externer Oracle-Tabellen zu Amazon Aurora PostgreSQL – kompatibel
- Migrieren von Redis-Workloads zu Redis Enterprise Cloud in AWS
- Starten Sie den AWS Replication Agent automatisch neu, ohne SELinux nach dem Neustart eines RHEL-Quellservers zu deaktivieren
- Transportieren von PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport

Oracle

- Konfigurieren von Links zwischen Oracle Database und Aurora PostgreSQL – kompatibel
- Konvertieren des Datentyps VARCHAR2(1) für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Emulieren von Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Inkrementelle Migration von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL mit Oracle SQL Developer und AWS SCT
- ???
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und AWS DMS mithilfe von AWS CLI und AWS CloudFormation
- ???
- Migrieren einer DB-Instance von Amazon RDS für Oracle zu einer anderen VPC
- Migrieren einer lokalen Oracle-Datenbank zu Amazon EC2 mithilfe von Oracle Data Pump
- Migrieren einer lokalen Oracle-Datenbank zu Amazon OpenSearch Service mit Logstash
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren einer On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle mithilfe des direkten Oracle Data Pump Imports über einen Datenbanklink
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle Data Pump
- Migrieren einer lokalen Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe eines Oracle-Bystanders und AWS DMS
- Migrieren einer lokalen Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren einer Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB mithilfe von AWS DMS und AWS SCT
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren einer Oracle-Datenbank zu Amazon DynamoDB mit AWS DMS

- Migrieren einer Oracle-Datenbank zu Amazon RDS für Oracle mithilfe von Oracle GoldenGate Flat File Adaptern
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren einer Oracle-Datenbank zu Aurora PostgreSQL mit AWS DMS und AWS SCT
- Migrieren einer Oracle JD Edwards- EnterpriseOne Datenbank zu AWS mithilfe von Oracle Data Pump und AWS DMS
- Migrieren einer partitionierten Oracle-Tabelle zu PostgreSQL mithilfe von AWS DMS
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren von Daten aus einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für MySQL
- Migrieren Sie von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mithilfe materialisierter Ansichten und AWS DMS
- Migrieren von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL mit SharePlex und AWS DMS
- Migrieren von Oracle Database zu Amazon RDS for PostgreSQL mithilfe von Oracle GoldenGate
- ???
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Migrieren von funktionsbasierten Indizes von Oracle zu PostgreSQL
- Migrieren älterer Anwendungen von Oracle Pro*C zu ECPG
- Migrieren von Oracle CLOB-Werten zu einzelnen Zeilen in PostgreSQL in AWS
- Migrieren von Oracle-Database-Fehlercodes zu einer mit Amazon Aurora PostgreSQL kompatiblen Datenbank
- Migrieren der Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren von nativen Oracle-Funktionen zu PostgreSQL mithilfe von Erweiterungen
- Migrieren von Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren der Oracle ROWID-Funktionalität zu PostgreSQL in AWS
- Migrieren von Oracle SERIALLY_REUSABLE-Pragma-Paketen zu PostgreSQL
- Migrieren von virtuell generierten Spalten von Oracle zu PostgreSQL
- Einrichten der Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL – kompatibel
- Validieren von Datenbankobjekten nach der Migration von Oracle zu Amazon Aurora PostgreSQL

SAP

- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren von SAP ASE zu Amazon RDS for SQL Server mit AWS DMS
- Migrieren von SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL – kompatibel mit AWS SCT und AWS DMS
- Reduzieren Sie die homogene Cutover-Zeit für die SAP-Migration mithilfe von Application Migration Service

Mehr Muster

- Bewerten Sie die Anwendungsbereitschaft für die Migration in die AWS Cloud mithilfe von CAST Highlight
- Bewerten der Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas in AWS
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- Erstellen eines erweiterten Mainframe-Datei-Viewers in der AWS Cloud
- Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode
- Herstellen einer Verbindung mit Application Migration Service-Daten- und Steuerebenen über ein privates Netzwerk
- Containerisieren Sie Mainframe-Workloads, die von Clari Age modernisiert wurden
- Konvertieren von JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL
- Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL
- Kopieren von Amazon DynamoDB-Tabellen über Konten hinweg mit AWS Backup
- Bereitstellen eines Cassandra-Clusters auf Amazon EC2 mit privaten statischen IPs, um einen Neuausgleich zu vermeiden
- Bereitstellen von Multi-Stack-Anwendungen mit AWS CDK mit TypeScript
- Emulieren von Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL
- Schätzen der Amazon RDS-Engine-Größe für eine Oracle-Datenbank mithilfe von AWR-Berichten
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Behandlung anonymer Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL
- Verarbeiten überlasteter Oracle-Funktionen in Aurora PostgreSQL – kompatibel
- Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS
- Migrieren von DB-Instances von Amazon RDS für Oracle zu anderen Konten, die AMS verwenden
- Migrieren eines lokalen Apache-Kafka-Clusters zu Amazon MSK mithilfe von MirrorMaker
- Migrieren von Apache Cassandra-Workloads zu Amazon Keyspaces mithilfe von AWS Glue

- Migrieren von Oracle 8i oder 9i zu Amazon RDS für Oracle mit SharePlex und AWS DMS
- Migrieren Sie Hadoop-Daten mithilfe von LiveData WANdisco Migrator zu Amazon S3
- Migrieren von Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten zu PostgreSQL
- Migrieren von Oracle-OUT-Bindungsvariablen in eine PostgreSQL-Datenbank
- Migrieren Sie RHEL-BYOL-Systeme mithilfe von AWS MGN zu Instances mit AWS-Lizenz
- ???
- Migrieren von SQL Server zu AWS mithilfe verteilter Verfügbarkeitsgruppen
- ???
- ???
- Modernisieren Sie die Mainframe-Ausgabeverwaltung in AWS mithilfe von OpenText Micro Focus Enterprise Server und LRS PageCenterX
- Ändern von HTTP-Headern bei der Migration von F5 zu einem Application Load Balancer in AWS
- Beheben von Verbindungsfehlern nach der Migration von Microsoft SQL Server zur AWS Cloud
- Senden Sie mithilfe von VMware Aria Operations for Logs Logs Logs von VMware Cloud on AWS an Splunk
- Einrichten der Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery
- Vereinfachen der Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM
- Übertragen Sie umfangreiche Db2-z/OS-Daten in CSV-Dateien an Amazon S3

Modernisierung

Themen

Analysieren und Visualisieren der Softwarearchitektur in CAST microSD

Erstellt von Arpita Sinha (Cast Software) und Bol Hurrell (Cast Software)

Umgebung: Produktion	Technologien: Modernisierung	Workload: Alle anderen Workloads

Übersicht

Dieses Muster zeigt, wie Sie CAST microSD verwenden können, um visuell durch ein komplexes Softwaresystem zu navigieren und eine präzise Analyse der Softwarestruktur durchzuführen. Wenn Sie CAST microSD auf diese Weise verwenden, können Sie fundiertere Entscheidungen über die Architektur Ihrer Anwendung treffen, insbesondere für Modernisierungszwecke.

Um die Architektur Ihrer Anwendung in CASTSpeed anzuzeigen, müssen Sie zuerst den Quellcode Ihrer Anwendung über die CAST-Konsole einbinden. Die Konsole veröffentlicht dann die Daten Ihrer Anwendung in CASTSpeed, wo Sie Ihre Anwendungsarchitekturschicht schichtweise visualisieren und navigieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Das Amazon Machine Image (AMI) für CAST microSD
- Eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance, die Folgendes enthält (eine speicheroptimierte r5.xlarge Amazon EC2-Instance wird empfohlen):
  - 4 vCPU
  - 32 GB RAM
  - 500 GB Mindestvolumen für Allzweck-Solid-State-Laufwerke (SSD) (gp3)
- CAST-Konsolen- und CAST microSD-Lizenzschlüssel (um die erforderlichen Lizenzschlüssel zu erhalten, wenden Sie sich an CAST unter aws.contact-me@castsoftware.com)
- Der vollständige Quellcode der Anwendung, die Sie im komprimierten (.zip) Format analysieren möchten

- Microsoft Edge, Mozilla Firefox oder Google Chrome

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für das Onboarding des Quellcodes einer Anwendung über die CAST-Konsole und das anschließende Anzeigen in CAST microSD:

Das Diagramm zeigt den folgenden Workflow:

1. CAST generiert Anwendungsquellcode-Metadaten durch Reverse-Engineering von Frontend-, Middleware- und Backend-Code.
2. Die von CAST generierten Anwendungsdaten werden automatisch in CAST microSD importiert, wo sie visualisiert und analysiert werden können.

Hier ist ein Snapshot der Funktionsweise dieses Prozesses:

Tools

- CAST microSD ist eine browserbasierte Anwendung, mit der Sie Ihr Softwaresystem visuell anzeigen und navigieren können, sodass Sie fundierte Entscheidungen über seine Architektur treffen können.
- Die CAST-Konsole ist eine browserbasierte Anwendung, mit der Sie CAST-AIP-Analysen konfigurieren, ausführen und verwalten können.

Hinweis: CAST microSD und CAST Console sind im AMI für CAST microSD enthalten.

Polen

Einrichten der CAST microSD-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die erste CAST-Konsolenkonfiguration aus.	1. Öffnen Sie Ihren Webbrowser und stellen	Softwarearchitekten, Entwickler, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie eine Verbindung mit der CAST-Konsole her, indem Sie die folgende URL eingeben: http://localhost:8081 2. Wenn Sie dazu aufgefordert werden, geben Sie Ihren Lizenzschlüssel für dieAST-Konsole ein. Wählen Sie anschließend Weiter. 3. Überprüfen Sie die Konfigurationseinstellungen. Wenn keine Änderungen erforderlich sind, wählen Sie Speichern und Fertigstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die erste CAST microSD-Konfiguration aus.	1. Öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung zu CASTSpeed her, indem Sie die folgende URL eingeben: http://localhost:8083 2. Wenn Sie dazu aufgefordert werden, melden Sie sich an, indem Sie Admin sowohl für den Benutzernamen als auch für das Passwort eingeben. 3. Wenn Sie dazu aufgefordert werden, geben Sie Ihren CAST microSD-Lizenzschlüssel ein. Wählen Sie dann Aktualisieren aus, um den Schlüssel zu speichern.	Softwarearchitekten, Entwickler, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den lokalen Server CAST Extend.	(Optional) Standardmäßig ist der lokale Server CAST Extend so konfiguriert, dass er im Offline-Modus funktioniert. Wenn dies akzeptabel ist, ist keine zusätzliche Konfiguration erforderlich. Wenn Sie jedoch lieber den lokalen CAST-Extended-Server im Online-/Proxy-Modus mit einer direkten Verbindung zu CAST Extend konfigurieren möchten, gehen Sie folgendermaßen vor. Hinweis: Informationen zu Anmeldeinformationen für CAST Extend finden Sie auf der Registrierungsseite für CAST Extend. 1. Verwenden Sie die Verknüpfung CAST Extend Admin Center auf dem Desktop, um Ihren Webbrowser zu laden und eine Verbindung mit dem lokalen CAST Extend-Server herzustellen. 2. Wählen Sie die Option Online aus. 3. Geben Sie Ihre CAST-Extended-Anmeldeinformationen (E-Mail und Passwort) ein und wählen	Softwarearchitekten, Entwickler, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Speichern, um den Vorgang abzuschließen.	

Onboarding Ihrer Anwendung in CAST microSD

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Quellcode für Ihre Anwendung vor.	Speichern Sie den Quellcode Ihrer Anwendung in einer einzigen, komprimierten ZIP-Datei.	Softwarearchitekten, Entwickler, technische Leiter
Fügen Sie Ihre Anwendung der CAST-Konsole hinzu.	1. Öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung mit der CAST-Konsole her, indem Sie die folgende URL eingeben: http://localhost:8081 2. Wenn Sie dazu aufgefordert werden, melden Sie sich an, indem Sie Admin sowohl für den Benutzernamen als auch für das Passwort eingeben. 3. Wählen Sie Anwendung hinzufügen. Geben Sie dann den Namen der Anwendung ein und wählen Sie Hinzufügen aus.	Softwarearchitekten, Entwickler, technische Leiter
Öffnen Sie den Quellcode-Bereitstellungsassistenten.	Suchen Sie die Anwendung, die Sie in der CAST-Kons	Softwarearchitekten, Entwickler, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ole erstellt haben. Wählen Sie dann Version hinzufügen aus.	
Laden Sie den Quellcode für Ihre Anwendung hoch.	Führen Sie eine der folgenden Aktionen aus: • Ziehen Sie die ZIP-Datei , die den Quellcode Ihrer Anwendung enthält, per Drag-and-Drop in den Quellcode-Bereitstellungsassistenten. • Wählen Sie das Symbol Cloud hochladen aus. Öffnen Sie dann die ZIP-Datei, die den Quellcode Ihrer Anwendung enthält.	Softwarearchitekten, Entwickler, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Analysepr ozess.	1. Geben Sie im Bereitste llungsassistenten die Versionsdetails und die Konfigurationsoptionen an. Weitere Informationen finden Sie unter Standard-Onboarding für CAST microSD in der CAST microSD-Dokumentation. 2. Stellen Sie sicher, dass die Option In CAST microSD veröffentlichen ausgewählt ist. Wählen Sie dannProceed aus. Hinweis: Wenn Sie Fortfahre n wählen, wird der Analysepr ozess für den Quellcode gestartet. Das Fortschri ttsfenster in der CAST-Kons ole zeigt jeden Schritt des Analyseprozesses und eine Benachrichtigung an, wenn die Analyse abgeschlossen ist.	Softwarearchitekten, Entwickle r, technische Leiter

Überprüfen Sie die Analyseergebnisse und Daten, die in CASTSpeed veröffentlicht wurden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status und die Protokolle.	Wenn alle Analyseaktionen abgeschlossen sind, überprüfe n Sie, ob im Fortschrittsfenste	Softwarearchitekten, Entwickle r, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	r eine Erfolgsmeldung angezeigt wird. Hinweis: Sie können die einzelnen Protokolle für jede Analyseaktion sofort nach Abschluss überprüfen. Um die Protokolle für eine bestimmte Aktion zu überprüfen, wählen Sie im Fenster Fortschritt die Option Protokoll anzeigen aus.	
Überprüfen Sie die Anwendungsdetails.	Überprüfen Sie im Bereich Anwendungsdetails die Details zu den Analyseergebnissen . Achten Sie darauf, sich die erkannten Technologien und die Quellcode-Organisation anzusehen.	Softwarearchitekten, Entwickler, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie CAST microSD und greifen Sie darauf zu.	1. Überprüfen Sie im Bereich Anwendungsverwaltung in der CAST-Konsole, ob der Versionsstatus Ihrer Anwendung imaging processed lautet. Es wird ein CAST microSD-Symbol angezeigt. 2. Wählen Sie das CAST microSD-Symbol, um direkt zu Ihren Anwendung sdaten in CAST microSD zu navigieren. Hinweis: Der Status Verarbeit etes Telefonie bedeutet, dass der Quellcode analysiert und in Ihre CASTSpeed-Instance hochgeladen wurde.	Softwarearchitekten, Entwickle r, technische Leiter

Beginnen Sie mit der Analyse Ihrer Anwendung mit CAST microSD

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei CAST microSD an.	Öffnen Sie Cast microSD und geben Sie die Standard-Administratoranmeldeinforma tionen ein (admin/admin). Die Daten Ihrer Anwendung werden angezeigt.	Softwarearchitekten, Entwickle r, technische Leiter
Erkunden Sie die Daten Ihrer Anwendung in CAST microSD.	Beginnen Sie mit dem Anzeigen Ihrer Softwarea rchitektur, indem Sie die	Softwarearchitekten, Entwickle r, technische Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CAST microSD-Funktionen verwenden. Für ein kurzes Tutorial zur Verwendung der Funktionen von CAST microSD wählen Sie das Hilfesymbol, um den CAST microSD Helper anzuzeigen. Weitere Informationen finden Sie im CAST microSD-B enutzerhandbuch.	

Zugehörige Ressourcen

Dokumentation zur CAST-Konsole

- Anmeldung
- Konfigurieren von Optionen über die CAST-Konsole

CAST microSD-Dokumentation

- Onboarding von Anwendungen für CAST microSD – Voraussetzungen
- Hinzufügen einer neuen Anwendung für CAST microSD
- Standard-Onboarding für CAST microSD – Prüfungsergebnisse
- Anmeldung
- Konfigurationsoptionen – Admin-Center-GUI

Weitere Ressourcen zu CAST microSD in AWS

- Application Modernization to AWS Accelerated by CAST – Technisch (AWS- PartnerCast Webinar, erfordert kostenloses Konto)

- Verwenden von CAST und AWS Migration Hub Refactor Spaces zur Modernisierung älterer Anwendungen (AWS-Blogbeitrag)
- Modernisieren von Anwendungen zu AWS-Architekturen mit CAST microSD (AWS-Workshop)
- AWS Marketplace: CAST microSD
- Alle CAST auf AWS-Ressourcen

Bewerten Sie die Anwendungsbereitschaft für die Migration in die AWS Cloud mithilfe von CAST Highlight

Erstellt von Greg Bola (Cast Software)

Umgebung: Produktion	Quelle: Quellcode der Legacy-Anwendung	Ziel: Faktorwechsel des Anwendungscodes in AWS
R-Typ: Neuarchitektur	Workload: IBM; Microsoft; Open-Source; Oracle	Technologien: Modernisierung; Migration; Container und Microservices
AWS-Services: Amazon RDS; Amazon S3		

Übersicht

CAST Highlight ist eine Software-as-a-Service (SaaS)-Lösung für die schnelle Analyse des Anwendungsportfolios. Dieses Muster beschreibt, wie Sie CAST Highlight konfigurieren und verwenden, um die Cloud-Bereitschaft benutzerdefinierter Softwareanwendungen im gesamten IT-Portfolio einer Organisation zu bewerten und die Modernisierung oder Migration in die Amazon Web Services (AWS) Cloud zu planen.

CAST Highlight generiert Einblicke in die Cloud-Bereitschaft einer Anwendung, identifiziert Code-Blocker, die vor einer Migration entfernt werden müssen, schätzt den Aufwand zum Entfernen dieser Blocker und empfiehlt AWS-Services, die einzelne Anwendungen nach der Migration verwenden könnten.

Dieses Muster beschreibt das Verfahren zum Einrichten und Verwenden von CAST Highlight, das aus fünf Schritten besteht: neue Benutzereinrichtung, Anwendungsverwaltung, Kampagnenverwaltung, Quellcodeanalyse und Ergebnisanalyse. Sie müssen alle Schritte im Abschnitt „Epics“ dieses Musters ausführen, um einen erfolgreichen Anwendungsscan und -analyse sicherzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives CAST-Highlight-Konto mit Portfolio Manager-Berechtigungen.
- Mindestens 300 MB freier Festplattenspeicher und 4 GB Arbeitsspeicher auf Ihrem lokalen Computer, um den lokalen CAST Highlight Agent zu installieren.
- Microsoft Windows 8 oder höher.
- Ihr Anwendungsquellcode muss in Textdateien gespeichert werden, auf die von dem Computer aus zugegriffen werden kann, auf dem der lokale Agent installiert ist. Kein Quellcode verlässt die Standorte und der gesamte Code wird lokal gescannt.

Architektur

Das folgende Diagramm veranschaulicht den Workflow für die Verwendung von CAST Highlight.

Der Workflow besteht aus folgenden Schritten:

1. Melden Sie sich beim CAST-Highlight-Portal an, laden Sie den lokalen Kundendienstmitarbeiter herunter und installieren Sie ihn auf Ihrem lokalen Computer. Amazon Simple Storage Service (Amazon S3) speichert das Installationspaket des lokalen Agenten.
2. Scannen Sie Ihre Quellcodedateien und erstellen Sie eine Ergebnisdatei.
3. Laden Sie die Ergebnisdatei in das CAST-Highlight-Portal hoch. Wichtig: In der Ergebnisdatei ist kein Quellcode enthalten.
4. Beantworten Sie Umfragefragen für jede Anwendung, die Sie gescannt haben.
5. Zeigen Sie die Dashboards und Berichte an, die im CAST-Highlight-Portal verfügbar sind. Amazon Relational Database Service (Amazon RDS) speichert den Code-Scan, die Analyseergebnisse und die CAST Highlight-Softwaredaten.

Technologie-Stack

CAST Highlight unterstützt die folgenden Technologien zur Analyse der Anwendungswolkenbereitschaft:

- Java
- COBOL
- C#
- C++

- Clojure
- PHP
- JavaScript
- TypeScript
- Python
- Microsoft Transact-SQL
- VB.Net
- Kotlin
- Scala
- Swift

Automatisierung und Skalierung

- Ein CLI-Analysator kann verwendet werden, um den CAST-Highlight-Analyseprozess zu automatisieren.

Tools

Für dieses Muster sind keine Tools erforderlich, wenn alle Voraussetzungen erfüllt sind. Sie können jedoch optionale Tools wie SCM-Dienstprogramme (Quellcode Management), Code-Extraktoren oder andere Tools zur Verwaltung Ihrer Quellcodedateien verwenden.

Polen

Neues Benutzer-Setup

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Ihr CAST-High light-Konto und wählen Sie Ihr Passwort aus.	Alle Erstbenutzer von CAST Highlight erhalten eine E-Mail zur Kontoaktivierung. Folgen Sie dem Aktivierungslink, um Ihr CAST-Highlight-Kon to zu aktivieren, und geben Sie ein Passwort ein, um den	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aktivierungsprozess abzuschli eßen.	
Melden Sie sich beim CAST-Highlight-Portal an.	Die Homepage CAST Highlight wird angezeigt , nachdem Sie Ihr neues Passwort eingegeben haben. Melden Sie sich beim CAST-Highlight-Portal mit Ihren Benutzeranmeldeinformatione n an.	N/A

Application Management

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Anwendungsdatensatz.	Navigieren Sie im CAST-High light-Portal zur Registerkarte Anwendung verwalten im Abschnitt Portfolio verwalten . Wählen Sie in der Kachel Anwendungen oben auf dem Bildschirm die Option Hinzufügen aus.	N/A
Wählen Sie einen Anwendung snamen aus.	Geben Sie einen Namen für Ihre Anwendung ein und wählen Sie dann Speichern aus. Dieser Name wird für Ihren Anwendungsdatensatz in CAST Highlight verwendet.	N/A
Wiederholen Sie die Schritte für alle Anwendungen.	Wiederholen Sie diese Schritte für jede Anwendung, die Sie scannen möchten.	N/A

Kampagnenverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Kampagne.	CAST Highlight verwendet „aign“, um eine Reihe von Anwendungen zu beschreib en, die zu einem bestimmten Zeitpunkt analysiert werden. Navigieren Sie im CAST-High light-Portal zur Registerkarte Kampagnen verwalten im Abschnitt Portfolio verwalten . Wählen Sie Kampagne erstellen, um den Bildschirm zur Kampagnenerstellung zu starten.	N/A
Geben Sie einen Namen ein und wählen Sie ein Abschluss datum für die Kampagne aus.	Geben Sie einen Namen für Ihre Kampagne ein und wählen Sie ein Schließun gsdatum dafür aus. Wichtig: Beitragende können nach dem Abschluss datum der Kampagne keine Ergebnisse der Anwendung sanalyse einreichen.	N/A
Entscheiden Sie sich dafür, Quellcode-Scan, Umfragean tworten sowie Domain- und Anwendungsbereich einzubezi ehen.	Wählen Sie eine oder mehrere der Standardbefragungen aus, die zur Verbesserung der Quellcodeanalysedaten mit qualitativen Informati onen verwendet werden. Die Umfragekategorien sind Auswirkungen auf das Geschäft, Aufwand für	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Softwarewartung, CloudReady, Anwendungseigenschaften und Green Impact. Wählen Sie die Domain und die Anwendungen aus, die während der Kampagne analysiert werden. Wichtig: Stellen Sie sicher, dass Sie alle Anwendungen, die Sie scannen möchten, im Abschnitt Anwendungen verwalten hinzufügen, bevor Sie mit der Kampagne beginnen.	
Passen Sie die Startmeldung an.	Passen Sie die Startnachricht an, die per E-Mail an alle Mitwirkenden gesendet wird, die den Anwendungen in der Kampagne zugeordnet sind.	N/A
Starten Sie die Kampagne.	Wählen Sie Abschließen, um die Kampagne zu starten.	N/A

Quellcodeanalyse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den lokalen CAST-Highlight-Agenten herunter.	Wählen Sie im CAST-Highlight-Portal Anwendungsscans aus und laden Sie den lokalen Kundendienstmitarbeiter auf Ihren lokalen Computer herunter.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den lokalen Agent.	Starten Sie das Installat ionsprogramm CAST Highlight Setup.exe und folgen Sie den angezeigten Einrichtu ngsanweisungen. Nachdem der lokale Agent installie rt wurde, können Sie Ihre Anwendungen analysieren.	N/A
Definieren Sie den Umfang des Code-Scans für den lokalen Kundendienstmitarb eiter.	Die Codeanalyse wird auf Dateiebene durchgeführt und berücksichtigt nicht die logischen Links oder Abhängigkeiten zwischen Dateien. Alle Dateien gelten als gleich und Teil der Anwendung. Um genaue und konsisten te Ergebnisse zu erzielen, bereiten Sie Ihren Code-Scan bereich vor, indem Sie die im lokalen Agent verfügbar en Datei- oder Ordneraus schlussfunktionen verwenden.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie Open-Source- oder COTS-Pakete ein.	(Optional) Wenn Sie Open-Source- oder kommerzielle off-the-shelf Pakete (COTS) einschließen möchten, stellen Sie sicher, dass sie in den Ordnern enthalten sind, die Sie scannen möchten. In der Regel werden externe Bibliotheken in einem Unterordner gruppiert, der als „Drittanbieter“ oder ähnlich bezeichnet wird, und der Hauptcode befindet sich häufig im Dateiordner „src/main“.	N/A
Schließen Sie Testklassen aus.	Testklassen werden in der Regel aus der Quellcode analyse ausgeschlossen, da sie im Allgemeinen nicht Teil der kompilierten Anwendung sind. Sie können sie jedoch bei Bedarf in den Scan aufnehmen.	N/A
Schließen Sie SCM-, Build- und Bereitstellungsordner aus.	Für konsistentere Ergebnisse sollten Sie vermeiden, SCM-, Build- oder Bereitstellungsordner (z. B. Git- oder Svn-Dateien) in Ihren Scan aufzunehmen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie Abhängigk eitsdateien ein.	Wenn Sie Einblicke in Frameworks und Abhängigk eiten wünschen, deren physische Dateien nicht Teil des Ordners sind, den Sie scannen, stellen Sie sicher, dass Sie die Abhängigk eitsdateien einschließen (z. B. pom.xml-, build.gradle-, package.json- oder .vcsproj-Dateien).	N/A
Rufen Sie den lokalen Agent auf.	Führen Sie den lokalen Agent auf Ihrem lokalen Windows-C omputer aus.	N/A
Wählen Sie den Ordner aus, der Ihren Quellcode enthält.	Wählen Sie den Ordner aus, der Ihren Quellcode enthält. Sie können mehrere Ordner hinzufügen, die vom lokalen Agent erkannt werden sollen. Obwohl der lokale Agent die Quellerkennung über Netzwerkpfade unterstützt, sollten Sie sicherstellen, dass sich Quellordner auf Ihrem lokalen Computer befinden. Wichtig: Wir empfehlen, mehrere Scans auszuführen, wenn sich mehr als 10.000 Dateien in Ihren Quellordnern befinden.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Dateierkennung.	Wählen Sie im Dashboard des lokalen Kundendienstmitarbeiters die Option Dateien ermitteln aus. Der lokale Agent erkennt Dateien in Ihren Ordnern und Unterordnern und erkennt deren Technologien. Sie können die Schaltfläche Abbrechen wählen, um die Erkennung jederzeit abzubrechen. Nachdem die Dateierkennung abgeschlossen ist, listet der lokale Agent die gefundenen Ordner und Dateien auf. Die Spalte Technologies zeigt die zugehörigen Technologien und die Anzahl der Dateien an. In der Spalte Pfad wird der Speicherort der Ordner und Dateien angezeigt.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verfeinern Sie die Konfiguration des Quellcode-Scans.	(Optional) Um den Scan des lokalen Kundendienstmitarbeiters zu verfeinern, können Sie eine oder mehrere Technologien für einen bestimmten Ordner oder eine bestimmte Datei deaktivieren. Wenn alle Technologien deaktiviert sind, wird Ihr Ordner oder Ihre Datei aus dem Geltungsbereich des Scans ausgeschlossen. Um Technologien zu deaktivieren, wählen Sie das gelbe Label der Technologie aus, die Sie deaktivieren möchten. Sie können auch das Filtersymbol auswählen, wenn Sie den Mauszeiger über eine Datei oder einen Ordner bewegen, um eine Technologie einer bestimmten Datei oder einem bestimmten Ordner zuzuordnen. Diese Einstellungen werden gespeichert und beschleunigen den Erkennungsprozess für den Ordner oder die Datei.	N/A
Starten Sie den Quellcode-Scan.	Nachdem Sie Ihren Scan konfiguriert haben, wählen Sie „Scandateien“, um mit dem Scanvorgang zu beginnen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach grünen oder grauen Labels.	Nachdem der Quellcodescan abgeschlossen ist, wird auf Ordner- und Dateiebene eine Statusbezeichnung angezeigt. Ein grünes Label bedeutet, dass Dateien mit der zugehörigen Technologie korrekt gescannt wurden. Ein graues Label bedeutet, dass Dateien nicht gescannt und ausgeschlossen wurden. Der Grund für den Ausschlus s wird angezeigt, wenn Sie den Mauszeiger über die Beschriftung jeder Datei bewegen. Mögliche Gründe für den Dateiausschluss sind Binärdateien, nicht lesbare Dateien, fehlende Dateien, externe Bibliothek, codierte Dateien, generierte Dateien, Syntaxfehler, Inhalte, die nicht in der erwarteten Sprache vorliegen, Code, der nicht mit genügend Analysekriterien übereinstimmt, Dateien, die die Größenbeschränkung (10 MB) überschreiten, Timeout-Probleme oder Nichtverf ügbarkeit des Analysators.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Scankonfiguration und den Scancode erneut.	(Optional) Sie können Ihre Scan-Konfigurationseinstellungen ändern und Dateien scannen auswählen, um die Dateien erneut zu scannen.	N/A
Bestätigen Sie die Scanergebnisse.	Wählen Sie Ergebnisse bestätigen, wenn die Scanergebnisse Ihren Anforderungen entsprechen.	N/A
Zeigen Sie Frameworks und Softwarebibliotheken an, die vom lokalen Agent gefunden wurden.	Sehen Sie sich die Frameworks und Softwarebibliotheken an, die von Ihren Anwendungen verwendet oder referenziert und vom lokalen Kundendienstmitarbeiter während des Codescans entdeckt wurden. Sie können Elemente aus diesen Listen beibehalten oder ignorieren, indem Sie ihre individuelle Schalterschaltfläche auswählen. Wählen Sie Abhängigkeiten bestätigen, um fortzufahren. Wichtig: Wenn ein Framework deaktiviert ist, wird es nicht im CAST-Highlight-Portal aufgeführt oder an Ihre Anwendung angehängt.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die Code-Scan ergebnisse.	Der lokale Kundendienstmitarb eiter zeigt eine Zusammenf assung Ihrer Code-Scan ergebnisse an, gruppiert nach Technologie. Wählen Sie Speichern und geben Sie den Ordner an, in dem die Ergebnisse gespeiche rt werden sollen. Der lokale Agent generiert eine ZIP-Datei pro Scan, die alle Analyseer gebnisse enthält. Abhängig von der Anzahl der verschiedenen Technolog ien und Stammquellordner generiert der lokale Agent automatisch eine oder mehrere CSV-Dateien mit der Benennungsstruktur FolderName.Speed.date.csv.	N/A
Laden Sie die Code-Scan ergebnisse in das CAST-High light-Portal hoch.	Wählen Sie im CAST-High light-Portal die Anwendung en aus, die Sie im Abschnitt Anwendungsscans analysiert haben. Wählen Sie Ergebniss e hochladen und dann die CSV-Dateien aus. Sie können die CSV-Dateien auch einzeln hochladen. Nachdem jede Datei hochgeladen wurde, wird ein Datensatz des Uploads auf Ihrem Bildschirm angezeigt.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie bei Bedarf Analyseergebnisdateien.	(Optional) Eine Analyseergebnisdatei kann während des Upload-Vorgangs jederzeit gelöscht werden, indem Sie das Papierkorbsymbol auswählen. Wichtig: Nur Benutzer mit Portfolio Manager-Berechtigungen oder der Beitragende, der die Ergebnisse hochgeladen hat, können die Ergebnisse löschen.	N/A
Nehmen Sie an der Umfrage zur Anwendung teil.	Für Anwendungen, für die eine Umfrage erforderlich ist, wird eine Schaltfläche angezeigt. Wählen Sie Verfeinern, beantworten Sie die Fragen für jeden Abschnitt der Umfrage und wählen Sie Senden, nachdem Sie fertig sind. Der Fortschritt Ihrer Umfrage wird oben auf Ihrem Bildschirm angezeigt. Sie können Ihre Ergebnisse einreichen, nachdem alle obligatorischen Informationen übermittelt wurden. Sie können die Daten jedoch in der CAST Highlight-Instance Ihrer Organisation anreichern, indem Sie alle Fragen beantworten.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Code-Scan ergebnisse.	Nachdem Sie alle CSV-Ergebnisdateien für die Anwendung hochgeladen und die Umfragefragen beantwortet haben, wählen Sie im Abschnitt Anwendungsscans die Option Senden aus. Dieser Schritt ist erforderlich, um den Prozess abzuschließen und sicherzustellen, dass die Ergebnisse im CAST-Highlight-Portal verfügbar sind.	N/A

Ergebnisanalyse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Homepage des CAST-Highlight-Portals an.	Die CAST-Highlight-Portalstartseite enthält Kacheln, die allgemeine Informationen über Ihr Anwendungsportfolio enthalten, z. B. Softwarezustand CloudReadyund Open-Source-Sicherheitswerte für Ihr gesamtes Portfolio. Die Homepage enthält auch die Anzahl der integrierten Anwendungen. Weitere Informationen zu den Definitionen von CAST-Highlight-Metriken und zur Messungsmethode finden Sie unter CAST-Highlight – Metriken	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Methode (Microsoft-PowerPoint Präsentation).	
Zeigen Sie das CloudReady Dashboard an.	Wählen Sie die CloudRead y Kachel aus, um das CloudReady Dashboard zu öffnen. Dies ist das primäre Dashboard auf Portfolioebene zur Bewertung der Cloud-Ber eitschaft Ihrer Anwendung en. Es hilft Ihnen bei der Planung und Entwicklung einer Portfolio-Roadmap für Ihre Cloud-Migration	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich das Dashboard von Portfolio Advisor für Cloud an.	Das Dashboard von Portfolio Advisor für Cloud segmentiert Anwendungen automatisch in empfohlene Migrationskategorien. Die Segmentierung basiert auf den technischen Merkmalen jeder Anwendung. Zu den Faktoren gehören die Quellcodeanalyse (Cloud-Bereitschaft, Softwareausfallsicherheit und mehr) und die Auswirkungen auf das Geschäft, die sich aus der Umfrage ergeben. Wählen Sie oben rechts Datenverarbeitung aus, um die anfänglichen Segmentierungsempfehlungen zu generieren. Die Blasen in den Diagrammen oben im Dashboard stellen jede Anwendung im Portfolio dar, geordnet nach der empfohlenen Segmentierung. Jede Anwendung ist auch in einer Datentabelle unter den Diagrammen aufgeführt, einschließlich relevanter Metriken für jede Anwendung. Zu den empfohlenen Segmenten gehören: • Hostwechsel – Eine Empfehlung, die Infrastru	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	kturkonfiguration der Anwendung zu ändern, um sie mithilfe einer Infrastru cture as a Service (IaaS)-Lösung in die Cloud zu verschieben. • Faktorwechsel – Eine Empfehlung, mäßige Änderungen am Anwendung scode durchzuführen, ohne die Architektur oder Funktionalität zu ändern, damit er mithilfe einer Container-as-a-Service (CaaS)- oder Platform-as-a-Service (PaaS)-Lösung migriert werden kann. • Neuarchitektur – Eine Empfehlung, den Anwendungscode drastisch zu ändern, um den Zustand der Anwendung zu verbessern und sie auf die Migration vorzubere iten, indem Sie eine PaaS-Lösung verwenden, oder sie als Serverless-Anwendu ng mithilfe einer FaaS-Lösu ng (Funktion as a Service) bereitzustellen. • Neuerstellung – Eine Empfehlung, den Code der Anwendung zu verwerfen und ihn mithilfe einer PaaS-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lösung erneut in der Cloud zu entwickeln oder ihn mithilfe einer FaaS-Lösu ng erneut als Serverless-Anwendung zu entwickeln. • Außerbetriebnahme – Eine Empfehlung, die Anwendung vollständ ig zu verwerfen oder sie möglicherweise durch eine Alternative zur kommerzie llen Software als Service (SaaS) zu ersetzen.	
Ändern Sie Segmentie rungsempfehlungen.	In einigen Fällen können Sie das von CAST Highlight empfohlene Segment ändern. Navigieren Sie dazu zur Anwendung in der Datentabe lle und wählen Sie ein anderes Segment aus der Dropdown-Liste neben dem Anwendung snamen aus. Wählen Sie dann oben rechts Speichern aus, um Ihre Änderungen zu speichern. Sie können diese Daten auch jederzeit exportieren, indem Sie oben rechts Export ierenauswählen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine zu analysier ende Anwendung aus.	Wählen Sie im Dashboard von Portfolio Advisor für Cloud eine Anwendungsbläsel aus, um diese Anwendung zu analysieren. Wählen Sie den Namen der Anwendung in der Tabelle nach dem Blasendiagramm aus, um mit der tieferen Analyse zu beginnen. Verschiedene Dashboard s stehen zur Verfügung, um einzelne Anwendung en zu analysieren, z. B. Code Insights (Software-Zustandsmuster), Trends und Softwarezusammensetzung (Open-Source-Risiken).	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die CloudReady Ergebnisse einer einzelnen Anwendung.	Wählen Sie die CloudRead y Registerkarte aus, auf der die CloudReady Gesamtbew ertung der Anwendung angezeigt wird. Dieser Wert ist ein gewichteter Durchschn itt auf der Grundlage einer Kombination aus Antworten auf die CloudReady Umfrage und dem CloudReady Code-Scan. Die Antworten auf die Umfragefragen werden in der Tabelle unter den Kacheln angezeigt. Wählen Sie CloudReady Code Scan, um die Code-Scan ergebnisse anzuzeigen. Es gibt eine Liste von CloudRead y Mustern, nach denen der Anwendungscode gescannt wurde. Diese Liste enthält die folgenden Spalten: • Cloud Requirement ist das spezifische Codemuster. • Technologie ist die Programmiersprache des Musters. „Auswirkung“ ist die Auswirkung des Musters auf die Anwendung (C = Code, F = Framework, A = Architektur). • Kritizität ist der Grad der Wichtigkeit, dieses	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Muster vor der Migration anzugehen. • Beitrag ist, wie dieses Muster zur CloudReady Gesamtbewertung beiträgt. Wenn das Muster grün ist, ist es ein Booster und erhöht den CloudReady Wert. Wenn das Muster rot ist, ist es ein Blocker und verringert den CloudRead y Wert. Wenn das Muster keine Farbe hat, ist es ein Blocker, der nicht erkannt wurde und den CloudReady Wert erhöht. • Blockierungen sind die Anzahl der einzelnen Vorkommen eines Blockermusters. Wählen Sie die Blockiernummer aus, um eine Liste der Quellcode dateien anzuzeigen, in denen das Muster erkannt wurde. • Est. Der Aufwand ist eine Schätzung der Anzahl der Tage, die benötigt werden, um die Hindernisse in jeder Zeile zu beheben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie Daten nach Microsoft Excel.	(Optional) Wählen Sie Nach Excel exportieren, um die Daten zur weiteren Analyse zu exportieren. Die Ergebnisd aten der Anwendungsanalyse können verwendet werden, um die Cloud-Bereitschaft einer Anwendung weiter zu analysieren und zu bestimmen , welcher Code vor einer Migration aktualisiert werden muss.	N/A
Empfehlungen anzeigen.	Wählen Sie Empfehlungen neben CloudReady Code Scan, um den Bildschirm Cloud-Service-Empfehlungen anzuzeigen. Dadurch werden AWS-Services identifiziert, die die Anwendung auf der Grundlage ihrer Eigenschaften einführen kann. Wiederholen Sie diesen Schritt, um Empfehlungen für alle von Ihnen analysierten Anwendungen anzuzeigen.	N/A

Zugehörige Ressourcen

Kampagnenverwaltung

- CAST Highlight Foundation Certification Training Abschnitt 3: Portfolio-Konfiguration (Video)

Quellcodeanalyse

- CAST Highlight Foundation Certification Training Abschnitt 4: Anwendungsanalyse (Video)

Sonstige Ressourcen

- CAST-Markierung in AWS Marketplace
- AWS und CAST: Beschleunigen Sie die Modernisierung von Anwendungen
- CAST Highlight – Dokumentation, Produkttutorials und Tools von Drittanbietern
- CAST-Markierung – Cloud-Bereitschafts-Produktdemo (Video)
- Application Portfolio Modernization with CAST Highlight (AWS-Workshop)

Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL

Erstellt von Tabby Ward (AWS)

Code-Repository: Elemente mithilfe von DynamoDB TLL in S3 archivieren	Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; Datenbanken; Serverless; Speicher und Backup; Kostenmanagement
Workload: Open-Source	AWS-Services: Amazon S3; Amazon DynamoDB ;Amazon Kinesis ;AWS Lambda	

Übersicht

Dieses Muster enthält Schritte zum Entfernen älterer Daten aus einer Amazon-DynamoDB-Tabelle und zum Archivieren in einem Amazon Simple Storage Service (Amazon S3)-Bucket auf Amazon Web Services (AWS), ohne eine Serverflotte verwalten zu müssen.

Dieses Muster verwendet Amazon DynamoDB Time to Live (TTL), um alte Elemente automatisch zu löschen, und Amazon DynamoDB Streams, um die TTL-abgelaufenen Elemente zu erfassen. Anschließend verbindet es DynamoDB Streams mit AWS Lambda, das den Code ausführt, ohne Server bereitzustellen oder zu verwalten.

Wenn dem DynamoDB-Stream neue Elemente hinzugefügt werden, wird die Lambda-Funktion initiiert und schreibt die Daten in einen Amazon-Data-Firehose-Bereitstellungsdatenstrom. Firehose bietet eine einfache, vollständig verwaltete Lösung zum Laden der Daten als Archiv in Amazon S3.

DynamoDB wird häufig verwendet, um Zeitreihendaten zu speichern, z. B. Clickstream-Daten von Webseiten oder Internet der Dinge (IoT)-Daten von Sensoren und verbundenen Geräten. Anstatt Elemente zu löschen, auf die weniger häufig zugegriffen wird, möchten viele Kunden sie zu Prüfungszwecken archivieren. TTL vereinfacht diese Archivierung, indem Elemente basierend auf dem Zeitstempelattribut automatisch gelöscht werden.

Elemente, die durch TTL gelöscht wurden, können in DynamoDB Streams identifiziert werden. Dabei wird eine zeitlich geordnete Abfolge von Änderungen auf Elementebene erfasst und die Abfolge bis

zu 24 Stunden lang in einem Protokoll gespeichert. Diese Daten können von einer Lambda-Funktion genutzt und in einem Amazon S3-Bucket archiviert werden, um die Speicherkosten zu senken. Um die Kosten weiter zu senken, können Amazon S3-Lebenszyklusregeln erstellt werden, um die Daten (sobald sie erstellt werden) automatisch in kostengünstige Speicherklassen wie S3 Glacier Instant Retrieval oder S3 Glacier Flexible Retrieval oder Amazon S3 Glacier Deep Archive für die langfristige Speicherung zu überführen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI) 1.7 oder höher, installiert und konfiguriert unter macOS , Linux oder Windows.
- Python 3.7 oder höher.
- Boto3, installiert und konfiguriert. Wenn Boto3 noch nicht installiert ist, führen Sie den `python -m pip install boto3` Befehl aus, um es zu installieren.

Architektur

Technologie-Stack

- Amazon DynamoDB
- Amazon DynamoDB Streams
- Amazon Data Firehose
- AWS Lambda
- Amazon S3

1. Elemente werden durch TTL gelöscht.
2. Der DynamoDB-Stream-Auslöser ruft die Lambda-Stream-Prozessorfunktion auf.
3. Die Lambda-Funktion speichert Datensätze im Firehose-Bereitstellungs-Stream im Batch-Format.
4. Datensätze werden im S3-Bucket archiviert.

Tools

- AWS CLI – Die AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services.
- Amazon DynamoDB – Amazon DynamoDB ist eine Schlüsselwert- und Dokumentdatenbank, die eine einstellige Millisekunden-Leistung in jeder Größenordnung bietet.
- Amazon DynamoDB Time to Live (TTL) – Mit Amazon DynamoDB TTL können Sie einen Zeitstempel pro Element definieren, um zu bestimmen, wann ein Element nicht mehr benötigt wird.
- Amazon DynamoDB Streams – Amazon DynamoDB Streams erfasst eine zeitlich geordnete Abfolge von Änderungen auf Elementebene in jeder DynamoDB-Tabelle und speichert diese Informationen bis zu 24 Stunden lang in einem Protokoll.
- Amazon Data Firehose – Amazon Data Firehose ist die einfachste Möglichkeit, Streaming-Daten zuverlässig in Data Lakes, Datenspeicher und Analyseservices zu laden.
- AWS Lambda – AWS Lambda führt Code aus, ohne dass Server bereitgestellt oder verwaltet werden müssen. Sie zahlen nur für die tatsächlich aufgewendete Zeit.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenweit führende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

Code

Der Code für dieses Muster ist im GitHub Archivieren von Elementen in S3 mithilfe des DynamoDB-TTL-Repositorys verfügbar.

Sekunden

Einrichten einer DynamoDB-Tabelle, TTL und eines DynamoDB-Streams

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DynamoDB-Tabelle.	Verwenden Sie die AWS CLI, um eine Tabelle in DynamoDB mit dem Namen zu erstellen `Reservation` . Wählen Sie zufällige Lesekapazitätseinheit (RCU) und Schreibkapazitätseinheit (WCU) aus und geben	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Ihrer Tabelle zwei Attribute : `ReservationID` und `ReservationDate` . `aws dynamodb create-table \ --table-name Reservation \ --attribute-definitions AttributeName=ReservationID,AttributeType=S AttributeName=ReservationDate,AttributeType=N \ --key-schema AttributeName=ReservationID,KeyType=HASH AttributeName=ReservationDate,KeyType=RANGE \ --provisioned-throughput ReadCapacityUnits=100,WriteCapacityUnits=100`  `ReservationDate` ist ein Epochenzeitstempel, der verwendet wird, um TTL zu aktivieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie DynamoDB TTL.	Verwenden Sie die AWS CLI, um DynamoDB TTL für das `ReservationDate` Attribut zu aktivieren. `aws dynamodb update-time-to-live \ --table-name Reservation\ --time-to-live-specification Enabled=true,AttributeName=ReservationDate`	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie einen DynamoDB-Stream.	Verwenden Sie die AWS CLI, um einen DynamoDB-Stream für die `Reservation` Tabelle mithilfe des `NEW_AND_OLD_IMAGES` Stream-Typs zu aktivieren. `aws dynamodb update-table \ --table-name Reservation \ --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES` Dieser Stream enthält Datensätze für neue Elemente, aktualisierte Elemente, gelöschte Elemente und Elemente, die durch TTL gelöscht werden. Die Datensätze für Elemente, die durch TTL gelöscht werden, enthalten ein zusätzliches Metadatenattribut, um sie von Elementen zu unterscheiden, die manuell gelöscht wurden. Das `userIdentity` Feld für TTL-Löschungen gibt an, dass der DynamoDB-Service die Löschaktion ausgeführt hat. In diesem Muster werden nur die durch TTL gelöschten	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Elemente archiviert, aber Sie können nur die Datensätze `principalId` archivieren, bei denen `eventName` gleich ist `REMOVE` und `userIdentity` enthält `dynamodb.amazonaws.com` .	

Erstellen und Konfigurieren eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Verwenden Sie die AWS CLI, um einen S3-Ziel-Bucket in Ihrer AWS-Region zu erstellen , und ersetzen Sie durch `us-east-1` Ihre Region. `aws s3api create-bucket \ --bucket reservationfirehosedestinationbucket \ --region us-east-1` Stellen Sie sicher, dass der Name des S3-Buckets global eindeutig ist, da der Namespace von allen AWS-Konten gemeinsam genutzt wird.	Cloud-Architekt, App-Entwickler
Erstellen Sie eine 30-tägige Lebenszyklusrichtlinie für den S3-Bucket.	1. Melden Sie sich bei der AWS-Managementkons	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ole an und öffnen Sie die Amazon S3-Konsole. 2. Wählen Sie den S3-Bucket aus, der die Daten aus Firehose enthält. 3. Wählen Sie im S3-Bucket die Registerkarte Verwaltung und dann Lebenszyklusregel hinzufügen aus. 4. Geben Sie im Dialogfeld Lebenszyklusregel einen Namen für Ihre Regel ein und konfigurieren Sie eine 30-tägige Lebenszyklusregel für Ihren Bucket.	

Erstellen eines Firehose-Bereitstellungs-Streams

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen Firehose-Bereitstellungs-Stream.	Laden Sie das `CreateFireHoseToS3.py` Codebeispiel aus dem GitHub Repository herunter und bearbeiten Sie es. Dieser Code ist in Python geschrieben und zeigt Ihnen, wie Sie einen Firehose-Bereitstellungs-Stream und eine AWS Identity and Access Management (IAM)-Rolle erstellen. Die IAM-Rolle verfügt über eine Richtlinie,	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit der Firehose in den S3-Ziel-Bucket schreiben kann. Verwenden Sie den folgenden Befehl und die folgenden Befehlszeilenargumente, um das Skript auszuführen. Argument 1= <Your_S3_bucket_ARN> , bei dem es sich um den Amazon-Ressourcennamen (ARN) für den Bucket handelt, den Sie zuvor erstellt haben Argument 2= Ihr Firehose-Name (Dieses Pilotprojekt verwendet `firehose_to_s3_stream` .) Argument 3= Ihr IAM-Rollenname (Dieses Pilotprojekt verwendet `firehose_to_s3` .) `python CreateFireHoseToS3.py <Your_S3_Bucket_ARN> firehose_to_s3_stream firehose_to_s3` Wenn die angegebene IAM-Rolle nicht vorhanden ist, erstellt das Skript eine Übernahmerolle mit einer Vertrauensbeziehungsrichtlinie sowie eine Richtlinie,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die ausreichende Amazon S3-Berechtigung gewährt. Beispiele für diese Richtlini en finden Sie im Abschnitt Zusätzliche Informationen.	
Überprüfen Sie den Firehose-Bereitstellungsdatenstrom.	Beschreiben Sie den Firehose-Bereitstellungsdat enstrom mithilfe der AWS CLI, um zu überprüfen, ob der Bereitstellungsdatenstrom erfolgreich erstellt wurde. `aws firehose describe-delivery-stream --delivery-stream-name firehose_to_s3_stream`	Cloud-Architekt, App-Entwickler

Erstellen einer Lambda-Funktion zur Verarbeitung des Firehose-Bereitstellungsdatenstroms

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Vertrauen srichtlinie für die Lambda-Fu nktion.	Erstellen Sie eine Vertrauen srichtliniendatei mit den folgenden Informationen. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Service"
	: "lambda.amazonaws.
	com"
	},
	"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>
	Dadurch erhält Ihre Funktion die Berechtigung, auf AWS-Ressourcen zuzugreifen.	

Erstellen Sie eine Ausführungsrolle für die Lambda-Funktion.	Führen Sie den folgenden Code aus, um die Ausführungsrolle zu erstellen.
	<pre>aws iam create-role
	--role-name lambda-
	ex --assume-role-poli
	cy-document file://Tr
	ustPolicy.json</pre>
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie der Rolle die Berechtigung hinzu.	Verwenden Sie den `attach-policy-to-role` Befehl , um der Rolle Berechtigungen hinzuzufügen.
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/IAMFullAccess`
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Lambda-Funktion.	Komprimieren Sie die `LambdaStreamProcessor.py` Datei aus dem Code-Repository, indem Sie den folgenden Befehl ausführen.
	`zip function.zip LambdaStreamProcessor.py`
	Wenn Sie die Lambda-Funktion erstellen, benötigen Sie den ARN der Lambda-Ausführungsrolle. Führen Sie den folgenden Code aus, um den ARN abzurufen.
	`aws iam get-role \ --role-name lambda-ex`
	Führen Sie den folgenden Code aus, um die Lambda-Funktion zu erstellen.
	`aws lambda create-function --function-name LambdaStreamProcessor \ --zip-file fileb://function.zip --handler LambdaStreamProcessor.handler --runtime python3.8 \ --role {Your Lamda Execution Role ARN}\`
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--environment Variables="{firehose_name=firehose_to_s3_stream,bucket_arn = arn:aws:s3:::reservationfirehosedestinationbucket,iam_role_name = firehose_to_s3, batch_size=400}"`	
Konfigurieren Sie den Lambda-Funktionsauslöser.	Verwenden Sie die AWS CLI, um den Auslöser (DynamoDB Streams) zu konfigurieren, der die Lambda-Funktion aufruft. Die Batchgröße von 400 soll vermeiden, dass Probleme mit der Lambda-Gleichzeitigkeit auftreten. `aws lambda create-event-source-mapping --function-name LambdaStreamProcessor \ --batch-size 400 --starting-position LATEST \ --event-source-arn <Your Latest Stream ARN From DynamoDB Console>`	Cloud-Architekt, App-Entwickler

Testen der Funktionalität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Tabelle Reservierung Elemente mit	Um die Funktionalität zu testen, fügen Sie der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
abgelaufenen Zeitstempeln hinzu.	`Reservation` Tabelle Elemente mit abgelaufenen Epochenzeitstempeln hinzu. TTL löscht Elemente automatisch basierend auf dem Zeitstempel. Die Lambda-Funktion wird bei DynamoDB-Stream-Aktivitäten initiiert und filtert das Ereignis, um `REMOVE` Aktivitäten oder gelöschte Elemente zu identifizieren. Anschließend werden Datensätze im Batch-Format im Firehose-Bereitstellungs-Stream abgelegt. Der Firehose-Bereitstellungs-Stream überträgt Elemente an einen Ziel-S3-Bucket mit dem `firehosetos3example/year=current year/month=current month/day=current day/hour=current hour/` Präfix. Wichtig: Um den Datenabruf zu optimieren, konfigurieren Sie Amazon S3 mit den `Prefix` und `ErrorOutputPrefix`, die im Abschnitt Zusätzliche Informationen beschrieben sind.	

Bereinigen der Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle Ressourcen.	Löschen Sie alle Ressourcen, um sicherzustellen, dass Ihnen keine Gebühren für Services berechnet werden, die Sie nicht verwenden.	Cloud-Architekt, App-Entwickler

Zugehörige Ressourcen

- Verwalten Ihres Speicher-Lebenszyklus
- Amazon S3-Speicherklassen
- AWS SDK for Python (Boto3)-Dokumentation

Zusätzliche Informationen

Erstellen und Konfigurieren eines Firehose-Bereitstellungsdatenstroms – Richtlinienbeispiele

Beispieldokument für eine Firehose-Richtlinie für vertrauenswürdige Beziehungen

```
firehose_assume_role = {
        'Version': '2012-10-17',
        'Statement': [
            {
                'Sid': '',
                'Effect': 'Allow',
                'Principal': {
                    'Service': 'firehose.amazonaws.com'
                },
                'Action': 'sts:AssumeRole'
            }
        ]
    }
```

Beispiel für eine S3-Berechtigungsrichtlinie

```
s3_access = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Action": [
                    "s3:AbortMultipartUpload",
                    "s3:GetBucketLocation",
                    "s3:GetObject",
                    "s3:ListBucket",
                    "s3:ListBucketMultipartUploads",
                    "s3:PutObject"
                ],
                "Resource": [
                    "{your s3_bucket ARN}/*",
                    "{Your s3 bucket ARN}"
                ]
            }
        ]
    }
```

Testen der Funktionalität – Amazon S3-Konfiguration

Die Amazon S3-Konfiguration mit dem folgenden `Prefix` und `ErrorOutputPrefix` wird zur Optimierung des Datenabrufs ausgewählt.

prefix

```
firehosetos3example/year=! {timestamp: yyyy}/month=! {timestamp:MM}/day=!
 {timestamp:dd}/hour=!{timestamp:HH}/
```

Firehose erstellt zunächst einen Basisordner mit dem Namen `firehosetos3example` direkt unter dem S3-Bucket. Anschließend werden die Ausdrücke `!{timestamp:yyyy}`, `!{timestamp:MM}!{timestamp:dd}`, und `!{timestamp:HH}` auf Jahr, Monat, Tag und Stunde im Java-DateTimeFormatterFormat ausgewertet.

Ein ungefährer Ankunftszeitstempel von 1604683577 in der Unix-Epochenzeit ergibt beispielsweise `year=2020`, `month=11day=06`, und `hour=05`. Daher wird der Speicherort in Amazon S3, an den Datensätze übermittelt werden, als ausgewertet`firehosetos3example/year=2020/month=11/day=06/hour=05/`.

ErrorOutputPrefix

```
firehosetos3erroroutputbase/!{firehose:random-string}/!{firehose:error-output-type}/!
{timestamp:yyyy/MM/dd}/
```

Das `ErrorOutputPrefix` führt zu einem Basisordner mit dem Namen `firehosetos3erroroutputbase` direkt unter dem S3-Bucket. Der Ausdruck `!{firehose:random-string}` wird zu einer zufälligen Zeichenfolge mit 11 Zeichen ausgewertet, z. B. `ztWxkdg3Thg`. Der Speicherort für ein Amazon S3-Objekt, an das fehlgeschlagene Datensätze übermittelt werden, könnte zu ausgewertet werden`firehosetos3erroroutputbase/ztWxkdg3Thg/processing-failed/2020/11/06/`.

Erstellen Sie einen Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager

Erstellt von Kevin Yung (AWS), Bols (Micro Focus), Abraham Rondon (Micro Focus) und Krithikani Selvam (AWS)

Umgebung: Produktion	Technologien: Modernisierung; Cloudnativ; DevOps; Infrastruktur

Übersicht

Dieses Muster führt eine skalierbare Architektur für Mainframe-Anwendungen ein, die Micro Focus Enterprise Server in Scale-Out Performance and Availability Cluster (PAC) und eine Auto Scaling-Gruppe von Amazon Elastic Compute Cloud (Amazon EC2) auf Amazon Web Services (AWS) verwenden. Die Lösung ist vollständig automatisiert mit Lebenszyklus-Hooks von AWS Systems Manager und Amazon EC2 Auto Scaling. Mithilfe dieses Musters können Sie Ihre Mainframe-Online- und Batch-Anwendungen so einrichten, dass eine hohe Ausfallsicherheit erreicht wird, indem Sie basierend auf Ihren Kapazitätsanforderungen automatisch auf- und abskalieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Micro Focus Enterprise Server-Software und -Lizenz. Weitere Informationen erhalten Sie beim Micro-Focus-Vertrieb.
- Ein Verständnis des Konzepts der Neuerstellung und Bereitstellung einer Mainframe-Anwendung für die Ausführung in Micro Focus Enterprise Server. Einen Überblick auf hoher Ebene finden Sie im Datenblatt zu Micro Focus Enterprise Server.
- Ein Verständnis der Konzepte in Micro Focus Enterprise Server Scale-Out Performance and Availability Cluster. Weitere Informationen finden Sie in der Micro Focus Enterprise Server-Dokumentation.

- Ein Verständnis des Gesamtkonzepts der Mainframe-Anwendung DevOps mit Continuous Integration (CI). Ein AWS Prescriptive Guidance-Muster, das von AWS und Micro Focus entwickelt wurde, finden Sie unter Mainframe-Modernisierung: DevOps on AWS mit Micro Focus.

Einschränkungen

- Eine Liste der Plattformen, die von Micro Focus Enterprise Server unterstützt werden, finden Sie im Datenblatt zu Micro Focus Enterprise Server.
- Die in diesem Muster verwendeten Skripts und Tests basieren auf Amazon EC2 Windows Server 2019. Andere Windows Server-Versionen und -Betriebssysteme wurden nicht auf dieses Muster getestet.
- Das Muster basiert auf Micro Focus Enterprise Server 6.0 für Windows. Frühere oder spätere Versionen wurden bei der Entwicklung dieses Musters nicht getestet.

Produktversionen

- Micro Focus Enterprise Server 6.0
- Windows Server 2019

Architektur

In der herkömmlichen Mainframe-Umgebung müssen Sie Hardware zum Hosten Ihrer Anwendungen und Unternehmensdaten bereitstellen. Um die Spitzen saisonaler, monatlicher, vierteljährlicher oder sogar unerwarteter Anforderungen zu bewältigen und zu bewältigen, müssen Mainframe-Benutzer durch den Kauf zusätzlicher Speicher- und Rechenkapazität skalieren. Eine Erhöhung der Anzahl der Speicher- und Rechenkapazitätsressourcen verbessert die Gesamtleistung, aber die Skalierung ist nicht linear.

Dies ist nicht der Fall, wenn Sie mit der Einführung eines On-Demand-Verbrauchsmodells in AWS beginnen, indem Sie Amazon EC2 Auto Scaling und Micro Focus Enterprise Servers verwenden. In den folgenden Abschnitten wird beschrieben, wie Sie mit einer Amazon EC2 Auto Scaling-Gruppe eine voll automatisierte, skalierbare Mainframe-Anwendungsarchitektur mit Micro Focus Enterprise Server Scale-Out Performance and Availability Cluster (PAC) erstellen.

Micro Focus Enterprise Server Auto Scaling-Architektur

Zunächst ist es wichtig, die Grundkonzepte von Micro Focus Enterprise Server zu verstehen. Diese Umgebung bietet eine Mainframe-kompatible x86-Bereitstellungsumgebung für Anwendungen, die traditionell auf dem IBM-Mainframe ausgeführt wurden. Es bietet sowohl Online- als auch Batch-Ausführungen und eine Transaktionsumgebung, die Folgendes unterstützt:

- IBM COBOL
- IBM PL/I
- IBM-JCL-Stapelverarbeitungsaufträge
- IBM-CICS- und IMS-TM-Transaktionen
- Web-Services
- Allgemeine Batch-Dienstprogramme, einschließlich SORT

Micro Focus Enterprise Server ermöglicht die Ausführung von Mainframe-Anwendungen mit minimalen Änderungen. Vorhandene Mainframe-Workloads können auf x86-Plattformen verschoben und modernisiert werden, um die nativen AWS Cloud-Erweiterungen für eine schnelle Expansion in neue Markte oder Regionen zu nutzen.

Das AWS Prescriptive Guidance-Muster Mainframe modernization: DevOps on AWS mit Micro Focus führte die Architektur ein, um die Entwicklung und das Testen von Mainframe-Anwendungen in AWS mithilfe von Micro Focus Enterprise Developer und Enterprise Test Server mit AWS CodePipeline und AWS zu beschleunigen CodeBuild. Dieses Muster konzentriert sich auf die Bereitstellung von Mainframe-Anwendungen in der AWS-Produktionsumgebung, um eine hohe Verfügbarkeit und Ausfallsicherheit zu erreichen.

In einer Mainframe-Produktionsumgebung haben Sie IBM Parallel Sysplex möglicherweise auf dem Mainframe eingerichtet, um eine hohe Leistung und hohe Verfügbarkeit zu erzielen. Um eine Scale-Out-Architektur ähnlich wie Sysplex zu erstellen, führte Micro Focus den Performance and Availability Cluster (PAC) auf Enterprise Server ein. PACs unterstützen die Bereitstellung von Mainframe-Anwendungen in mehreren Enterprise Server-Regionen, die als einzelnes Image verwaltet und in Amazon EC2-Instances skaliert werden. PACs unterstützen auch eine vorhersehbare Anwendungsleistung und einen Systemdurchsatz bei Bedarf.

In einem PAC arbeiten mehrere Enterprise Server-Instances als eine einzige logische Entität zusammen. Wenn eine Enterprise Server-Instance ausfällt, wird die Geschäftskontinuität daher nicht unterbrochen, da die Kapazität mit anderen Regionen geteilt wird, während neue Instances automatisch mit der Verwendung von branchenüblichen Funktionen wie einer Amazon EC2 Auto Scaling-Gruppe beginnen. Dadurch werden einzelne Fehlerpunkte entfernt und die Ausfallsicherheit

gegenüber Hardware-, Netzwerk- und Anwendungsproblemen verbessert. Aufskalierte Enterprise Server-Instances können mithilfe der Enterprise Server Common Web Administration (ESCWA)-APIs betrieben und verwaltet werden, wodurch die betriebliche Wartung und Servicefähigkeit von Enterprise Servers vereinfacht werden.

Hinweis: Micro Focus empfiehlt, dass der Leistungs- und Verfügbarkeitscluster (CCP) aus mindestens drei Enterprise-Server-Regionen bestehen sollte, damit die Verfügbarkeit nicht beeinträchtigt wird, falls eine Enterprise-Server-Region ausfällt oder gewartet werden muss.

Die PAC-Konfiguration erfordert einen unterstützten relationalen Datenbankverwaltungsservice (RDBMS), um die Regionsdatenbank, eine regionsübergreifende Datenbank und optionale Datenspeicherdatenbanken zu verwalten. Eine Datenspeicherdatenbank sollte für verwaltete Virtual Storage Access Method (VSAM)-Dateien verwendet werden, die die Micro Focus Database File Handler-Unterstützung verwenden, um die Verfügbarkeit und Skalierbarkeit zu verbessern. Zu den unterstützten RDBMSs gehören:

- Microsoft SQL Server 2009 R2 und höher
- PostgreSQL 10.x, einschließlich Amazon Aurora PostgreSQL – kompatible Edition
- DB2 10.4 und höher

Einzelheiten zu den unterstützten RDBMS- und PAC-Anforderungen finden Sie unter Micro Focus Enterprise Server – Voraussetzungen und Micro Focus Enterprise Server – Empfohlene PAC-Konfiguration.

Das folgende Diagramm zeigt ein typisches AWS-Architektur-Setup für einen Micro Focus PAC.

	Komponente	Beschreibung
1	Automatische Skalierungsgruppe für Enterprise Server-Instances	Richten Sie eine Auto-Scaling-Gruppe ein, die mit Enterprise-Server-Instances in einem PAC bereitgestellt wird. Die Anzahl der Instances kann mithilfe von CloudWatch Metriken nach oben oder unten skaliert werden, die von

		Amazon- CloudWatch Alarmen initiiert werden.
2	Automatische Skalierun gsgruppe für Enterprise Server ESCWA-Instances	Richten Sie eine Auto Scaling-Gruppe ein, die mit Enterpris e Server Common Web Administration (ESCWA) bereitgestellt wird. ESCWA bietet Cluster-Management -APIs. Die ESCWA-Server fungieren als Steuerebene, um Enterprise Server hinzuzufü gen oder zu entfernen und Enterprise Server-Regionen im PAC während der automatis chen Skalierungsereigni sse der Enterprise Server-Instance zu starten oder zu stoppen. Da die ESCWA-Ins tance nur für die PAC-Verwa ltung verwendet wird, ist ihr Verkehrsmuster vorhersehbar und der gewünschte Kapazität sbedarf für die automatis che Skalierung kann auf 1 festgelegt werden.
3	Amazon-Aurora-Instance in einer Multi-AZ-Einrichtung	Richten Sie ein relationa les Datenbankmanagemen tsystem (RDBMS) ein, um sowohl Benutzer- als auch Systemdatendateien zu hosten, die für die Enterprise-Server-Instances freigegeben werden sollen.

4	Amazon ElastiCache -for-Redis-Instance und -Replikat	Richten Sie eine primäre ElastiCache Redis-Instance und mindestens ein Replikat ein, um Benutzerdaten zu hosten und als Scale-Out -Repository (SOR) für die Enterprise Server-Instances zu fungieren. Sie können ein oder mehrere Scale-Out -Repositorys konfigurieren, um bestimmte Arten von Benutzerdaten zu speichern. Enterprise Server verwendet eine Redis-NoSQL-Datenbank als SOR, eine Anforderung zur Aufrechterhaltung der PAC-Integrität.
5	Network Load Balancer	Richten Sie einen Load Balancer ein, der einen Hostnamen für Anwendungen bereitstellt, um eine Verbindung zu den von Enterprise Server-Instances bereitgestellten Services herzustellen (z. B. den Zugriff auf die Anwendung über einen 3270-Emulator).

Diese Komponenten stellen die Mindestanforderung für einen Micro Focus Enterprise Server PAC-Cluster dar. Der nächste Abschnitt behandelt die Automatisierung der Clusterverwaltung.

Verwenden von AWS Systems Manager Automation für die Skalierung

Nachdem der PAC-Cluster auf AWS bereitgestellt wurde, wird der PAC über die Enterprise Server Common Web Administration (ESCWA)-APIs verwaltet.

Um die Cluster-Verwaltungsaufgaben bei automatischen Skalierungsereignissen zu automatisieren, können Sie Systems Manager Automation-Runbooks und Amazon EC2 Auto Scaling mit Amazon verwenden EventBridge. Die Architektur dieser Automatisierungen ist im folgenden Diagramm dargestellt.

	Komponente	Beschreibung
1	Lebenszyklus-Hook für die automatische Skalierung	Richten Sie Auto-Scaling-Lebenszyklus-Hooks ein und senden Sie Benachrichtigungen an Amazon, EventBridge wenn neue Instances gestartet werden und vorhandene Instances in der Auto-Scaling-Gruppe beendet werden.
2	Amazon EventBridge	Richten Sie eine Amazon-EventBridge Regel ein, um automatische Skalierungsereignisse an Systems Manager Automation-Runbook-Ziele weiterzuleiten.
3	Automation-Runbooks	Richten Sie Systems Manager Automation-Runbooks ein, um Windows- PowerShell Skripts auszuführen und ESCWA-APIs aufzurufen, um den PAC zu verwalten. Beispiele finden Sie im Abschnitt Zusätzliche Informationen.
4	Enterprise Server ESCWA-Instance in einer Auto-Scaling-Gruppe	Richten Sie eine Enterprise Server ESCWA-Instance in einer Auto-Scaling-Gruppe ein.

	Die ESCWA-Instance stellt APIs zur Verwaltung des PAC bereit.

Tools

- Micro Focus Enterprise Server – Micro Focus Enterprise Server bietet die Ausführungsumgebung für Anwendungen, die mit jeder IDE-Variante (integrierte Entwicklungsumgebung) von Enterprise Developer erstellt wurden.
- Amazon EC2 Auto Scaling – Mit Amazon EC2 Auto Scaling können Sie sicherstellen, dass Sie über die richtige Anzahl von Amazon EC2-Instances verfügen, um die Last Ihrer Anwendung zu bewältigen. Sie erstellen Sammlungen von EC2-Instances, die als Auto Scaling-Gruppen bezeichnet werden, und geben die minimale und maximale Anzahl von Instances an.
- Amazon ElastiCache for Redis – Amazon ElastiCache ist ein Webservice zum Einrichten, Verwalten und Skalieren eines verteilten In-Memory-Datenspeichers oder einer Cache-Umgebung in der Cloud. Es handelt sich um eine leistungsstarke, skalierbare und kostengünstige Caching-Lösung.
- Amazon RDS – Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der AWS Cloud vereinfacht. Es bietet kostengünstige, anpassbare Kapazität für eine relationale Datenbank und verwaltet allgemeine Datenbankverwaltungsaufgaben.
- AWS Systems Manager – AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur in AWS anzeigen und steuern können. Mit der Systems Manager-Konsole können Sie Betriebsdaten aus mehreren AWS-Services anzeigen und Betriebsaufgaben in Ihren AWS-Ressourcen automatisieren. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem er Ihre verwalteten Instances scannt und über festgestellte Richtlinienverstöße (oder Abhilfemaßnahmen ergreifen) berichtet.

Polen

Erstellen einer Amazon Aurora-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS-CloudFormation Vorlage für eine Amazon Aurora-Instance.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine CloudFormation Vorlage zu erstellen, die eine Amazon Aurora PostgreSQL -kompatible Edition-Instance erstellt.	Cloud-Architekt
Stellen Sie einen CloudFormation Stack bereit, um die Amazon-Aurora-Instance zu erstellen.	Verwenden Sie die CloudFormation Vorlage , um eine Aurora PostgreSQL kompatible Instance zu erstellen, für die die Multi-AZ-Replikation für Produktions-Workloads aktiviert ist.	Cloud-Architekt
Konfigurieren Sie die Datenbankverbindungseinstellungen für Enterprise Server.	Folgen Sie den Anweisungen in der Micro-Focus-Dokumentation, um die Verbindungszeichenfolgen und die Datenbankkonfiguration für Micro Focus Enterprise Server vorzubereiten.	Dateningenieur, DevOps Techniker

Erstellen eines Amazon- ElastiCache Clusters für die Redis-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für den Amazon-ElastiCache Cluster für die Redis-Instance.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine CloudFormation Vorlage zu erstellen, die einen	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon- ElastiCache Cluster für die Redis-Instance erstellt.	
Stellen Sie den CloudFormation Stack bereit, um einen Amazon- ElastiCache Cluster für die Redis-Instance zu erstellen.	Erstellen Sie den Amazon-ElastiCache Cluster für die Redis-Instance, für die die Multi-AZ-Replikation für Produktions-Workloads aktiviert ist.	Cloud-Architekt
Konfigurieren Sie die PSOR-Verbindungseinstellungen für Enterprise Server.	Folgen Sie den Anweisungen in der Micro-Focus-Dokumentation, um die Konfiguration des PAC Scale-Out Repository (PSOR)-Verbindung für Micro Focus Enterprise Server PAC vorzubereiten.	DevOps Techniker

Erstellen einer ESCWA-Auto-Scaling-Gruppe für Micro Focus Enterprise Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Micro Focus Enterprise Server-AMI.	Erstellen Sie eine Amazon EC2 Windows Server-Instance und installieren Sie die Micro Focus Enterprise Server-Binärdatei in der EC2-Instance. Erstellen Sie ein Amazon Machine Image (AMI) der EC2-Instance. Weitere Informationen finden Sie in derEnterprise Server-Installationsdokumentation.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für Enterprise Server ESCWA.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine Vorlage für die Erstellung eines benutzerdefinierten Stacks von Enterprise Server ESCWA in einer Auto Scaling-Gruppe zu erstellen.	Cloud-Architekt
Stellen Sie den CloudFormation Stack bereit, um eine Amazon EC2-Skalierungsgruppe für Enterprise Server ESCWA zu erstellen.	Verwenden Sie die CloudFormation Vorlage, um die Auto-Scaling-Gruppe mit dem in der vorherigen Geschichte erstellten ESCWA-AMI von Micro Focus Enterprise Server bereitzustellen.	Cloud-Architekt

Erstellen eines AWS Systems Manager Automation-Runbooks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für ein Systems Manager Automation-Runbook.	Verwenden Sie die Beispielcodeausschnitte im Abschnitt Zusätzliche Informationen, um eine CloudFormation Vorlage zu erstellen, die ein Systems Manager Automation-Runbook zur Automatisierung der PAC-Erstellung, Enterprise Server-Skalierung nach unten und Enterprise Server-Skalierung nach oben erstellt.	Cloud-Architekt
Stellen Sie den CloudFormation Stack bereit, der das	Verwenden Sie die CloudFormation Vorlage , um einen Stack bereitzustellen, der das	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Systems Manager Automation-Runbook enthält.	Automation-Runbook für die PAC-Erstellung, Enterprise Server Scale-In und Enterprise Server Scale-Out enthält.	

Erstellen einer Auto-Scaling-Gruppe für Micro Focus Enterprise Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für die Einrichtung einer Auto-Scaling-Gruppe für Micro Focus Enterprise Server.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine CloudFormation Vorlage zu erstellen, die eine Auto Scaling-Gruppe erstellt. Diese Vorlage verwendet dasselbe AMI wieder, das für die ESCWA-Instance von Micro Focus Enterprise Server erstellt wurde. Verwenden Sie dann einen AWS-Beispielcodeausschnitt, um das Auto Scaling-Lebenszyklusereignis zu erstellen und Amazon so einzurichten EventBridge , dass es nach Scale-Out- und Scale-In-Ereignissen in derselben CloudFormation Vorlage filtert.	Cloud-Architekt
Stellen Sie den CloudFormation Stack für die Auto-Scaling-Gruppe für Micro Focus Enterprise Servers bereit.	Stellen Sie den CloudFormation Stack bereit, der die Auto-Scaling-Gruppe für	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Micro Focus Enterprise Server enthält.	

Zugehörige Ressourcen

- Micro Focus Enterprise Server – Leistungs- und Verfügbarkeitscluster (PAC)
- Lebenszyklus-Hooks für Amazon EC2 Auto Scaling
- Ausführen von Automatisierungen mit Auslösern unter Verwendung von EventBridge

Zusätzliche Informationen

Die folgenden Szenarien müssen automatisiert sein, um die PAC-Cluster zu vergrößern oder zu verkleinern.

Automatisierung zum Starten oder Neuerstellen eines PAC

Zu Beginn eines PAC-Clusters erfordert Enterprise Server, dass ESCWA APIs aufruft, um eine PAC-Konfiguration zu erstellen. Dies startet und fügt Enterprise Server-Regionen zum PAC hinzu. Gehen Sie wie folgt vor, um einen PAC zu erstellen oder neu zu erstellen:

1. Konfigurieren Sie ein PAC Scale-Out Repository (PSOR) in ESCWA mit einem bestimmten Namen.

```
POST /server/v1/config/groups/sors
```

2. Erstellen Sie einen PAC mit einem bestimmten Namen und fügen Sie ihm den PSOR hinzu.

```
POST /server/v1/config/groups/pacs
```

3. Konfigurieren Sie die Regionsdatenbank und die regionsübergreifende Datenbank, wenn Sie zum ersten Mal einen PAC einrichten.

   Hinweis: In diesem Schritt werden SQL-Abfragen und das Micro Focus Enterprise Suite-Befehlszeilen-Tool dbhfhadmin verwendet, um die Datenbank zu erstellen und Anfangsdaten zu importieren.

4. Installieren Sie die PAC-Definition in den Enterprise Server-Regionen.

```
POST /server/v1/config/mfds
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

5. Starten Sie Enterprise Server-Regionen im PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

Die vorherigen Schritte können mithilfe eines Windows- PowerShell Skripts implementiert werden.

In den folgenden Schritten wird erläutert, wie Sie eine Automatisierung für die Erstellung eines PAC mithilfe des Windows- PowerShell Skripts erstellen.

1. Erstellen Sie eine Amazon EC2-Startvorlage, die das Windows-PowerShell Skript im Rahmen des Bootstrap-Prozesses herunterlädt oder erstellt. Sie können beispielsweise EC2-Benutzerdaten verwenden, um das Skript aus einem Amazon Simple Storage Service (Amazon S3)-Bucket herunterzuladen.
2. Erstellen Sie ein AWS Systems Manager Automation-Runbook, um das Windows- PowerShell Skript aufzurufen.
3. Verknüpfen Sie das Runbook mit der ESCWA-Instance mithilfe des Instance-Tags.
4. Erstellen Sie eine ESCWA-Auto-Scaling-Gruppe mithilfe der Startvorlage.

Sie können den folgenden AWS CloudFormation -Beispielausschnitt verwenden, um das Automation-Runbook zu erstellen.

Beispielausschnitt für ein Systems Manager Automation-Runbook CloudFormation , das für die PAC-Erstellung verwendet wird

```
PACInitDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to create Enterprise Server PAC
       mainSteps:
       - action: aws:runPowerShellScript
         name: CreatePAC
         inputs:
```

```
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              C:\Scripts\PAC-Init.ps1
  PacInitAutomation:
     Type: AWS::SSM::Document
     Properties:
       DocumentType: Automation
       Content:
         description: Prepare Micro Focus PAC Cluster via ESCWA Server
         schemaVersion: '0.3'
         assumeRole: !GetAtt SsmAssumeRole.Arn
         mainSteps:
           - name: RunPACInitDocument
             action: aws:runCommand
             timeoutSeconds: 300
             onFailure: Abort
             inputs:
               DocumentName: !Ref PACInitDocument
               Targets:
                 - Key: tag:Enterprise Server - ESCWA
                   Values:
                     - "true"
   PacInitDocumentAssociation:
     Type: AWS::SSM::Association
     Properties:
       DocumentVersion: "$LATEST"
       Name: !Ref PACInitDocument
       Targets:
         - Key: tag:Enterprise Server - ESCWA
           Values:
             - "true"
```

Weitere Informationen finden Sie unter Micro Focus Enterprise Server – Konfigurieren eines CCP.

Automatisierung für die Skalierung mit einer neuen Enterprise Server-Instance

Wenn eine Enterprise-Server-Instance skaliert wird, muss ihre Enterprise-Server-Region zum PAC hinzugefügt werden. In den folgenden Schritten wird erläutert, wie Sie ESCWA-APIs aufrufen und die Enterprise-Server-Region zum PAC hinzufügen.

1. Installieren Sie die PAC-Definition in den Enterprise Server-Regionen.

```
POST '/server/v1/config/mfds'
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

2. Warm Starten Sie die Region im PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

3. Fügen Sie die Enterprise Server-Instance dem Load Balancer hinzu, indem Sie die Auto-Scaling-Gruppe dem Load Balancer zuordnen.

Die vorherigen Schritte können mithilfe eines Windows- PowerShell Skripts implementiert werden. Weitere Informationen finden Sie unter Micro Focus Enterprise Server – Konfigurieren eines CCP.

Die folgenden Schritte können verwendet werden, um eine ereignisgesteuerte Automatisierung zu erstellen, um eine neu gestartete Enterprise Server-Instance mithilfe des Windows- PowerShell Skripts zu einem PAC hinzuzufügen.

1. Erstellen Sie eine Amazon EC2-Startvorlage für Enterprise Server-Instance, die während ihres Bootstraps eine Enterprise Server-Region bereitstellt. Sie können beispielsweise den Micro Focus Enterprise Server-Befehl mfds verwenden, um eine Regionskonfiguration zu importieren. Weitere Informationen und Optionen, die für diesen Befehl verfügbar sind, finden Sie in der Enterprise Server-Referenz .
2. Erstellen Sie eine Auto-Scaling-Gruppe für Enterprise Server, die die im vorherigen Schritt erstellte Startvorlage verwendet.
3. Erstellen Sie ein Systems Manager Automation-Runbook, um das Windows- PowerShell Skript aufzurufen.
4. Verknüpfen Sie das Runbook mit der ESCWA-Instance mithilfe des Instance-Tags.
5. Erstellen Sie eine Amazon- EventBridge Regel, um nach dem Ereignis Erfolgreiches Starten der EC2-Instance für die Auto-Scaling-Gruppe von Enterprise Server zu filtern, und erstellen Sie das Ziel, um das Automation-Runbook zu verwenden.

Sie können den folgenden Beispielausschnitt verwenden CloudFormation , um das Automation-Runbook und die EventBridge Regel zu erstellen.

Beispielausschnitt für Systems Manager, CloudFormation der zum Skalieren von Enterprise Server-Instances verwendet wird

```
  ScaleOutDocument:
     Type: AWS::SSM::Document
     Properties:
       DocumentType: Command
       Content:
         schemaVersion: '2.2'
         description: Operation Runbook to Adding MFDS Server into an existing PAC
         parameters:
           MfdsPort:
             type: String
           InstanceIpAddress:
             type: String
             default: "Not-Available"
           InstanceId:
             type: String
             default: "Not-Available"
         mainSteps:
         - action: aws:runPowerShellScript
           name: Add_MFDS
           inputs:
             onFailure: Abort
             timeoutSeconds: "300"
             runCommand:
             - |
               $ip = "{{InstanceIpAddress}}"
               if ( ${ip} -eq "Not-Available" ) {
                 $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
               }
               C:\Scripts\Scale-Out.ps1 -host_ip ${ip} -port {{MfdsPort}}

   PacScaleOutAutomation:
     Type: AWS::SSM::Document
     Properties:
       DocumentType: Automation
       Content:
         parameters:
           MfdsPort:
             type: String
           InstanceIpAddress:
             type: String
             default: "Not-Available"
           InstanceId:
```

```
            type: String
            default: "Not-Available"
        description: Scale Out 1 New Server in Micro Focus PAC Cluster via ESCWA
Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleOutCommand
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleOutDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                InstanceId: "{{InstanceId}}"
                MfdsPort: "{{MfdsPort}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
```

Automatisierung für die Skalierung in einer Enterprise Server-Instance

Ähnlich wie beim Aufskalieren wird bei der Skalierung einer Enterprise Server-Instance in das Ereignis EC2 Instance-terminate Lifecycle Action initiiert und die folgenden Prozess- und API-Aufrufe sind erforderlich, um eine Micro Focus Enterprise Server-Instance aus dem PAC zu entfernen.

1. Halten Sie die Region in der beendenden Enterprise Server-Instance an.

```
POST "/native/v1/regions/${host_ip}/${port}/${region_name}/stop"
```

2. Entfernen Sie die Enterprise Server-Instance aus dem PAC.

```
DELETE "/server/v1/config/mfds/${uid}"
```

3. Senden Sie ein Signal, um die Enterprise Server-Instance weiter zu beenden.

Die vorherigen Schritte können in einem Windows- PowerShell Skript implementiert werden. Weitere Informationen zu diesem Prozess finden Sie unter Micro Focus Enterprise Server-Dokument – Verwalten eines PAC.

In den folgenden Schritten wird erläutert, wie Sie eine ereignisgesteuerte Automatisierung erstellen, um eine Enterprise Server-Instance aus einem PAC zu beenden, indem Sie das Windows- PowerShell Skript wiederverwenden.

1. Erstellen Sie ein Systems Manager Automation-Runbook, um das Windows- PowerShell Skript aufzurufen.
2. Verknüpfen Sie das Runbook mit der ESCWA-Instance mithilfe des Instance-Tags.
3. Erstellen Sie einen Auto-Scaling-Gruppen-Lebenszyklus-Hook für die Beendigung einer EC2-Instance.
4. Erstellen Sie eine Amazon- EventBridge Regel, um das Ereignis EC2 Instance-terminate Lifecycle Action für die Auto-Scaling-Gruppe von Enterprise Server zu filtern, und erstellen Sie das Ziel für die Verwendung des Automation-Runbooks.

Sie können die folgende CloudFormation Beispielvorlage verwenden, um ein Systems Manager Automation-Runbook, einen Lebenszyklus-Hook und eine EventBridge Regel zu erstellen.

Beispielausschnitt für ein Systems Manager Automation-Runbook CloudFormation , das für die Skalierung einer Enterprise Server-Instance verwendet wird

```
ScaleInDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to Remove MFDS Server from PAC
       parameters:
         MfdsPort:
           type: String
         InstanceIpAddress:
           type: String
           default: "Not-Available"
         InstanceId:
           type: String
           default: "Not-Available"
       mainSteps:
       - action: aws:runPowerShellScript
         name: Remove_MFDS
         inputs:
           onFailure: Abort
```

```
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-In.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleInAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale In 1 New Server in Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleInCommand
            action: aws:runCommand
            timeoutSeconds: "600"
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleInDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                MfdsPort: "{{MfdsPort}}"
                InstanceId: "{{InstanceId}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
          - name: TerminateTheInstance
            action: aws:executeAwsApi
            inputs:
```

```
            Service: autoscaling
            Api: CompleteLifecycleAction
            AutoScalingGroupName: !Ref AutoScalingGroup
            InstanceId: "{{ InstanceId }}"
            LifecycleActionResult: CONTINUE
            LifecycleHookName: !Ref ScaleInLifeCycleHook
```

Automatisierung für einen Amazon EC2 Auto Scaling-Auslöser

Der Prozess der Einrichtung einer Skalierungsrichtlinie für Enterprise Server-Instances erfordert ein Verständnis des Anwendungsverhaltens. In den meisten Fällen können Sie Skalierungsrichtlinien für die Ziel-Nachverfolgung einrichten. Sie können beispielsweise die durchschnittliche CPU-Auslastung als Amazon- CloudWatch Metrik verwenden, um für die Auto-Scaling-Richtlinie festzulegen. Weitere Informationen finden Sie unter Skalierungsrichtlinien für die Zielverfolgung für Amazon EC2 Auto Scaling. Für Anwendungen mit regelmäßigen Datenverkehrsmustern sollten Sie eine prädiktive Skalierungsrichtlinie verwenden. Weitere Informationen finden Sie unter Prädiktive Skalierung für Amazon EC2 Auto Scaling.

Erstellen einer Serverless-Architektur mit mehreren Mandanten in Amazon OpenSearch Service

Erstellt von Tabby Ward (AWS) und Nisha Gambhir (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; SaaS; Serverless	Workload: Open-Source
AWS-Services: Amazon OpenSearch Service; AWS Lambda ;Amazon S3; Amazon API Gateway		

Übersicht

Amazon OpenSearch Service ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von Elasticsearch, einer beliebten Open-Source-Such- und Analyse-Engine, vereinfacht. Amazon OpenSearch Service bietet Freitextsuche sowie Erfassung und Dashboarding für Streaming-Daten wie Protokolle und Metriken nahezu in Echtzeit.

Software-as-a-Service (SaaS)-Anbieter verwenden Amazon OpenSearch Service häufig, um eine breite Palette von Anwendungsfällen zu bewältigen, z. B. um Kundeneinblicke auf skalierbare und sichere Weise zu gewinnen und gleichzeitig Komplexität und Ausfallzeiten zu reduzieren.

Die Verwendung von Amazon OpenSearch Service in einer mandantenfähigen Umgebung führt eine Reihe von Überlegungen ein, die sich auf Partitionierung, Isolation, Bereitstellung und Verwaltung Ihrer SaaS-Lösung auswirken. SaaS-Anbieter müssen überlegen, wie sie ihre Elasticsearch-Cluster mit sich ständig ändernden Workloads effektiv skalieren können. Sie müssen auch überlegen, wie sich Tiering und verrauschte Nachbarbedingungen auf ihr Partitionierungsmodell auswirken könnten.

Dieses Muster überprüft die Modelle, die verwendet werden, um Tenant-Daten mit Elasticsearch-Konstrukten darzustellen und zu isolieren. Darüber hinaus konzentriert sich das Muster auf eine einfache Serverless-Referenzarchitektur als Beispiel, um die Indizierung und Suche mit Amazon OpenSearch Service in einer mandantenfähigen Umgebung zu demonstrieren. Es implementiert das Pool-Datenpartitionierungsmodell, das denselben Index für alle Mandanten verwendet und gleichzeitig die Datenisolierung eines Mandanten beibehält. Dieses Muster verwendet die folgenden

Amazon Web Services (AWS)-Services: Amazon API Gateway ,AWS Lambda, Amazon Simple Storage Service (Amazon S3) und Amazon OpenSearch Service .

Weitere Informationen zum Poolmodell und anderen Datenpartitionierungsmodellen finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2.x, installiert und konfiguriert unter macOS , Linux oder Windows
- Python-Version 3.7
- pip3 – Der Python-Quellcode wird als ZIP-Datei bereitgestellt, die in einer Lambda-Funktion bereitgestellt werden soll. Wenn Sie den Code lokal verwenden oder anpassen möchten, führen Sie die folgenden Schritte aus, um den Quellcode zu entwickeln und neu zu kompilieren:
  1. Generieren Sie die `requirements.txt` Datei, indem Sie den folgenden Befehl im selben Verzeichnis wie die Python-Skripte ausführen: `pip3 freeze > requirements.txt`
  2. Installieren Sie die Abhängigkeiten: `pip3 install -r requirements.txt`

Einschränkungen

- Dieser Code wird in Python ausgeführt und unterstützt derzeit keine anderen Programmiersprachen.
- Die Beispielanwendung beinhaltet keine regionsübergreifende AWS- oder Notfallwiederherstellungs-(DR)-Unterstützung.
- Dieses Muster dient nur zu Demonstrationszwecken. Es ist nicht für die Verwendung in einer Produktionsumgebung vorgesehen.

Architektur

Das folgende Diagramm veranschaulicht die High-Level-Architektur dieses Musters. Die Architektur umfasst Folgendes:

- AWS Lambda zum Indizieren und Abfragen des Inhalts

- Amazon OpenSearch Service zur Durchführung der Suche
- Amazon API Gateway zur Bereitstellung einer API-Interaktion mit dem Benutzer
- Amazon S3 zum Speichern von Rohdaten (nicht indiziert)
- Amazon CloudWatch zur Überwachung von Protokollen
- AWS Identity and Access Management (IAM) zum Erstellen von Mandantenrollen und -richtlinien

Automatisierung und Skalierung

Der Einfachheit halber verwendet das Muster AWS CLI, um die Infrastruktur bereitzustellen und den Beispielcode bereitzustellen. Sie können eine AWS- CloudFormation Vorlage oder AWS Cloud Development Kit (AWS CDK)-Skripte erstellen, um das Muster zu automatisieren.

Tools

AWS-Services

- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung von AWS-Services und -Ressourcen mithilfe von Befehlen in Ihrer Befehlszeilen-Shell.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon API Gateway – Amazon API Gateway ist ein AWS-Service zum Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST-, HTTP- und - WebSocket APIs in jeder Größenordnung.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, mit dem Sie jederzeit und von überall im Internet beliebige Informationen speichern und abrufen können.
- Amazon OpenSearch Service – Amazon OpenSearch Service ist ein vollständig verwalteter Service, mit dem Sie Elasticsearch kostengünstig und in großem Umfang bereitstellen, sichern und ausführen können.

Code

Der Anhang enthält Beispieldateien für dieses Muster. Dazu zählen:

- `index_lambda_package.zip` – Die Lambda-Funktion zur Indizierung von Daten in Amazon OpenSearch Service mithilfe des Poolmodells.
- `search_lambda_package.zip` – Die Lambda-Funktion für die Suche nach Daten in Amazon OpenSearch Service.
- `Tenant-1-data` – Beispiel-Rohdaten (nicht indiziert) für Tenant-1.
- `Tenant-2-data` – Beispiel-Rohdaten (nicht indiziert) für Tenant-2.

Wichtig: Die Geschichte in diesem Muster enthält CLI-Befehlsbeispiele, die für Unix, Linux und macOS formatiert sind. Ersetzen Sie unter Windows den umgekehrten Schrägstrich (\), das Unix-Fortsetzungszeichen, am Ende jeder Zeile durch ein Caret-Zeichen oder Zirkumflex (^).

Polen

Erstellen und Konfigurieren eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket in Ihrer AWS-Region. Dieser Bucket enthält die nicht indizierten Mandantendaten für die Beispielanwendung. Stellen Sie sicher, dass der Name des S3-Buckets global eindeutig ist, da der Namespace von allen AWS-Konten gemeinsam genutzt wird. Um einen S3-Bucket zu erstellen, können Sie den AWS CLI-Befehl create-bucket wie folgt verwenden: `aws s3api create-bucket \`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--bucket tenantraw data \ --region <your-AWS-Region>` wobei der Name des S3-Buckets `tenantraw data` ist. (Sie können jeden eindeutigen Namen verwenden, der den Bucket-Namensrichtlinien folgt.)	

Erstellen und Konfigurieren eines Elasticsearch-Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon-OpenSearch Service-Domain.	Führen Sie den AWS CLI-create-elasticsearch-domainBefehl aus, um eine Amazon OpenSearch Service-Domäne zu erstellen: `aws es create-elasticsearch-domain \ --domain-name vpc-cli-example \ --elasticsearch-version 7.10 \ --elasticsearch-cluster-config InstanceType=t3.medium.elasticsearch,InstanceCount=1 \ --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=10 \`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--domain-endpoint-options "{\"EnforceHTTPS\": true}" \ --encryption-at-rest-options "{\"Enabled\": true}" \ --node-to-node-encryption-options "{\"Enabled\": true}" \ --advanced-security-options "{\"Enabled\": true, \"InternalUserDatabaseEnabled\": true, \ \"MasterUserOptions\": {\"MasterUserName\": \"KibanaUser\", \ \"MasterUserPassword\": \"NewKibanaPassword@123\"}}" \ --vpc-options "{\"SubnetIds\": [\"<subnet-id>\"], \"SecurityGroupIds\": [\"<sg-id>\"]}" \ --access-policies "{\"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \ \"Principal\": {\"AWS\": \"*\" }, \"Action\":\"es:*\", \ \"Resource\": \"arn:aws:es:region:account-id:domain\/vpc-cli-example\/*\" }] }"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Anzahl der Instances ist auf 1 gesetzt, da die Domain zu Testzwecken bestimmt ist. Sie müssen die differenz ierte Zugriffskontrolle mithilfe des `advanced-security-options` Parameters aktivieren, da die Details nach der Erstellung der Domain nicht mehr geändert werden können. Dieser Befehl erstellt einen Masterbenutzernamen (`KibanaUser`) und ein Passwort, mit dem Sie sich bei der Kibana-Konsole anmelden können. Da die Domain Teil einer Virtual Private Cloud (VPC) ist, müssen Sie sicherstellen, dass Sie die Elasticsearch-Instance erreichen können, indem Sie die zu verwendende Zugriffsrichtlinie angeben. Weitere Informationen finden Sie unter Starten Ihrer Amazon OpenSearch Service-Domains mit einer VPC in der AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie einen Bastion-Host ein.	Richten Sie eine Amazon Elastic Compute Cloud (Amazon EC2)-Windows-Instance als Bastion-Host für den Zugriff auf die Kibana-Konsole ein. Die Elasticsearch-Sicherheitsgruppe muss Datenverkehr von der Amazon EC2-Sicherheitsgruppe zulassen. Anweisungen finden Sie im Blogbeitrag Controlling Network Access to EC2 Instances Using a Bastion Server .
	
	Wenn der Bastion-Host eingerichtet wurde und Sie die Sicherheitsgruppe haben, die der Instance zugeordnet ist, verwenden Sie den AWS CLI-authorize-security-group-ingressBefehl , um der Elasticsearch-Sicherheitsgruppe die Berechtigung hinzuzufügen, um Port 443 von der Amazon EC2-Sicherheitsgruppe (Bastion-Host) zuzulassen.
	
	`aws ec2 authorize-security-group-ingress \`
	`  --group-id <SecurityGroupIdfElasticSearch> \`
	`  --protocol tcp \`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--port 443 \` `--source-group <SecurityGroupIdfBashionHostEC2>`	

Erstellen und Konfigurieren der Lambda-Indexfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Lambda-Ausführungsrolle.	Führen Sie den AWS CLI-Befehl create-role aus, um der Lambda-Indexfunktion Zugriff auf AWS-Services und -Ressourcen zu gewähren:
	`aws iam create-role \`
	`--role-name index-lambda-role \`
	`--assume-role-policy-document file://lambda_assume_role.json`
	wobei ein JSON-Dokument im aktuellen Ordner `lambda_assume_role.json` ist, das `AssumeRole` Berechtigungen für die Lambda-Funktion wie folgt erteilt:
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Effect": "Allow",`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Principa
	l": {
	
	  "Service": "lambda.a
	mazonaws.com"
	  },
	"Action":
	 "sts:AssumeRole"
	  }
	  ]
	 }</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie der Lambda-Rolle verwaltete Richtlinien hinzu.	Führen Sie den AWS CLI-attach-role-policyBefehl aus, um verwaltete Richtlinien an die im vorherigen Schritt erstellte Rolle anzuhänge n. Diese beiden Richtlinien erteilen der Rolle Berechtig ungen zum Erstellen einer Elastic Network-Schnittste lle und zum Schreiben von Protokollen in CloudWatch - Protokolle.
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Cloud-Architekt, Cloud-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Richtlinie, um der Lambda-Indexfunktion die Berechtigung zum Lesen der S3-Objekte zu erteilen.	Führen Sie den AWS CLI-Befehl create-policy für aus, um der Lambda-Indexfunktion die `s3:GetObject` Berechtigung zum Lesen der Objekte im S3-Bucket zu erteilen:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3-policy.json`
	Die Datei `s3-policy.json` ist ein JSON-Dokument im aktuellen Ordner, das `s3:GetObject` Berechtigungen erteilt, um Lesezugriff auf S3-Objekte zu gewähren. Wenn Sie bei der Erstellung des S3-Buckets einen anderen Namen verwendet haben, geben Sie den richtigen Bucket-Namen im `Resource` Abschnitt im Folgenden an:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject",`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Resource
	": "arn:aws:s3:::tena
	ntrawdata/*"
	}
	]
	}</pre>	

Fügen Sie die Amazon S3-Berechtigungsrichtlinie an die Lambda-Ausführungsrolle an.	Führen Sie den AWS CLI-attach-role-policyBefehl aus, um die Amazon S3-Berechtigungsrichtlinie, die Sie im vorherigen Schritt erstellt haben, an die Lambda-Ausführungsrolle anzuhängen:
	<pre>aws iam attach-role-policy \
	--role-name index-lambda-role \
	--policy-arn <PolicyARN></pre>
	wobei der Amazon-Ressourcenname (ARN) der Amazon S3-Berechtigungsrichtlinie `PolicyARN` ist. Sie können diesen Wert aus der Ausgabe des vorherigen Befehls abrufen.
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Lambda-Indexfunktion.	Führen Sie den AWS CLI-Befehl create-function aus, um die Lambda-Indexfunktion zu erstellen, die auf Amazon OpenSearch Service zugreift:
	`aws lambda create-function \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip \`
	`  --handler lambda_index.lambda_handler \`
	`  --runtime python3.7 \`
	`  --role "arn:aws:iam::account-id:role/index-lambda-role" \`
	`  --timeout 30 \`
	`  --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \`
	`  \"SecurityGroupIds\": [\"<sg-1>\"]}"`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erlauben Sie Amazon S3, die Lambda-Indexfunktion aufzurufen.	Führen Sie den AWS CLI-Befehl add-permission aus, um Amazon S3 die Berechtigung zum Aufrufen der Lambda-Indexfunktion zu erteilen: `aws lambda add-permission \ --function-name index-lambda-function \ --statement-id s3-permissions \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn "arn:aws:s3:::tentrawdata" \ --source-account "<account-id>"`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Lambda-Auslöser für das Amazon S3-Ereignis hinzu.	Führen Sie den AWS CLI-put-bucket-notification-configuration Befehl aus, um Benachrichtigungen an die Lambda-Indexfunktion zu senden, wenn das Amazon S3-`ObjectCreated` Ereignis erkannt wird. Die Indexfunktion wird ausgeführt, wenn ein Objekt in den S3-Bucket hochgeladen wird. `aws s3api put-bucket-notification-configuration \ --bucket tenantrawdata \ --notification-configuration file://s3-trigger.json` Die Datei `s3-trigger.json` ist ein JSON-Dokument im aktuellen Ordner, das die Ressourcenrichtlinie zur Lambda-Funktion hinzufügt, wenn das Amazon S3-`ObjectCreated` Ereignis eintritt.	Cloud-Architekt, Cloud-Administrator

Erstellen und Konfigurieren der Lambda-Suchfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Lambda-Ausführungsrolle.	Führen Sie den AWS CLI-Befehl create-role aus, um der Lambda-Suchfunktion Zugriff auf AWS-Services und -Ressourcen zu gewähren:
	`aws iam create-role \ --role-name search-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	wobei ein JSON-Dokument im aktuellen Ordner `lambda_assume_role.json` ist, das `AssumeRole` Berechtigungen für die Lambda-Funktion wie folgt erteilt:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>] }</pre>	

Hängen Sie verwaltete Richtlinien an die Lambda-Rolle an.	Führen Sie den AWS CLI-attach-role-policyBefehl aus, um verwaltete Richtlinien an die im vorherigen Schritt erstellte Rolle anzuhängen. Diese beiden Richtlinien erteilen der Rolle Berechtigungen zum Erstellen einer Elastic Network-Schnittstelle und zum Schreiben von Protokollen in CloudWatch Protokolle.
	<pre>aws iam attach-role-policy \
	  --role-name search-lambda-role \
	  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
	
	aws iam attach-role-policy \
	  --role-name search-lambda-role \
	  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole</pre>
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lambda-Suchfunktion.	Führen Sie den AWS CLI-Befehl create-function aus, um die Lambda-Suchfunktion zu erstellen, die auf Amazon OpenSearch Service zugreift: `aws lambda create-function \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip \ --handler lambda_search.lambda_handler \ --runtime python3.7 \ --role "arn:aws:iam::account-id:role/search-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Cloud-Architekt, Cloud-Administrator

Erstellen und Konfigurieren von Tenant-Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Tenant-IAM-Rollen.	Führen Sie den AWS CLI-Befehl create-role aus, um zwei Tenant-Rollen zu erstellen, die zum Testen	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	der Suchfunktion verwendet werden:
	
	`aws iam create-role \ --role-name Tenant-1-role \ --assume-role-policy-document file://assume-role-policy.json`
	
	`aws iam create-role \ --role-name Tenant-2-role \ --assume-role-policy-document file://assume-role-policy.json`
	
	Die Datei `assume-role-policy.json` ist ein JSON-Dokument im aktuellen Ordner, das der Lambda-Ausführungsrolle `AssumeRole` Berechtigungen erteilt:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "<Lambda execution role for index function>", "AWS": "<Lambda execution role for search function>"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>},
	"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Tenant-IAM-Richtlinie.	Führen Sie den AWS CLI-Befehl create-policy aus, um eine Tenant-Richtlinie zu erstellen, die Zugriff auf Elasticsearch-Operationen gewährt:
	`aws iam create-policy \ --policy-name tenant-policy \ --policy-document file://policy.json`
	Die Datei `policy.json` ist ein JSON-Dokument im aktuellen Ordner, das Berechtigungen für Elasticsearch erteilt:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpDelete", "es:ESHttpGet", "es:ESHttpHead", "es:ESHttpPost", "es:ESHttpPut",`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"es:ESHttpPatch"
	            ],
	            "Resource":
	[
	                "<ARN of
	Elasticsearch domain
	created earlier>"
	            ]
	        }
	    ]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die Tenant-IAM-Richtlinie an die Tenant-Rollen an.	Führen Sie den AWS CLI-attach-role-policyBefehl aus, um die Tenant-IAM-Richtlinie an die beiden Tenant-Rollen anzuhängen, die Sie im vorherigen Schritt erstellt haben:
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/tenant-policy \`
	`  --role-name Tenant-1-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/tenant-policy \`
	`  --role-name Tenant-2-role`
	
	Der Richtlinien-ARN stammt aus der Ausgabe des vorherigen Schritts.
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Richtlinie, um Lambda Berechtigungen zur Übernahme der Rolle zu erteilen.	Führen Sie den AWS CLI-Befehl create-policy aus, um eine Richtlinie zu erstellen, damit Lambda die Tenant-Rolle übernimmt:
	`aws iam create-policy \ --policy-name assume-tenant-role-policy \ --policy-document file://lambda_policy.json`
	Die Datei `lambda_policy.json` ist ein JSON-Dokument im aktuellen Ordner, das Berechtigungen für erteilt `AssumeRole` :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<ARN of tenant role created earlier>" } ] }`
	Für können Sie ein Platzhalt erzeichen verwenden `Resource`, um zu vermeiden
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, dass für jeden Mandanten eine neue Richtlinie erstellt wird.	

Erstellen Sie eine IAM-Richtlinie, um der Lambda-Indexrolle die Berechtigung für den Zugriff auf Amazon S3 zu erteilen.	Führen Sie den AWS CLI-Befehl create-policy aus, um der Lambda-Indexrolle die Berechtigung für den Zugriff auf die Objekte im S3-Bucket zu erteilen:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3_lambda_policy.json`
	Die Datei `s3_lambda_policy.json` ist das folgende JSON-Richtliniendokument im aktuellen Ordner:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::tenantrawdata/*" } ] }`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die Richtlinie an die Lambda-Ausführungsrolle an.	Führen Sie den AWS CLI-attach-role-policyBefehl aus, um die im vorherige n Schritt erstellte Richtlini e an den Lambda-Index anzuhängen und die zuvor erstellten Ausführungsrollen zu durchsuchen:
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name index-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name search-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/s3-permission-policy \`
	`  --role-name index-lambda-role`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Richtlinien-ARN stammt aus der Ausgabe des vorherigen Schritts.	

Erstellen und Konfigurieren einer Such-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine REST-API in API Gateway.	Führen Sie den CLI-create-rest-apiBefehl aus, um eine REST-API-Ressource zu erstellen: `aws apigateway create-rest-api \ --name Test-Api \ --endpoint-configuration "{ \"types\": [\"REGIONAL\"] }"` Für den Endpunktkonfigurationstyp können Sie angeben, `EDGE` anstatt Edge-Standorte anstelle einer bestimmten AWS-Region `REGIONAL` zu verwenden. Notieren Sie sich den Wert des `id` Feldes aus der Befehlsausgabe. Dies ist die API-ID, die Sie in nachfolgenden Befehlen verwenden werden.	Cloud-Architekt, Cloud-Administrator
Erstellen Sie eine Ressource für die Such-API.	Die Such-API-Ressource startet die Lambda-Su	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	chfunktion mit dem Ressourcennamen `search`. (Sie müssen keine API für die Lambda-Indexfunktion erstellen, da sie automatisch ausgeführt wird, wenn Objekte in den S3-Bucket hochgeladen werden.)
	
	1. Führen Sie den AWS CLI-Befehl get-resources aus, um die übergeordnete ID für den Stammpfad abzurufen:
	
	`aws apigateway get-resources \`
	`  --rest-api-id <API-ID>`
	
	Notieren Sie sich den Wert des Feldes ID. Sie verwenden diese übergeordnete ID im nächsten Befehl.
	
	`{`
	`  "items": [`
	`  {`
	`  "id": "zpsri964ck",`
	`  "path": "/"`
	`  }`
	`  ]`
	`}`
	
	2. Führen Sie den AWS CLI-Befehl create-resource aus, um eine Ressource für die Such-API zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`parent-id` Geben Sie für die ID aus dem vorherigen Befehl an. `aws apigateway create-resource \ --rest-api-id <API-ID> \ --parent-id <Parent-ID> \ --path-part search`	
Erstellen Sie eine GET-Methode für die Such-API.	Führen Sie den AWS CLI-Befehl put-method aus, um eine `GET` Methode für die Such-API zu erstellen: `aws apigateway put-method \ --rest-api-id <API-ID> \ --resource-id <ID from the previous command output> \ --http-method GET \ --authorization-type "NONE" \ --no-api-key-required` `resource-id` Geben Sie für die ID aus der Ausgabe des `create-resource` Befehls an.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Methodenantwort für die Such-API.	Führen Sie den AWS CLI-put-method-responseBefehl aus, um eine Methodenantwort für die Such-API hinzuzufügen: `aws apigateway put-method-response \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --status-code 200 \ --response-models "{\"application/json\": \"Empty\"}"` `resource-id` Geben Sie für die ID aus der Ausgabe des vorherigen `create-resource` Befehls an.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine Proxy-Lambda-Integration für die Such-API ein.	Führen Sie den AWS CLI-Befehl put-integration aus, um eine Integration mit der Lambda-Suchfunktion einzurichten: `aws apigateway put-integration \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --type AWS_PROXY \ --integration-http-method GET \ --uri arn:aws:apigateway:region:lambda:path/2015-03-31/functions/arn:aws:lambda:<region>:<account-id>:function:<function-name>/invocations` `resource-id` Geben Sie für die ID aus dem vorherigen `create-resource` Befehl an.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erteilen Sie API Gateway die Berechtigung zum Aufrufen der Lambda-Suchfunktion.	Führen Sie den AWS CLI-Befehl add-permission aus, um API Gateway die Berechtigung zur Verwendung der Suchfunktion zu erteilen: `aws lambda add-permission \ --function-name <function-name> \ --statement-id apigateway-get \ --action lambda:InvokeFunction \ --principal apigateway.amazonaws.com \ --source-arn "arn:aws:execute-api:<region>:<account-id>:api-id/*/GET/search"` Ändern Sie den `source-arn` Pfad, wenn Sie anstelle von einen anderen API-Ressourcennamen verwendet haben`search`.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Such-API bereit.	Führen Sie den AWS CLI-Befehl create-deployment aus, um eine Stufenressource mit dem Namen zu erstellen`dev`:
	`aws apigateway create-deployment \`
	`  --rest-api-id <API-ID> \`
	`  --stage-name dev`
	Wenn Sie die API aktualisieren, können Sie denselben CLI-Befehl verwenden, um sie auf derselben Stufe erneut bereitzustellen.
		Cloud-Architekt, Cloud-Administrator

Erstellen und Konfigurieren von Kibana-Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der Kibana-Konsole an.	1. Suchen Sie den Link zu Kibana in Ihrem Domain-Dashboard in der Amazon-OpenSearch Service-Konsole. Die URL hat die folgende Form: `<domain-endpoint>/_plugin/kibana/` . 2. Verwenden Sie den Bastion-Host, den Sie im ersten Epic konfiguriert haben, um auf die Kibana-Konsole zuzugreifen.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Melden Sie sich bei der Kibana-Konsole an, indem Sie den Master-Benutzernamen und das Passwort aus dem vorherigen Schritt verwenden, als Sie die Amazon- OpenSearch Service-Domain erstellt haben. 4. Wenn Sie aufgefordert werden, einen Mandanten auszuwählen, wählen Sie Privat aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie Kibana-Rollen.	Um eine Datenisolierung bereitzustellen und sicherzustellen, dass ein Mandant die Daten eines anderen Mandanten nicht abrufen kann, müssen Sie die Dokumentensicherheit verwenden, die es Mandanten ermöglicht, nur auf Dokumente zuzugreifen, die ihre Mandanten-ID enthalten. 1. Wählen Sie in der Kibana-Konsole im Navigationsbereich Sicherheit, Rolle aus. 2. Erstellen Sie eine neue Tenant-Rolle. 3. Legen Sie Cluster-Berechtigungen auf fest`indices_all` , wodurch CRUD-Berechtigungen (Erstellen, Lesen, Aktualisieren und Löschen) für den Amazon-OpenSearch Service-Index erteilt werden. 4. Beschränken Sie Indexberechtigungen auf den `tenant-data` Index. (Der Indexname sollte mit dem Namen in den Lambda-Such- und Indexfunktionen übereinstimmen.)	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Legen Sie Indexbere chtigungen auf festindices_all , damit Benutzer alle indexbezo genen Operationen ausführen können. (Je nach Ihren Anforderungen können Sie Operationen für einen detaillierteren Zugriff einschränken.) 6. Verwenden Sie für die Sicherheit auf Dokumente bene die folgende Richtlini e, um Dokumente nach Mandanten-ID zu filtern und die Datenisolierung für Mandanten in einem freigegebenen Index bereitzustellen: `{ "bool": { "must": { "match": { "TenantId": "Tenant-1" } } } }` Bei Indexnamen, Eigenscha ften und Werten wird zwischen Groß- und Kleinschreibung unterschi eden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie Benutzer Rollen zu.	1. Wählen Sie die Registerkarte Zugeordnete Benutzer für die Rolle und dann Benutzer zuordnen aus. 2. Geben Sie im Abschnitt Backend-Rollen den ARN der IAM-Mandantenrolle an, die Sie zuvor erstellt haben, und wählen Sie dann Zuordnen aus. Dadurch wird die IAM-Tenant-Rolle der Kibana-Rolle zugeordnet, sodass die Tenant-spezifische Suche nur Daten für diesen Mandanten zurückgibt. Wenn der IAM-Rollenname für Tenant-1 beispielsweise lautet`Tenant-1-Role` , geben Sie den ARN für `Tenant-1-Role` (aus der Tabelle Tenant-Rollen erstellen und konfigurieren) im Feld Backend-Rollen für die Tenant-1-Kibana-Rolle an. 3. Wiederholen Sie die Schritte 1 und 2 für Tenant-2. Wir empfehlen Ihnen, die Erstellung der Mandanten - und Kibana-Rollen zum Zeitpunkt des Mandanten-	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Onboardings zu automatisieren.	
Erstellen Sie den Tenant-Datenindex.	Wählen Sie im Navigationsbereich unter Management die Option Entwicklungstools aus und führen Sie dann den folgenden Befehl aus. Mit diesem Befehl wird der `tenant-data` Index erstellt, um die Zuordnung für die -`TenantId`Eigenschaft zu definieren. `PUT /tenant-data { "mappings": { "properties": { "TenantId": { "type": "keyword"} } } }`	Cloud-Architekt, Cloud-Administrator

Erstellen von VPC-Endpunkten für Amazon S3 und AWS STS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt für Amazon S3.	Führen Sie den AWS CLI-create-vpc-endpointBefehl aus, um einen VPC-Endpunkt für Amazon S3 zu erstellen . Der Endpunkt ermöglicht der Lambda-Indexfunktion in der VPC den Zugriff auf den Amazon S3-Service.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws ec2 create-vpc-endpoint \ --vpc-id <VPC-ID> \ --service-name com.amazonaws.us-east-1.s3 \ --route-table-ids <route-table-ID>` Geben Sie für die VPC an`vpc-id`, die Sie für die Lambda-Indexfunktion verwenden. `service-name` Verwenden Sie für die richtige URL für den Amazon S3-Endpunkt. Geben Sie für die Routing-Tabelle an`route-table-ids` , die dem VPC-Endpunkt zugeordnet ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen VPC-Endpunkt für AWS STS.	Führen Sie den AWS CLI-create-vpc-endpoint Befehl aus, um einen VPC-Endpunkt für AWS Security Token Service (AWS STS) zu erstellen. Der Endpunkt ermöglicht dem Lambda-Index und den Suchfunktionen in der VPC den Zugriff auf den AWS STS-Service. Die Funktionen verwenden AWS STS, wenn sie die IAM-Rolle übernehmen.
	
	`aws ec2 create-vpc-endpoint \`
	`  --vpc-id <VPC-ID> \`
	`  --vpc-endpoint-type Interface \`
	`  --service-name com.amazonaws.us-east-1.sts \`
	`  --subnet-id <subnet-ID> \`
	`  --security-group-id <security-group-ID>`
	
	Geben Sie für die VPC an `vpc-id`, die Sie für den Lambda-Index und die Suchfunktionen verwenden. Geben Sie für das Subnetz an `subnet-id`, in dem dieser Endpunkt erstellt werden soll. Geben Sie für die Sicherheitsgruppe an `security-`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`group-id` , der dieser Endpunkt zugeordnet werden soll. (Es könnte mit der Sicherheitsgruppe übereinst immen, die Lambda verwendet .)	

Testen von Mehrmandantenfähigkeit und Datenisolierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Python-Dateien für den Index und die Suchfunktionen.	1. Bearbeiten Sie in der `index_lambda_packa ge.zip` Datei die `lamba_index.py` Datei , um die AWS-Konto-ID, die AWS-Region und die Elasticsearch-Endpunktinfor mationen zu aktualisieren. 2. Bearbeiten Sie in der `search_lambda_pack age.zip` Datei die `lambda_search.py` Datei , um die AWS-Konto-ID, die AWS-Region und die Elasticsearch-Endpunktinfor mationen zu aktualisieren. Sie können den Elasticsearch-Endpunkt auf der Registerk arte Übersicht der Amazon-OpenSearch Service-Konsole abrufen. Sie hat das Format	Cloud-Architekt, App-Entwi ckler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<AWS-Region>.es.amazonaws.com` .	

Aktualisieren Sie den Lambda-Code.	Verwenden Sie den AWS CLI-update-function-codeBefehl , um den Lambda-Code mit den Änderungen zu aktualisieren, die Sie an den Python-Dateien vorgenommen haben:
	
	`aws lambda update-function-code \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip`
	
	`aws lambda update-function-code \`
	`  --function-name search-lambda-function \`
	`  --zip-file fileb://search_lambda_package.zip`
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie Rohdaten in den S3-Bucket hoch.	Verwenden Sie den AWS CLI cp-Befehl, um Daten für die Objekte Tenant-1 und Tenant-2 in den `tenantrawdata` Bucket hochzuladen (geben Sie den Namen des S3-Buckets an, den Sie für diesen Zweck erstellt haben):
	`aws s3 cp tenant-1-data s3://tenantrawdata`
	`aws s3 cp tenant-2-data s3://tenantrawdata`
	Der S3-Bucket ist so eingerichtet, dass die Lambda-Indexfunktion bei jedem Hochladen von Daten ausgeführt wird, sodass das Dokument in Elasticsearch indiziert wird.
		Cloud-Architekt, Cloud-Administrator

Suchen Sie Daten von der Kibana-Konsole aus.	Führen Sie in der Kibana-Konsole die folgende Abfrage aus: `GET tenant-data/_search` Diese Abfrage zeigt alle Dokumente an, die in Elasticsearch indiziert sind. In diesem Fall sollten Sie zwei separate Dokumente für Tenant-1 und Tenant-2 sehen.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Such-API von API Gateway aus.	1. Öffnen Sie in der API Gateway-Konsole die Such-API, wählen Sie die `GET` Methode innerhalb der Suchressource und dann Testen aus.
	2. Geben Sie im Testfenster die folgende Abfrageze ichenfolge (wobei die Groß- und Kleinschreibung beachtet wird) für die Mandanten-ID an und wählen Sie dann Testen aus.
	`TenantId=Tenant-1`
	Die Lambda-Funktion sendet eine Abfrage an Amazon OpenSearch Service, die das Tenant-Dokument basierend auf der Sicherheit auf Dokumente bene filtert. Die Methode gibt das Dokument zurück, das zu Tenant-1 gehört.
	3. Ändern Sie die Abfrageze ichenfolge wie folgt:
	`TenantId=Tenant-2`
	Diese Abfrage gibt das Dokument zurück, das zu Tenant-2 gehört.
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bildschirmbilder finden Sie im Abschnitt Zusätzliche Informationen.	

Zugehörige Ressourcen

- AWS SDK für Python (Boto3)
- AWS Lambda-Dokumentation
- Dokumentation zu Amazon API Gateway
- Amazon S3-Dokumentation
- Amazon OpenSearch -Service-Dokumentation
  - Differenzierte Zugriffskontrolle in Amazon OpenSearch Service
  - Erstellen einer Suchanwendung mit Amazon OpenSearch Service
  - Starten Ihrer Amazon- OpenSearch Service-Domains innerhalb einer VPC

Zusätzliche Informationen

Datenpartitionierungsmodelle

Es gibt drei gängige Datenpartitionierungsmodelle, die in Systemen mit mehreren Mandanten verwendet werden: Silo, Pool und Hybrid. Welches Modell Sie wählen, hängt von der Compliance, dem lauten Nachbarn, dem Betrieb und den Isolationsanforderungen Ihrer Umgebung ab.

Silomodell

Im Silomodell werden die Daten jedes Mandanten in einem separaten Speicherbereich gespeichert, in dem keine Mischung von Mandantendaten stattfindet. Sie können zwei Ansätze verwenden, um das Silomodell mit Amazon OpenSearch Service zu implementieren: Domain pro Mandant und Index pro Mandant.

- Domain pro Mandanten – Sie können eine separate Amazon- OpenSearch Service-Domain (synonym mit einem Elasticsearch-Cluster) pro Mandanten verwenden. Die Platzierung jedes Mandanten in einer eigenen Domain bietet alle Vorteile, die mit der Bereitstellung von Daten in einem eigenständigen Konstrukt verbunden sind. Dieser Ansatz führt jedoch zu Herausforderungen

in Bezug auf Management und Agilität. Aufgrund seiner verteilten Natur ist es schwieriger, den Betriebszustand und die Aktivität von Mandanten zu aggregieren und zu bewerten. Dies ist eine kostspielige Option, bei der jede Amazon- OpenSearch Service-Domäne mindestens drei Hauptknoten und zwei Datenknoten für Produktions-Workloads haben muss.

- Index pro Mandant – Sie können Mandantendaten in separaten Indizes innerhalb eines Amazon-OpenSearch Service-Clusters platzieren. Bei diesem Ansatz verwenden Sie beim Erstellen und Benennen des Index eine Mandanten-ID, indem Sie die Mandanten-ID dem Indexnamen voranstellen. Der Ansatz Index pro Mandanten hilft Ihnen dabei, Ihre Siloziele zu erreichen, ohne einen vollständig separaten Cluster für jeden Mandanten einzuführen. Es kann jedoch zu Speicherdruck kommen, wenn die Anzahl der Indizes zunimmt, da dieser Ansatz mehr Shards erfordert und der Hauptknoten mehr Zuweisung und Neuausgleich bewältigen muss.

Isolierung im Silomodell – Im Silomodell verwenden Sie IAM-Richtlinien, um die Domains oder Indizes zu isolieren, die die Daten jedes Mandanten enthalten. Diese Richtlinien verhindern, dass ein Mandant auf die Daten eines anderen Mandanten zugreift. Um Ihr Silo-Isolationsmodell zu implementieren, können Sie eine ressourcenbasierte Richtlinie erstellen, die den Zugriff auf Ihre Mandantenressource steuert. Dies ist oft eine Domain-Zugriffsrichtlinie, die angibt, welche Aktionen ein Prinzipal für die Unterressourcen der Domain ausführen kann, einschließlich Elasticsearch-Indizes und APIs. Mit identitätsbasierten IAM-Richtlinien können Sie zulässige oder verweigerte Aktionen für die Domain, Indizes oder APIs in Amazon OpenSearch Service angeben. Das `-Action` Element einer IAM-Richtlinie beschreibt die spezifischen Aktionen, die von der Richtlinie zugelassen oder verweigert werden, und das `-Principal` Element gibt die betroffenen Konten, Benutzer oder Rollen an.

Die folgende Beispielrichtlinie gewährt Tenant-1 nur Vollzugriff (wie durch angegeben`es:*`) auf die Unterressourcen in der Domain`tenant-1`. Das nachgestellte `/*` im `-Resource` Element gibt an, dass diese Richtlinie für die Unterressourcen der Domäne gilt, nicht für die Domäne selbst. Wenn diese Richtlinie in Kraft ist, dürfen Mandanten keine neue Domain erstellen oder Einstellungen für eine vorhandene Domain ändern.

```
{
   "Version": "2012-10-17",
   "Statement": [
```

```
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::aws-account-id:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:Region:account-id:domain/tenant-1/*"
      }
   ]
}
```

Um den Mandanten pro Index-Silomodell zu implementieren, müssen Sie diese Beispielrichtlinie ändern, um Tenant-1 weiter auf den angegebenen Index oder die Indizes zu beschränken, indem Sie den Indexnamen angeben. Die folgende Beispielrichtlinie beschränkt Tenant-1 auf den `tenant-index-1` Index.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:Region:account-id:domain/test-domain/tenant-index-1/*"
      }
   ]
}
```

Poolmodell

Im Poolmodell werden alle Mandantendaten in einem Index innerhalb derselben Domain gespeichert. Die Mandanten-ID ist in den Daten (Dokument) enthalten und wird als Partitionsschlüssel verwendet, sodass Sie ermitteln können, welche Daten zu welchem Mandanten gehören. Dieses Modell reduziert den Verwaltungsaufwand. Der Betrieb und die Verwaltung des gebündelten Index ist einfacher und effizienter als die Verwaltung mehrerer Indizes. Da Mandantendaten jedoch innerhalb desselben Index zusammengeführt werden, verlieren Sie die natürliche Mandantenisolierung, die das Silomodell bietet. Dieser Ansatz kann auch die Leistung beeinträchtigen, da es zu einem verrauschten Nachbarn kommt.

Mandantenisolierung im Poolmodell – Im Allgemeinen ist die Mandantenisolierung im Poolmodell schwierig zu implementieren. Der IAM-Mechanismus, der mit dem Silomodell verwendet wird, erlaubt es Ihnen nicht, die Isolation basierend auf der in Ihrem Dokument gespeicherten Mandanten-ID zu beschreiben.

Ein alternativer Ansatz besteht darin, die FGAC-Unterstützung (Fine-Grained Access Control) zu verwenden, die von Open Distro for Elasticsearch bereitgestellt wird. Mit FGAC können Sie Berechtigungen auf Index-, Dokument- oder Feldebene steuern. Bei jeder Anfrage wertet FGAC die Benutzeranmeldeinformationen aus und authentifiziert entweder den Benutzer oder verweigert den Zugriff. Wenn FGAC den Benutzer authentifiziert, ruft es alle diesem Benutzer zugeordneten Rollen ab und verwendet den vollständigen Satz von Berechtigungen, um zu bestimmen, wie die Anforderung verarbeitet werden soll.

Um die erforderliche Isolation im gebündelten Modell zu erreichen, können Sie die Sicherheit auf Dokumentebene verwenden, mit der Sie eine Rolle auf eine Teilmenge von Dokumenten in einem Index beschränken können. Die folgende Beispielrolle schränkt Abfragen an Tenant-1 ein. Indem Sie diese Rolle auf Tenant-1 anwenden, können Sie die erforderliche Isolation erreichen.

```
{
   "bool": {
     "must": {
       "match": {
         "tenantId": "Tenant-1"
       }
     }
   }
 }
```

Hybrid-Modell

Das Hybridmodell verwendet eine Kombination aus Silo- und Poolmodellen in derselben Umgebung, um jedem Mandantenkontingent (z. B. kostenlose, Standard- und Premium-Kontingente) einzigartige Erlebnisse zu bieten. Jede Stufe folgt demselben Sicherheitsprofil, das im Poolmodell verwendet wurde.

Mandantenisolierung im Hybridmodell – Im Hybridmodell folgen Sie demselben Sicherheitsprofil wie im Poolmodell, bei dem die Verwendung des FGAC-Sicherheitsmodells auf Dokumentebene

die Mandantenisolierung bereitstellt. Obwohl diese Strategie die Clusterverwaltung vereinfacht und Agilität bietet, erschwert sie andere Aspekte der Architektur. Ihr Code erfordert beispielsweise zusätzliche Komplexität, um zu bestimmen, welches Modell jedem Mandanten zugeordnet ist. Sie müssen auch sicherstellen, dass Single-Tenant-Abfragen nicht die gesamte Domain sättigen und die Erfahrung anderer Mandanten beeinträchtigen.

Testen in API Gateway

Testfenster für Tenant-1-Abfragen

Testfenster für die Tenant-2-Abfrage

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Bereitstellen von Multi-Stack-Anwendungen mit AWS CDK mit TypeScript

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

Umgebung: Produktion	Technologien: Modernisierung; Migration; DevOps	Workload: Alle anderen Workloads
AWS-Services: Amazon API Gateway ;AWS Lambda ;Amazon Kinesis		

Übersicht

Dieses Muster bietet einen step-by-step Ansatz für die Anwendungsbereitstellung auf Amazon Web Services (AWS) mit AWS Cloud Development Kit (AWS CDK) mit TypeScript. Beispielsweise stellt das Muster eine serverlose Echtzeitanalyseanwendung bereit.

Das Muster erstellt und stellt verschachtelte Stack-Anwendungen bereit. Der übergeordnete AWS- CloudFormation Stack ruft die untergeordneten oder verschachtelten Stacks auf. Jeder untergeordnete Stack erstellt und stellt die AWS-Ressourcen bereit, die im CloudFormation Stack definiert sind. AWS CDK Toolkit, der Befehl der Befehlszeilenschnittstelle (Command Line Interface`cdk`, CLI), ist die primäre Schnittstelle für die CloudFormation Stacks.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Bestehende Virtual Private Cloud (VPC) und Subnetze
- AWS CDK Toolkit installiert und konfiguriert
- Ein Benutzer mit Administratorberechtigungen und einer Reihe von Zugriffsschlüsseln.
- Node.js
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)

Einschränkungen

- Da AWS CDK AWS verwendet CloudFormation, unterliegen AWS-CDK-Anwendungen CloudFormation Service Quotas. Weitere Informationen finden Sie unter AWS- CloudFormation Kontingente.

Produktversionen

Dieses Muster wurde mit den folgenden Tools und Versionen erstellt und getestet.

- AWS CDK Toolkit 1.83.0
- Node.js 14.13.0
- npm 7.0.14

Das Muster sollte mit jeder Version von AWS CDK oder npm funktionieren. Beachten Sie, dass die Node.js-Versionen 13.0.0 bis 13.6.0 nicht mit dem AWS-CDK kompatibel sind.

Architektur

Zieltechnologie-Stack

- AWS Amplify-Konsole
- Amazon API Gateway
- AWS-CDK
- Amazon CloudFront
- Amazon Cognito
- Amazon DynamoDB
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)

Zielarchitektur

Das folgende Diagramm zeigt die Bereitstellung von Multi-Stack-Anwendungen mit AWS CDK mit TypeScript.

Das folgende Diagramm zeigt die Architektur der Beispielanwendung Serverless in Echtzeit.

Tools

Tools

- AWS Amplify Console ist das Kontrollzentrum für die Bereitstellung von Fullstack-Web- und mobilen Anwendungen in AWS. Das Hosting der Amplify-Konsole bietet einen git-basierten Workflow zum Hosten von Serverless-Fullstack-Webanwendungen mit kontinuierlicher Bereitstellung. Die Admin-Benutzeroberfläche ist eine visuelle Oberfläche für Frontend-Web- und Mobilentwickler zum Erstellen und Verwalten von App-Backends außerhalb der AWS-Konsole.
- Amazon API Gateway ist ein AWS-Service zum Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST-, HTTP- und - WebSocket APIs in jeder Größenordnung.
- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, das Sie bei der Interaktion mit Ihrer AWS CDK-App unterstützt. Der `cdk` CLI-Befehl ist das primäre Tool für die Interaktion mit Ihrer AWS-CDK-App. Es führt Ihre App aus, fragt das von Ihnen definierte Anwendungsmodell ab und erstellt und stellt die vom AWS-CDK generierten AWS- CloudFormation Vorlagen bereit.
- Amazon CloudFront ist ein Webservice, der die Verteilung statischer und dynamischer Webinhalte wie HTML-, CSS-, .js- und Image-Dateien beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden, um eine geringere Latenz und verbesserte Leistung zu erzielen.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und mobilen Apps. Ihre Benutzer können sich direkt oder über einen Drittanbieter anmelden.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Echtzeit-Streaming-Daten an Ziele wie Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk und alle benutzerdefinierten HTTP-Endpunkte oder HTTP-Endpunkte, die unterstützten Drittanbietern gehören.
- Amazon Kinesis Data Streams ist ein Service zum Erfassen und Verarbeiten großer Datensätze in Echtzeit.

- AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Code für dieses Muster ist angehängt.

Sekunden

AWS CDK Toolkit installieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS CDK Toolkit.	Führen Sie den folgenden Befehl aus, um AWS CDK Toolkit global zu installieren. `npm install -g aws-cdk`	DevOps
Überprüfen Sie die Version.	Führen Sie den folgenden Befehl aus, um die AWS CDK Toolkit-Version zu überprüfen. `cdk --version`	DevOps

Einrichten von AWS-Anmeldeinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Anmeldein formationen ein.	Um Anmeldeinformationen einzurichten, führen Sie den `aws configure` Befehl aus	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	und folgen Sie den Anweisungen.
	
	`$aws configure`
	`AWS Access Key ID [None]:`
	`AWS Secret Access Key [None]: your_secret_access_key`
	`Default region name [None]:`
	`Default output format [None]:`	

Projektcode herunterladen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den angehängten Projektcode herunter.	Weitere Informationen zum Verzeichnis und zur Dateistruktur finden Sie im Abschnitt Zusätzliche Informationen.	DevOps

Bootstrapping der AWS-CDK-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrappen Sie die Umgebung.	Führen Sie den folgenden Befehl aus, um die AWS-CloudFormation Vorlage für das Konto und die AWS-Region bereitzustellen, die Sie verwenden möchten.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk bootstrap <account>/<Region>` Weitere Informationen finden Sie in der AWS-Dokumentation.	

Erstellen und Bereitstellen des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Projekt.	Führen Sie den `npm run build` Befehl aus, um den Projektcode zu erstellen.	DevOps
Stellen Sie das Projekt bereit.	Um den Projektcode bereitzustellen, führen Sie den `cdk deploy` Befehl aus.	

Überprüfen von Ausgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Stack-Erstellung.	Wählen Sie in der AWS-Managementkonsole CloudFormation. Überprüfen Sie in den Stacks für das Projekt, ob ein übergeordneter Stack und zwei untergeordnete Stacks erstellt wurden.	DevOps

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Daten an Kinesis Data Streams.	Konfigurieren Sie Ihr AWS-Konto so, dass Daten mit Amazon Kinesis Data Generator (KDG) an Kinesis Data Streams gesendet werden. Weitere Informati onen finden Sie unter Amazon Kinesis Data Generator.	DevOps
Erstellen Sie einen Amazon Cognito-Benutzer.	Um einen Amazon Cognito-B enutzer zu erstellen, laden Sie die CloudFormation Vorlage cognito-setup.json aus dem Abschnitt Erstellen eines Amazon Cognito-Benutzers auf der Hilfeseite des Kinesis Data Generators herunter. Initiieren Sie die Vorlage und geben Sie dann Ihren Amazon Cognito-Benutzernamen und Ihr Passwort ein. Auf der Registerkarte Outputs wird die URL des Kinesis Data Generators aufgeführt.	DevOps
Melden Sie sich bei Kinesis Data Generator an	Verwenden Sie die von Ihnen angegebenen Amazon Cognito-Anmeldeinformatione n und die URL des Kinesis Data Generators, um sich bei KDG anzumelden.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendung.	Fügen Sie in KDG in Datensatzvorlage, Vorlage 1 den Testcode aus dem Abschnitt Zusätzliche Informationen ein und wählen Sie Daten senden aus.	DevOps
API Gateway testen.	Nachdem die Daten aufgenommen wurden, testen Sie API Gateway mithilfe der `GET` Methode , um Daten abzurufen.	DevOps

Zugehörige Ressourcen

Referenzen

- AWS Cloud Development Kit
- AWS-CDK auf GitHub
- Arbeiten mit verschachtelten Stacks
- AWS-Beispiel – Serverless-Echtzeitanalysen

Zusätzliche Informationen

Verzeichnis- und Dateidetails

Dieses Muster richtet die folgenden drei Stacks ein.

- `parent-cdk-stack.ts` – Dieser Stack fungiert als übergeordneter Stack und ruft die beiden untergeordneten Anwendungen als verschachtelte Stacks auf.
- `real-time-analytics-poc-stack.ts` – Dieser verschachtelte Stack enthält die Infrastruktur und den Anwendungscode.
- `real-time-analytics-web-stack.ts` – Dieser verschachtelte Stack enthält nur den statischen Webanwendungscode.

Wichtige Dateien und ihre Funktionalität

- `bin/real-time-analytics-poc.ts` – Eintrittspunkt der AWS-CDK-Anwendung. Es lädt alle Stacks, die unter definiert sind`lib/`.
- `lib/real-time-analytics-poc-stack.ts` – Definition des Stacks der AWS-CDK-Anwendung (`real-time-analytics-poc`).
- `lib/real-time-analytics-web-stack.ts` – Definition des Stacks der AWS-CDK-Anwendung (`real-time-analytics-web-stack`).
- `lib/parent-cdk-stack.ts` – Definition des Stacks der AWS-CDK-Anwendung (`parent-cdk`).
- `package.json` – npm-Modulmanifest, das den Anwendungsnamen, die Version und Abhängigkeiten enthält.
- `package-lock.json` – Wird von npm verwaltet.
- `cdk.json` – Toolkit zum Ausführen der Anwendung.
- `tsconfig.json` – Die TypeScript Konfiguration des Projekts.
- `.gitignore` – Liste der Dateien, die Git von der Quellkontrolle ausschließen soll.
- `node_modules` – Wird von npm gepflegt und enthält die Abhängigkeiten des Projekts.

Der folgende Abschnitt des Codes im übergeordneten Stack ruft untergeordnete Anwendungen als verschachtelte AWS-CDK-Stacks auf.

```
import * as cdk from '@aws-cdk/core';
import { Construct, Stack, StackProps } from '@aws-cdk/core';
import { RealTimeAnalyticsPocStack } from './real-time-analytics-poc-stack';
import { RealTimeAnalyticsWebStack } from './real-time-analytics-web-stack';


export class CdkParentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);


    new RealTimeAnalyticsPocStack(this, 'RealTimeAnalyticsPocStack');
    new RealTimeAnalyticsWebStack(this, 'RealTimeAnalyticsWebStack');
  }
}
```

Code zum Testen

```
session={{date.now('YYYYMMDD')}}|sequence={{date.now('x')}}|
reception={{date.now('x')}}|instrument={{random.number(9)}}|
l={{random.number(20)}}|price_0={{random.number({"min":10000,
 "max":30000})}}|price_1={{random.number({"min":10000, "max":30000})}}|
price_2={{random.number({"min":10000, "max":30000})}}|
price_3={{random.number({"min":10000, "max":30000})}}|
price_4={{random.number({"min":10000, "max":30000})}}|
price_5={{random.number({"min":10000, "max":30000})}}|
price_6={{random.number({"min":10000, "max":30000})}}|
price_7={{random.number({"min":10000, "max":30000})}}|
price_8={{random.number({"min":10000, "max":30000})}}|
```

Testen von API Gateway

Testen Sie API Gateway in der API Gateway-Konsole mithilfe der -`GET`Methode.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren der Bereitstellung verschachtelter Anwendungen mit AWS SAM

Erstellt von Dr. Rahul Sharad Gaikwad (AWS), Dmitry G (AWS), Ishwar Chaiwale (AWS) und Tabby Ward (AWS)

Code-Repository: aws-sam-nested-stack-sample	Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; Serverless; DevOps
Workload: Alle anderen Workloads	AWS-Services: AWS Serverless Application Repository	

Übersicht

Auf Amazon Web Services (AWS) ist AWS Serverless Application Model (AWS SAM) ein Open-Source-Framework, das Kurzsyntax zum Formulieren von Funktionen, APIs, Datenbanken und Ereignisquellenzuordnungen bereitstellt. Mit nur wenigen Zeilen für jede Ressource können Sie die gewünschte Anwendung definieren und sie mithilfe von YAML modellieren. Während der Bereitstellung transformiert und erweitert SAM die SAM-Syntax in die AWS- CloudFormation Syntax, mit der Sie Serverless-Anwendungen schneller erstellen können.

AWS SAM vereinfacht die Entwicklung, Bereitstellung und Verwaltung von Serverless-Anwendungen auf der AWS-Plattform. Es bietet ein standardisiertes Framework, schnellere Bereitstellung, lokale Testfunktionen, Ressourcenmanagement, nahtlose Integration in Entwicklungstools und eine erfreutde Community. Diese Funktionen machen es zu einem wertvollem Tool für die effiziente und effektive Erstellung von Serverless-Anwendungen.

Dieses Muster verwendet AWS SAM-Vorlagen, um die Bereitstellung verschachtelter Anwendungen zu automatisieren. Eine verschachtelte Anwendung ist eine Anwendung innerhalb einer anderen Anwendung. Übergeordnete Anwendungen rufen ihre untergeordneten Anwendungen auf. Dies sind lose gekoppelte Komponenten einer Serverless-Architektur.

Mithilfe verschachtelter Anwendungen können Sie schnell hochentwickelte Serverless-Architekturen erstellen, indem Sie Services oder Komponenten wiederverwenden, die unabhängig voneinander erstellt und verwaltet werden, aber mit AWS SAM und dem Serverless Application

Repository bestehen. Verschachtelte Anwendungen helfen Ihnen, Anwendungen zu erstellen, die leistungsfähiger sind, doppelte Arbeit zu vermeiden und Konsistenz und bewährte Methoden in Ihren Teams und Organisationen sicherzustellen. Um verschachtelte Anwendungen zu demonstrieren, stellt das Muster ein Beispiel für eine serverlose AWS-Warenkorbanwendung bereit.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine vorhandene Virtual Private Cloud (VPC) und Subnetze
- Eine integrierte Entwicklungsumgebung wie AWS Cloud9 oder Visual Studio Code (weitere Informationen finden Sie unter Tools zum Erstellen auf AWS)
- Python-Wheel-Bibliothek mit Pip-Installationsrad installiert, sofern sie noch nicht installiert ist

Einschränkungen

- Die maximale Anzahl von Anwendungen, die in einer Serverless-Anwendung verschachtelt werden können, beträgt 200.
- Die maximale Anzahl von Parametern für eine verschachtelte Anwendung kann 60 haben.

Produktversionen

- Diese Lösung basiert auf AWS SAM Command Line Interface (AWS SAM CLI) Version 1.21.1, aber diese Architektur sollte mit späteren AWS SAM CLI-Versionen funktionieren.

Architektur

Zieltechnologie-Stack

- Amazon API Gateway
- AWS SAM
- Amazon Cognito
- Amazon DynamoDB
- AWS Lambda
- Amazon Simple Queue Service-Warteschlange (Amazon SQS)

Zielarchitektur

Das folgende Diagramm zeigt, wie Benutzeranfragen an die Einkaufsservices gestellt werden, indem APIs aufgerufen werden. Die Anforderung des Benutzers, einschließlich aller erforderlichen Informationen, wird an Amazon API Gateway und den Amazon Cognito-Genehmiger gesendet, der Authentifizierungs- und Autorisierungsmechanismen für die APIs durchführt.

Wenn ein Element in DynamoDB hinzugefügt, gelöscht oder aktualisiert wird, wird ein Ereignis in DynamoDB Streams abgelegt, was wiederum eine Lambda-Funktion initiiert. Um das sofortige Löschen alter Elemente als Teil eines synchronen Workflows zu vermeiden, werden Nachrichten in eine SQS-Warteschlange gestellt, wodurch eine Worker-Funktion zum Löschen der Nachrichten initiiert wird.

Bei dieser Lösungseinrichtung dient AWS SAM CLI als Schnittstelle für AWS- CloudFormation Stacks. AWS SAM-Vorlagen stellen verschachtelte Anwendungen automatisch bereit. Die übergeordnete SAM-Vorlage ruft die untergeordneten Vorlagen auf und der übergeordnete CloudFormation Stack stellt die untergeordneten Stacks bereit. Jeder untergeordnete Stack erstellt die AWS-Ressourcen, die in den AWS SAM- CloudFormation Vorlagen definiert sind.

1. Erstellen Sie die Stacks und stellen Sie sie bereit.
2. Der Auth- CloudFormation Stack enthält Amazon Cognito .
3. Der Produkt- CloudFormation Stack enthält eine Lambda-Funktion und Amazon API Gateway
4. Der Warenkorb- CloudFormation Stack enthält eine Lambda-Funktion, Amazon API Gateway, die SQS-Warteschlange und die Amazon-DynamoDB-Datenbank.

Tools

Tools

- Amazon API Gateway unterstützt Sie beim Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST-, HTTP- und - WebSocket APIs in jeder Größenordnung.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.

- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie Serverless-Anwendungen in der AWS Cloud erstellen können.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Code

Der Code für dieses Muster ist im GitHub AWS SAM Nested Stack Sample-Repository verfügbar.

Sekunden

Installieren der AWS SAM-CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SAM CLI.	Informationen zur Installation der AWS SAM CLI finden Sie in den Anweisungen in der AWS SAM-Dokumentation.	DevOps Techniker
Richten Sie AWS-Anmeldeinformationen ein.	Um AWS-Anmeldeinformationen festzulegen, damit die AWS SAM-CLI in Ihrem Namen Aufrufe an AWS-Services tätigen kann, führen Sie den `aws configure` Befehl aus und folgen Sie den Anweisungen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	` [None]: your_secr`
	`et_access_key`
	`Default region name`
	` [None]:`
	`Default output format`
	` [None]:`
	
	Weitere Informationen zum Einrichten Ihrer -Anmeldei nformationen finden Sie unter Authentifizierung und -Anmeldeinformationen.	

Initialisieren des AWS SAM-Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das AWS SAM-Code-Repository.	1. Klonen Sie das verschachtelte Stack-Beispiel-Repository aws sam für dieses Muster, indem Sie den folgenden Befehl eingeben.
	
	`git clone https://g`
	`ithub.com/aws-samp`
	`les/aws-sam-nested-`
	`stack-sample.git`
	
	2. Navigieren Sie in das geklonte Verzeichnis, indem
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den folgenden Befehl eingeben. `cd aws-sam-nested-stack-sample`	
Stellen Sie Vorlagen bereit, um das Projekt zu initialisieren.	Um das Projekt zu initialisieren, führen Sie den `SAM init` Befehl aus. Wenn Sie aufgefordert werden, eine Vorlagenquelle auszuwählen, wählen Sie `Custom Template Location`.	DevOps Techniker

Kompilieren und Erstellen des SAM-Vorlagencodes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS SAM-Anwendungsvorlagen.	Überprüfen Sie die Vorlagen für die verschachtelten Anwendungen. In diesem Beispiel werden die folgenden verschachtelten Anwendungsvorlagen verwendet: • `auth.yaml` – Diese Vorlage richtet Ressourcen im Zusammenhang mit der Authentifizierung ein, z. B. Amazon Cognito und AWS Systems Manager Parameter Store. • `product-mock.yaml` – Diese Vorlage stellt	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	produktbezogene Ressourcen wie Lambda-Funktionen und Amazon API Gateway bereit. • `shoppingcart-service.yaml` – Diese Vorlage richtet Ressourcen im Zusammenhang mit dem Warenkorb ein, z. B. AWS Identity and Access Management (IAM), DynamoDB-Tabellen und Lambda-Funktionen.	
Überprüfen Sie die übergeordnete Vorlage.	Überprüfen Sie die Vorlage, die die verschachtelten Anwendungsvorlagen aufruft. In diesem Beispiel ist die übergeordnete Vorlage `template.yml` . Alle separaten Anwendungen sind in der einzelnen übergeordneten Vorlage verschachtelt`template.yml` .	DevOps Techniker
Kompilieren und erstellen Sie den AWS SAM-Vorlagencode.	Führen Sie mit der AWS SAM CLI den folgenden Befehl aus. `sam build`	DevOps Techniker

Bereitstellen der AWS SAM-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendungen bereit.	Führen Sie den folgenden Befehl aus, um den SAM-Vorlagencode zu starten, der die verschachtelten Anwendungs- CloudFormation Stacks erstellt und Code in der AWS-Umgebung bereitstellt. `sam deploy --guided --stack-name shopping-cart-nested-stack --capabilities CAPABILITY_IAM CAPABILITY_AUTO_EXPAND` Der Befehl fordert Sie mit einigen Fragen auf. Beantworten Sie alle Fragen mit y.	DevOps Techniker

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Stacks.	Gehen Sie wie folgt vor, um die AWS- CloudFormation Stacks und AWS-Ressourcen zu überprüfen, die in den AWS SAM-Vorlagen definiert wurden: 1. Melden Sie sich bei der AWS-Managementkonsole	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an und navigieren Sie zur CloudFormation Konsole. 2. Stellen Sie sicher, dass die übergeordneten und untergeordneten Stacks aufgelistet sind. In diesem Beispiel `sam-shopping-cart` ist der übergeordnete Stack, der die verschachtelten Auth-, Produkt- und Stacks aufruft. Der Produkt-Stack gibt den API Gateway-URL-Link für das Produkt als Ausgabe an.	

Zugehörige Ressourcen

Referenzen

- AWS Serverless Application Model (AWS SAM)
- AWS SAM auf GitHub
- Serverless Cart Microservice (AWS-Beispielanwendung)

Tutorials und Videos

- Erstellen einer Serverless-App
- AWS Online Tech Talks: Serverless Application Building and Deployments with AWS SAM

Zusätzliche Informationen

Nachdem der gesamte Code vorhanden ist, hat das Beispiel die folgende Verzeichnisstruktur:

- sam_stacks – Dieser Ordner enthält die `shared.py` Ebene . Eine Ebene ist ein Dateiarchiv, das Bibliotheken, eine benutzerdefinierte Laufzeit oder andere Abhängigkeiten enthält. Mit Ebenen können Sie Bibliotheken in Ihrer Funktion verwenden, ohne sie in ein Bereitstellungspaket aufnehmen zu müssen.
- product-mock-service – Dieser Ordner enthält alle produktbezogenen Lambda-Funktionen und -Dateien.
- shopping-cart-service – Dieser Ordner enthält alle Lambda-Funktionen und -Dateien im Zusammenhang mit dem Einkaufen.

Implementieren Sie die SaaSSaaSTenant-Isolation für Amazon S3 mithilfe eines AWS Lambda-Token-Verkäufers

Erstellt von Tabby Ward (AWS), Sr Periyathambi (AWS) und Bol Davis (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; SaaS	AWS-Services: AWS Identity and Access Management ;AWS Lambda ;Amazon S3; AWS STS

Übersicht

SaaSSaaSAnwendungen mit mehreren Mandanten müssen Systeme implementieren, um sicherzustellen, dass die Mandantenisolierung aufrechterhalten wird. Wenn Sie Mandantendaten auf derselben Amazon Web Services (AWS)-Ressource speichern – z. B. wenn mehrere Mandanten Daten im selben Amazon Simple Storage Service (Amazon S3)-Bucket speichern – müssen Sie sicherstellen, dass kein mandantenübergreifender Zugriff möglich ist. Token-Verkäufermaschinen (TVMs) sind eine Möglichkeit, die Isolation von Mandantendaten bereitzustellen. Diese Maschinen bieten einen Mechanismus zum Abrufen von Token und abstrahieren gleichzeitig die Komplexität der Generierung dieser Token. Entwickler können ein TVM verwenden, ohne über detaillierte Kenntnisse darüber zu verfügen, wie es Token erzeugt.

Dieses Muster implementiert ein TVM mithilfe von AWS Lambda . Das TVM generiert ein Token, das aus temporären STS-Anmeldeinformationen (Security Token Service) besteht, die den Zugriff auf die Daten eines einzelnen SaaS-Mandanten in einem S3-Bucket einschränken.

TVMs und der Code, der mit diesem Muster bereitgestellt wird, werden in der Regel mit Ansprüchen verwendet, die von JSON Web Tokens (JWTs) abgeleitet werden, um Anfragen für AWS-Ressourcen einer AWS Identity and Access Management (IAM)-Richtlinie im Mandantenbereich zuzuordnen. Sie können den Code in diesem Muster als Grundlage verwenden, um eine SaaS-Anwendung zu implementieren, die bereichsbezogene, temporäre STS-Anmeldeinformationen basierend auf den in einem JWT-Token angegebenen Ansprüchen generiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI) Version 1.19.0 oder höher, installiert und konfiguriert unter macOS , Linux oder Windows. Alternativ können Sie AWS CLI Version 2.1 oder höher verwenden.

Einschränkungen

- Dieser Code wird in Java ausgeführt und unterstützt derzeit keine anderen Programmiersprachen.
- Die Beispielanwendung beinhaltet keine regionsübergreifende AWS- oder Notfallwiederherstellungs-(DR)-Unterstützung.
- Dieses Muster zeigt, wie ein Lambda TVM für eine SaaS-Anwendung einen eingeschränkten Mandantenzugriff ermöglichen kann. Es ist nicht für die Verwendung in Produktionsumgebungen vorgesehen.

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon S3
- IAM
- AWS Security Token Service (AWS STS)

Zielarchitektur

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Security Token Service (AWS STS) hilft Ihnen, temporäre Anmeldeinformationen mit eingeschränkten Berechtigungen für Benutzer anzufordern.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Quellcode für dieses Muster ist als Anhang verfügbar und enthält die folgenden Dateien:

- `s3UploadSample.jar` stellt den Quellcode für eine Lambda-Funktion bereit, die ein JSON-Dokument in einen S3-Bucket hochlädt.
- `tvm-layer.zip` stellt eine wiederverwendbare Java-Bibliothek bereit, die ein Token (Temporäre STS-Anmeldeinformationen) für die Lambda-Funktion bereitstellt, um auf den S3-Bucket zuzugreifen und das JSON-Dokument hochzuladen.
- `token-vending-machine-sample-app.zip` stellt den Quellcode bereit, der zum Erstellen dieser Artefakte und Kompilierungsanweisungen verwendet wird.

Um diese Dateien zu verwenden, folgen Sie den Anweisungen im nächsten Abschnitt.

Polen

Bestimmen von Variablenwerten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie Variablen werte.	Die Implementierung dieses Musters umfasst mehrere Variablennamen, die konsisten t verwendet werden müssen. Bestimmen Sie die Werte, die für jede Variable verwendet werden sollen, und geben Sie diesen Wert an, wenn Sie in	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nachfolgenden Schritten dazu aufgefordert werden. <AWS-Konto-ID> Die 12-stellige Konto-ID, die dem AWS-Konto zugeordnet ist, in dem Sie dieses Muster implementieren. Informationen zum Auffinden Ihrer AWS cccount-ID finden Sie unter Ihre AWS-Konto-ID und der zugehörige Alias in der IAM-Dokumentation. <AWS Region> Die AWS-Region, in der Sie dieses Muster implementieren. Weitere Informationen zu AWS-Regionen finden Sie unter Regionen und Availability Zones auf der AWS-Website. <sample-tenant-name> Der Name eines Mandanten, der in der Anwendung verwendet werden soll. Wir empfehlen, der Einfachheit halber nur alphanumerische Zeichen in diesem Wert zu verwenden, aber Sie können einen beliebigen gültigen Namen für einen S3-Objektschlüssel verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<sample-tvm-role-name> Der Name der IAM-Rolle , die der Lambda-Funktion zugeordnet ist, die die TVM und die Beispielanwendung ausführt. Der Rollennam e ist eine Zeichenfolge, die aus alphanumerischen Groß- und Kleinbuchstaben ohne Leerzeichen besteht. Sie können auch eines der folgenden Zeichen einfügen: Unterstrich (_), Pluszeich en (+), Gleichheitszeichen (=), Komma (,), Punkt (.), At- Zeichen (@) und Bindestri ch (-). Der Rollenname muss innerhalb des Kontos eindeutig sein. <sample-app-role-name> Der Name der IAM-Rolle, die von der Lambda-Funktion angenommen wird, wenn sie bereichsbezogene, temporäre STS-Anmeldeinformationen generiert. Der Rollennam e ist eine Zeichenfolge, die aus alphanumerischen Groß- und Kleinbuchstaben ohne Leerzeichen besteht. Sie können auch eines der folgenden Zeichen einfügen: Unterstrich (_), Pluszeich en (+), Gleichheitszeichen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(=), Komma (,), Punkt (.), At-Zeichen (@) und Bindestrich (-). Der Rollenname muss innerhalb des Kontos eindeutig sein. <sample-app-function-name> Der Name der Lambda-Funktion. Dies ist eine Zeichenfolge mit einer Länge von bis zu 64 Zeichen. <sample-app-bucket-name> Der Name eines S3-Buckets, auf den zugegriffen werden muss, mit Berechtigungen, die auf einen bestimmten Mandanten beschränkt sind. S3-Bucket-Namen: • Muss zwischen 3 und 63 Zeichen lang sein. • Darf nur aus Kleinbuchstaben, Zahlen, Punkten (.) und Bindestrichen (-) bestehen. • Muss mit einem Buchstaben oder einer Zahl beginnen und enden. • Darf nicht als IP-Adresse (z. B. 192.168.5.4) formatiert sein. • Muss innerhalb einer Partition eindeutig sein. Eine Partition ist eine Gruppe	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von Regionen. AWS verfügt derzeit über drei Partitionen: `aws` (Standardregionen), `aws-cn` (China-Regionen) und `aws-us-gov` (AWS GovCloud [USA]-Regionen).	

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für die Beispielanwendung.	Verwenden Sie den folgenden AWS CLI-Befehl, um einen S3-Bucket zu erstellen. Geben Sie den Wert <sample-app-bucket-name> im Codeausschnitt an: `aws s3api create-bucket --bucket <sample-app-bucket-name>` Die Lambda-Beispielanwendung lädt JSON-Dateien in diesen Bucket hoch.	Cloud-Administrator

Erstellen der IAM-TVM-Rolle und -Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine TVM-Rolle.	Verwenden Sie einen der folgenden AWS CLI-Befehle, um eine IAM-Rolle zu erstellen. Geben Sie den Wert	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<sample-tvm-role-name> im Befehl an.
	
	Für macOS- oder Linux-Shells:
	
	`aws iam create-role \ --role-name <sample-tvm-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ]}'`
	
	Für die Windows-Befehlszeile:
	
	`aws iam create-role ^ --role-name <sample-tvm-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Principal\": {\"Service\":`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>\"lambda.amazonaws
	.com\"}, \"Action\":
	\"sts:AssumeRole\"
	}]}"</pre>
	Die Lambda-Beispielanw endung übernimmt diese Rolle, wenn die Anwendung aufgerufen wird. Die Fähigkeit, die Anwendungsrolle mit einer bereichsbezogenen Richtlinie anzunehmen, gibt dem Code umfassendere Berechtigungen für den Zugriff auf den S3-Bucket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine eingebundene TVM-Rollenrichtlinie.	Verwenden Sie einen der folgenden AWS CLI-Befehle, um eine IAM-Richtlinie zu erstellen. Geben Sie die Werte <sample-tvm-role-name>,<AWS Account ID> und <sample-app-role-name> im Befehl an.
	
	Für macOS- oder Linux-Shells:
	
	`aws iam put-role-policy \`
	`--role-name <sample-tvm-role-name> \`
	`--policy-name assume-app-role \`
	`--policy-document '{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Effect": "Allow",`
	`"Action": "sts:AssumeRole",`
	`"Resource": "arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>"`
	`}`
	`]}'`
	
	Für die Windows-Befehlszeile:
	
	`aws iam put-role-policy ^`
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--role-name <sample-tvm-role-name> ^ --policy-name assume-app-role ^ --policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Resource\": \"arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>\"}]}"` Diese Richtlinie ist an die TVM-Rolle angehängt. Sie gibt dem Code die Möglichkeit, die Anwendungsrolle anzunehmen, die über umfassendere Berechtigungen für den Zugriff auf den S3-Bucket verfügt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die verwaltete Lambda-Richtlinie an.	Verwenden Sie den folgenden AWS CLI-Befehl, um die `AWSLambdaBasicExecutionRole` IAM-Richtlinie anzuhängen. Geben Sie den Wert **<sample-tvm-role-name>** im Befehl an:
	`aws iam attach-role-policy \ --role-name <sample-tvm-role-name> \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Für die Windows-Befehlszeile:
	`aws iam attach-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Diese verwaltete Richtlinie ist an die TVM-Rolle angehängt, damit Lambda Protokolle an Amazon senden kann CloudWatch.
		Cloud-Administrator

Erstellen der IAM-Anwendungsrolle und -richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendungsrolle.	Verwenden Sie einen der folgenden AWS CLI-Befehle, um eine IAM-Rolle zu erstellen. Geben Sie die Werte <sample-app-role-name>, <AWS Account ID> und <sample-tvm-role-name> im Befehl an. Für macOS- oder Linux-Shells: `aws iam create-role \ --role-name <sample-app-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>" }, "Action": "sts:AssumeRole" } ]}'` Für die Windows-Befehlszeile:	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws iam create-role ^ --role-name <sample-app-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\",\"Principal\": {\"AWS\": \"arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>\"},\"Action\": \"sts:AssumeRole\" }]}"` Die Lambda-Beispielanwendung übernimmt diese Rolle mit einer bereichsbezogenen Richtlinie, um einen mandantenbasierten Zugriff auf einen S3-Bucket zu erhalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine eingebundene Anwendungsrollenrichtlinie.	Verwenden Sie einen der folgenden AWS CLI-Befehle, um eine IAM-Richtlinie zu erstellen. Geben Sie die Werte **<sample-app-role-name>** und **<sample-app-bucket-name>** im Befehl an. Für macOS- oder Linux-Shells: `aws iam put-role-policy \ --role-name <sample-app-role-name> \ --policy-name s3-bucket-access \ --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"], "Resource": "arn:aws:s3:::<sample-app-bucket-name>/*" }, { "Effect": "Allow",`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Action":
	["s3:ListBucket"],
	"Resource
	": "arn:aws:s3:::<sam
	ple-app-bucket-name>"
	}
	]}'</pre>
	Für die Windows-Befehlszeile:
	<pre>aws iam put-role-policy
	^
	--role-name <sample-a
	pp-role-name> ^
	--policy-name s3-bucket
	-access ^
	--policy-documen
	t "{\"Version\":
	\"2012-10-17\",
	\"Statement\":
	[{\"Effect\": \"Allow
	\", \"Action\":
	[\"s3:PutObject\",
	\"s3:GetObject\",
	\"s3:DeleteObject\
	"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-na
	me>/*\"}, {\"Effect\":
	\"Allow\", \"Action\
	": [\"s3:ListBucket
	\"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-name>
	\"}]}"</pre>
	Diese Richtlinie ist an die Anwendungsrolle angehängt. Sie bietet einen breiten Zugriff auf Objekte im S3-Bucket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn die Beispielanwendung die Rolle übernimmt, sind diese Berechtigungen auf einen bestimmten Mandanten mit der dynamisch generierten Richtlinie des TVM beschränkt.	

Erstellen der Lambda-Beispielanwendung mit TVM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die kompilierten Quelldateien herunter.	Laden Sie die `tvm-layer.zip` Dateien `s3UploadSample.jar` und herunter, die als Anlagen enthalten sind. Der Quellcode, der zum Erstellen dieser Artefakte und Kompilierungsinstuctions verwendet wird, finden Sie unter `token-vending-machine-sample-app.zip` .	Cloud-Administrator
Erstellen Sie die Lambda-Ebene.	Verwenden Sie den folgenden AWS CLI-Befehl, um eine Lambda-Ebene zu erstellen, die das TVM für Lambda zugänglich macht. Hinweis: Wenn Sie diesen Befehl nicht von dem Speicherort aus ausführen, an den Sie heruntergeladen haben `tvm-layer`	Cloud-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`.zip` , geben Sie `tvm-layer.zip` im `--zip-file` Parameter den richtigen Pfad zu an.
	
	`aws lambda publish-layer-version \ --layer-name sample-token-vending-machine \ --compatible-runtimes java11 \ --zip-file fileb://tvm-layer.zip`
	
	Für die Windows-Befehlszeile:
	
	`aws lambda publish-layer-version ^ --layer-name sample-token-vending-machine ^ --compatible-runtimes java11 ^ --zip-file fileb://tvm-layer.zip`
	
	Dieser Befehl erstellt eine Lambda-Ebene, die die wiederverwendbare TVM-Bibliothek enthält.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

So erstellen Sie die Lambda-Funktion:	Verwenden Sie den folgenden AWS CLI-Befehl, um eine Lambda-Funktion zu erstellen. Geben Sie die Werte **<sample-app-function-name>**, **<AWS Account ID>**, **<AWS Region>**, **<sample-tvm-role-name>**, **<sample-app-bucket-name>** und **<sample-app-role-name>** im Befehl an.
	
	Hinweis: Wenn Sie diesen Befehl nicht von dem Speicherort aus ausführen , an den Sie heruntergeladen haben `s3UploadSample.jar` , geben Sie `s3UploadSample.jar` im `--zip-file` Parameter den richtigen Pfad zu an.
	
	`aws lambda create-function \`
	`--function-name <sample-app-function-name> \`
	`--timeout 30 \`
	`--memory-size 256 \`
	`--runtime java11 \`
	`--role arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name> \`
	`--handler com.amazon.aws.s3UploadSample.App \`
	`--zip-file fileb://s3UploadSample.jar \`
		Cloud-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
--layers arn:aws:l
ambda:<AWS Region>:<
AWS Account ID>:layer
:sample-token-vend
ing-machine:1 \
--environment "Variable
s={S3_BUCKET=<sample-
app-bucket-name>,
ROLE=arn:aws:iam::<AWS
 Account ID>:role/
<sample-app-role-n
ame>}"
```

Für Windows-Befehlszeile:

```
aws lambda create-fu
nction ^
--function-name
 <sample-app-function-
name>  ^
--timeout 30 ^
--memory-size 256 ^
--runtime java11 ^
--role arn:aws:i
am::<AWS Account
 ID>:role/<sample-tvm-
role-name> ^
--handler com.amazo
n.aws.s3UploadSamp
le.App ^
--zip-file fileb://s
3UploadSample.jar ^
--layers arn:aws:l
ambda:<AWS Region>:<
AWS Account ID>:layer
:sample-token-vend
ing-machine:1 ^
--environment "Variable
s={S3_BUCKET=<samp
le-app-bucket-name
>,ROLE=arn:aws:iam
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`::<AWS Account ID>:role/<sample-app-role-name>}"` Dieser Befehl erstellt eine Lambda-Funktion mit dem Beispielanwendungscode und der angehängten TVM-Ebene. Außerdem werden zwei Umgebungsvariablen festgelegt: `S3_BUCKET` und `ROLE`. Die Beispielanwendung verwendet diese Variablen, um die zu übernehmende Rolle und den S3-Bucket zum Hochladen von JSON-Dokumenten zu bestimmen.	

Testen der Beispielanwendung und TVM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Lambda-Beispielanwendung auf.	Verwenden Sie einen der folgenden AWS CLI-Befehle, um die Lambda-Beispielanwendung mit der erwarteten Nutzlast zu starten. Geben Sie die Werte <sample-app-function-name> und <sample-tenant-name> im Befehl an. Für macOS- und Linux-Shells: `aws lambda invoke \`	Cloud-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--function <sample-app-function-name> \ --invocation-type RequestResponse \ --payload '{"tenant": "<sample-tenant-name>"}' \ --cli-binary-format raw-in-base64-out response.json`
	
	Für die Windows-Befehlszeile:
	
	`aws lambda invoke ^ --function <sample-app-function-name> ^ --invocation-type RequestResponse ^ --payload "{\"tenant\": \"<sample-tenant-name>\"}" ^ --cli-binary-format raw-in-base64-out response.json`
	
	Dieser Befehl ruft die Lambda-Funktion auf und gibt das Ergebnis in einem `response.json` Dokument zurück. Auf vielen Unix-basierten Systemen können Sie `response.json` zu ändern, `/dev/stdout` um die Ergebnisse direkt in Ihre Shell auszugeben, ohne eine weitere Datei zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Wenn Sie den Wert <sample-tenant-name> in nachfolgenden Aufrufen dieser Lambda-Funktion ändern, werden der Speicherort des JSON-Dokuments und die Berechtigungen geändert, die das Token bereitstellt.	
Zeigen Sie den S3-Bucket an, um erstellte Objekte anzuzeigen.	Navigieren Sie zu dem S3-Bucket (<sample-app-bucket-name>), den Sie zuvor erstellt haben. Dieser Bucket enthält ein S3-Objektpräfix mit dem Wert <sample-tenant-name>. Unter diesem Präfix finden Sie ein JSON-Dokument mit dem Namen mit einer UUID. Wenn Sie die Beispielanwendung mehrmals aufrufen, werden weitere JSON-Dokumente hinzugefügt.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie Cloudwatch-Protokolle für die Beispielanwendung an.	Zeigen Sie die Cloudwatch-Protokolle an, die der Lambda-Funktion mit dem Namen <sample-app-function-name> zugeordnet sind. Anweisungen finden Sie unter Zugreifen auf Amazon- CloudWatch Protokolle für AWS Lambda in der AWS Lambda-Dokumentation. Sie können die vom TVM generierte Richtlinie für den Mandantenbereich in diesen Protokollen anzeigen. Diese Tenant-Richtlinie erteilt Berechtigungen für die Beispielanwendung für die Amazon S3-PutObject, -DeleteObject, GetObject- und -ListBucketAPIs, jedoch nur für das Objektpräfix, das mit <sample-tenant-name> verknüpft ist. APIs Wenn Sie bei nachfolgenden Aufrufen der Beispielanwendung <sample-tenant-name> ändern, aktualisiert die TVM die bereichsbezogene Richtlinie so, dass sie dem in der Aufrufnutzlast angegebenen Mandanten entspricht. Diese dynamisch generierte Richtlinie zeigt, wie der Zugriff im Mandantenbereich mit einem TVM in SaaS-Anwe	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ndungen aufrechterhalten werden kann. Die TVM-Funktionalität wird in einer Lambda-Ebene bereitgestellt, sodass sie an andere Lambda-Funktionen angehängt werden kann, die von einer Anwendung verwendet werden, ohne den Code replizieren zu müssen. Eine Veranschaulichung der dynamisch generiert en Richtlinie finden Sie im Abschnitt Zusätzliche Informati onen.	

Zugehörige Ressourcen

- Isolierung von Mandanten mit dynamisch generierten IAM-Richtlinien (Blogbeitrag)
- Anwenden dynamisch generierter Isolationsrichtlinien in SaaS-Umgebung (Blogbeitrag)
- AWS SaaS Boost (eine Open-Source-Referenzumgebung, mit der Sie Ihr SaaS-Angebot zu AWS verschieben können)

Zusätzliche Informationen

Das folgende Amazon-Cloudwatch-Protokoll zeigt die dynamisch generierte Richtlinie, die vom TVM-Code in diesem Muster erstellt wurde. In diesem Screenshot ist`DOC-EXAMPLE-BUCKET` <sample-app-bucket-name> und <sample-tenant-name> `test-tenant-1`. Die von dieser Richtlinie mit Geltungsbereich zurückgegebenen STS-Anmeldeinformationen können keine Aktionen für Objekte im S3-Bucket ausführen, mit Ausnahme von Objekten, die dem Objektschlüsselpräfix zugeordnet sind`test-tenant-1`.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Implementieren Sie das Serverless-Saga-Muster mithilfe von AWS Step Functions

Erstellt von Tabby Ward (AWS), Rohan Mehta (AWS) und Rimpy Tewani (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; Serverless; Cloudnativ	Workload: Open-Source
AWS-Services: Amazon API Gateway; Amazon DynamoDB ;AWS Lambda ;Amazon SNS ;AWS Step Functions		

Übersicht

In einer Microservices-Architektur besteht das Hauptziel darin, entkoppelte und unabhängige Komponenten zu erstellen, um Agilität, Flexibilität und schnellere Markteinführungszeit für Ihre Anwendungen zu fördern. Aufgrund der Entkopplung hat jede Microservice-Komponente ihre eigene Datenpersistenzschicht. In einer verteilten Architektur können sich Geschäftstransaktionen über mehrere Microservices erstrecken. Da diese Microservices keine einzige Atomizitäts-, Konsistenz-, Isolations- und Haltbarkeitstransaktion (ACID) verwenden können, können Teiltransaktionen auftreten. In diesem Fall ist eine gewisse Steuerlogik erforderlich, um die bereits verarbeiteten Transaktionen rückgängig zu machen. Das verteilte Saga-Muster wird normalerweise für diesen Zweck verwendet.

Das Saga-Muster ist ein Fehlerverwaltungsmuster, das dazu beiträgt, Konsistenz in verteilten Anwendungen herzustellen und Transaktionen zwischen mehreren Microservices zu koordinieren, um die Datenkonsistenz aufrechtzuerhalten. Wenn Sie das Saga-Muster verwenden, veröffentlicht jeder Service, der eine Transaktion durchführt, ein Ereignis, das nachfolgende Services auslöst, um die nächste Transaktion in der Kette durchzuführen. Dies wird fortgesetzt, bis die letzte Transaktion in der Kette abgeschlossen ist. Wenn eine Geschäftstransaktion fehlschlägt, orchestriert Saga eine Reihe von Ausgleichstransaktionen, die die Änderungen rückgängig machen, die durch die vorherigen Transaktionen vorgenommen wurden.

Dieses Muster zeigt, wie Sie die Einrichtung und Bereitstellung einer Beispielanwendung (die Reisereservierungen verarbeitet) mit Serverless-Technologien wie AWS Step Functions ,AWS Lambda und Amazon DynamoDB automatisieren. Die Beispielanwendung verwendet auch Amazon API Gateway und Amazon Simple Notification Service (Amazon SNS), um einen Saga-Ausführungskoordinator zu implementieren. Das Muster kann mit einem Infrastructure as Code (IaC)-Framework wie dem AWS Cloud Development Kit (AWS CDK), dem AWS Serverless Application Model (AWS SAM) oder Terraform bereitgestellt werden.

Weitere Informationen zum Saga-Muster und anderen Datenpersistenzmustern finden Sie im Leitfaden Aktivieren der Datenpersistenz in Microservices auf der Website AWS Prescriptive Guidance.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Erstellen eines AWS- CloudFormation Stacks. Weitere Informationen finden Sie unter Zugriffskontrolle in der - CloudFormation Dokumentation.
- IaC-Framework Ihrer Wahl (AWS-CDK, AWS SAM oder Terraform), das mit Ihrem AWS-Konto konfiguriert ist, sodass Sie die Framework-CLI verwenden können, um die Anwendung bereitzustellen.
- NodeJS , wird verwendet, um die Anwendung zu erstellen und lokal auszuführen.
- Ein Code-Editor Ihrer Wahl (z. B. Visual Studio Code, Sublime oder Atom).

Produktversionen

- NodeJS Version 14
- AWS-CDK-Version 2.37.1
- AWS SAM Version 1.71.0
- Terraform Version 1.3.7

Einschränkungen

Event Sourcing ist eine natürliche Möglichkeit, das Saga-Orchestrierungsmuster in einer Microservices-Architektur zu implementieren, in der alle Komponenten lose gekoppelt sind und keine direkten Kenntnisse übereinander haben. Wenn Ihre Transaktion eine kleine Anzahl von Schritten

(drei bis fünf) umfasst, könnte das Saga-Muster eine hervorragende Ergänzung sein. Die Komplexität steigt jedoch mit der Anzahl der Microservices und der Anzahl der Schritte.

Tests und Debugging können bei Verwendung dieses Designs schwierig werden, da Sie alle Services ausführen müssen, um das Transaktionsmuster zu simulieren.

Architektur

Zielarchitektur

Die vorgeschlagene Architektur verwendet AWS Step Functions, um ein Saga-Muster zu erstellen, um Flüge zu reservieren, Autoverleih zu reservieren und Zahlungen für einen Urlaub zu verarbeiten.

Das folgende Workflow-Diagramm veranschaulicht den typischen Ablauf des Reisereservierungssystems. Der Workflow besteht aus der Reservierung von Flugreisen („ReserveFlightBezahlung der Reservierung eines ReserveCarRentalAutos („Bezahler“ („ProcessPaymentBeantwortung der Flugreservierungen“ „ConfirmFlightBezahlt und Bestätigung der AutoverleiheConfirmCarRental“) gefolgt von einer Erfolgsbenachrichtigung, wenn diese Schritte abgeschlossen sind. Wenn das System jedoch auf Fehler beim Ausführen einer dieser Transaktionen stößt, schlägt es abwärts. Beispielsweise löst ein Fehler bei der Zahlungsabwicklung („ProcessPayment“) eine Erstattung („RefundPayment“) aus, der dann eine Stornierung des Autos und des Fluges („CancelRentalReservation“ und „CancelFlightReservation“) auslöst, wodurch die gesamte Transaktion mit einer Fehlermeldung beendet wird.

Dieses Muster stellt separate Lambda-Funktionen für jede Aufgabe bereit, die im Diagramm hervorgehoben ist, sowie drei DynamoDB-Tabellen für Flüge, Autoverleih und Zahlungen. Jede Lambda-Funktion erstellt, aktualisiert oder löscht die Zeilen in den jeweiligen DynamoDB-Tabellen, je nachdem, ob eine Transaktion bestätigt oder zurückgesetzt wurde. Das Muster verwendet Amazon SNS, um Textnachrichten (SMS) an Abonnenten zu senden und sie über fehlgeschlagene oder erfolgreiche Transaktionen zu benachrichtigen.

Automatisierung und Skalierung

Sie können die Konfiguration für diese Architektur mithilfe eines der IaC-Frameworks erstellen. Verwenden Sie einen der folgenden Links für Ihre bevorzugte IaC-.

- Bereitstellen mit AWS CDK

- Bereitstellen mit AWS SAM
- Bereitstellen mit Terraform

Tools

AWS-Services

- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. Über die grafische Step-Functions-Konsole sehen Sie den Workflow Ihrer Anwendung als eine Reihe von ereignisgesteuerten Schritten.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet. Sie können mit DynamoDB eine Datenbanktabelle erstellen, mit der eine beliebige Datenmenge gespeichert und abgerufen werden kann und der Anforderungsdatenverkehr verarbeitet werden kann.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon API Gateway ist ein AWS-Service zum Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST-, HTTP- und - WebSocket APIs in jeder Größenordnung.
- Amazon Simple Notification Service (Amazon SNS)ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten bereitstellt.
- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework zur Definition Ihrer Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen wie TypeScript, JavaScript, Python, Java und C#/.Netz.
- AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework für die Erstellung von Serverless-Anwendungen. Es bietet eine Kurznotation, um Funktionen, APIs, Datenbanken und Ereignisquellenzuordnungen auszudrücken.

Code

Der Code für eine Beispielanwendung, die das Saga-Muster demonstriert, einschließlich der IaC-Vorlage (AWS CDK, AWS SAM oder Terraform), der Lambda-Funktionen und der DynamoDB-Tabellen, finden Sie unter den folgenden Links. Folgen Sie den Anweisungen im ersten Epics, um diese zu installieren.

- Bereitstellen mit AWS CDK
- Bereitstellen mit AWS SAM
- Bereitstellen mit Terraform

Polen

Installieren von Paketen, Kompilieren und Erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die NPM-Pakete.	Erstellen Sie ein neues Verzeichnis, navigieren Sie in einem Terminal zu diesem Verzeichnis und klonen Sie das GitHub Repository Ihrer Wahl aus dem Abschnitt Code weiter oben in diesem Muster. Führen Sie im Stammordner mit der `-package.json` Datei den folgenden Befehl aus, um alle Node Package Manager (NPM)-Pakete herunterzuladen und zu installieren: `npm install`	Entwickler, Cloud-Architekt
Kompilieren Sie Skripts.	Führen Sie im Stammordner den folgenden Befehl aus, um den TypeScript Transpiler anzuweisen, alle erforderlichen JavaScript Dateien zu erstellen: `npm run build`	Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Achten Sie auf Änderungen und kompilieren Sie sie neu.	Führen Sie im Stammordner den folgenden Befehl in einem separaten Terminalfenster aus, um nach Codeänder ungen zu suchen, und kompilieren Sie den Code, wenn er eine Änderung erkennt: `npm run watch`	Entwickler, Cloud-Architekt
Führen Sie Einheitentests durch (nur AWS-CDK).	Wenn Sie das AWS-CDK verwenden, führen Sie im Stammordner den folgenden Befehl aus, um die Tests der Jest-Einheit durchzuführen: `npm run test`	Entwickler, Cloud-Architekt

Bereitstellen von Ressourcen für das AWS-Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Demo-Stack in AWS bereit.	Wichtig: Die Anwendung ist AWS-regionsunabhängig. Wenn Sie ein Profil verwenden , müssen Sie die Region entweder explizit im AWS Command Line Interface (AWS CLI)-Profil oder über AWS CLI-Umgebungsvaria blen deklarieren.	Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Führen Sie im Stammordner den folgenden Befehl aus, um eine Bereitstellungsgruppe zu erstellen und sie im Standard-AWS-Konto und in der Standardregion bereitzustellen.
	
	AWS-CDK:
	
	`cdk bootstrap`
	`cdk deploy`
	
	AWS SAM:
	
	`sam build`
	`sam deploy --guided`
	
	Terraform:
	
	`terraform init`
	`terraform apply`
	
	Dieser Schritt kann einige Minuten dauern. Dieser Befehl verwendet die Standardanmeldeinformationen, die für die AWS CLI konfiguriert wurden.
	
	Notieren Sie sich die API Gateway-URL, die nach Abschluss der Bereitstellung in der Konsole angezeigt wird. Sie benötigen diese Informati	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen, um den Saga-Ausf ührungsablauf zu testen.	

Vergleichen Sie den bereitges tellten Stack mit dem aktuellen Status.	Führen Sie im Stammordn er den folgenden Befehl aus, um den bereitgestellten Stack mit dem aktuellen Status zu vergleichen, nachdem Sie Änderungen am Quellcode vorgenommen haben:
	AWS-CDK:
	`cdk diff`
	AWS SAM:
	`sam deploy`
	Terraform:
	`terraform plan`
		Entwickler, Cloud-Architekt

Testen des Ausführungsablaufs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Saga-Ausf ührungsablauf.	Navigieren Sie zu der API Gateway-URL, die Sie im vorherigen Schritt notiert haben, als Sie den Stack bereitgestellt haben. Diese URL löst den Start des Zustandsautomaten aus. Weitere Informationen zum	Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bearbeiten des Flows des Zustandsautomaten durch Übergabe verschiedener URL-Parameter finden Sie im Abschnitt Zusätzliche Informationen. Um die Ergebnisse anzuzeigen, melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zur Step Functions-Konsole. Hier können Sie jeden Schritt des Saga-Zustandsautomaten sehen. Sie können auch die DynamoDB-Tabelle anzeigen, um die eingefügten, aktualisierten oder gelöschten Datensätze anzuzeigen. Wenn Sie den Bildschirm häufig aktualisieren, können Sie die Änderung des Transaktionsstatus von `pending` zu beobachten`confirmed` . Sie können das SNS-Thema abonnieren, indem Sie den Code in der `stateMachine.ts` Datei mit Ihrer Mobiltelefonnummer aktualisieren, um SMS-Nachrichten bei erfolgreichen oder fehlgeschlagenen Reservierungen zu empfangen. Weitere Informationen finden Sie unter Amazon	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SNS im Abschnitt Zusätzliche Informationen.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen Sie Ressourcen.	Um die für diese Anwendung bereitgestellten Ressourcen zu bereinigen, können Sie einen der folgenden Befehle verwenden.
	AWS-CDK:
	`cdk destroy`
	AWS SAM:
	`sam delete`
	Terraform:
	`terraform destroy`
		App-Entwickler, Cloud-Architekt

Zugehörige Ressourcen

Technische Papiere

- Implementieren von Microservices in AWS
- Serverless Application Lens
- Aktivieren der Datenpersistenz in Microservices

AWS-Servicedokumentation

- Erste Schritte mit dem AWS-CDK
- Erste Schritte mit AWS SAM
- AWS Step Functions
- Amazon DynamoDB
- AWS Lambda
- Amazon API Gateway
- Amazon SNS

Tutorials

- Praktische Workshops für Serverless Computing

Zusätzliche Informationen

Code

Zu Testzwecken stellt dieses Muster API Gateway und eine Test-Lambda-Funktion bereit, die den Step-Functions-Zustandsautomaten auslöst. Mit Step Functions können Sie die Funktionalität des Reisereservierungssystem steuern, indem Sie einen `run_type` Parameter übergeben, um Fehler in „ReserveFlight“, „ReserveCarRental“, „ProcessPayment“, „ConfirmFlight“ und „“ nachzuahmenConfirmCarRental.

Die `saga` Lambda-Funktion (`sagaLambda.ts`) nimmt Eingaben von den Abfrageparametern in der API Gateway-URL entgegen, erstellt das folgende JSON-Objekt und übergibt es zur Ausführung an Step Functions:

```
let input = {
"trip_id": tripID, //  value taken from query parameter, default is AWS request ID
"depart_city": "Detroit",
"depart_time": "2021-07-07T06:00:00.000Z",
"arrive_city": "Frankfurt",
"arrive_time": "2021-07-09T08:00:00.000Z",
"rental": "BMW",
"rental_from": "2021-07-09T00:00:00.000Z",
"rental_to": "2021-07-17T00:00:00.000Z",
"run_type": runType // value taken from query parameter, default is "success"
```

```
};
```

Sie können mit verschiedenen Flows des Step-Functions-Zustandsautomaten experimentieren, indem Sie die folgenden URL-Parameter übergeben:

- Erfolgreiche Ausführung https://{api-Gateway-URL}
- Reservieren von Telefonie https://{api gateway url}?runType =failFlightsReservation
- Bestätigen Sie den HTTPS://{api-Gateway url}?runType =failFlightsConfirmation
- Reservieren Sie ein Auto, das fehlschlägt https://{api gateway url}?runType = failCarRentalReservierung
- Bestätigen Sie den Ausfall des Autos https://{api Gateway url}?runType =failCarRentalConfirmation
- Zahlungsfehler verarbeiten https://{api gateway url}?runType =failPayment
- Übergeben einer Journey ID Bol https://{api gateway url}?tripID ={standardmäßig ist die Fahrt-ID die AWS-Anforderungs-ID}

IaC-Vorlagen

Die verknüpften Repositorys enthalten IaC-Vorlagen, mit denen Sie die gesamte Beispielanwendung für die Reisereservierung erstellen können.

- Bereitstellen mit AWS CDK
- Bereitstellen mit AWS SAM
- Bereitstellen mit Terraform

DynamoDB-Tabellen

Im Folgenden finden Sie die Datenmodelle für die Flug-, Autoverleih- und Zahlungstabellen.

```
Flight Data Model:
 var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: flightReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: flightReservationID},
        'depart_city' : {S: event.depart_city},
        'depart_time': {S: event.depart_time},
```

```
        'arrive_city': {S: event.arrive_city},
        'arrive_time': {S: event.arrive_time},
        'transaction_status': {S: 'pending'}
      }
    };

Car Rental Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: carRentalReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: carRentalReservationID},
        'rental': {S: event.rental},
        'rental_from': {S: event.rental_from},
        'rental_to': {S: event.rental_to},
        'transaction_status': {S: 'pending'}
      }
    };

Payment Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: paymentID},
        'trip_id' : {S: event.trip_id},
        'id': {S: paymentID},
        'amount': {S: "750.00"}, // hard coded for simplicity as implementing any
 monetary transaction functionality is beyond the scope of this pattern
        'currency': {S: "USD"},
        'transaction_status': {S: "confirmed"}
      }
    };
```

Lambda-Funktionen

Die folgenden Funktionen werden erstellt, um den Ablauf und die Ausführung des Zustandsautomaten in Step Functions zu unterstützen:

- Reserve Bols : Fügt einen Datensatz mit einem `transaction_status` von in die DynamoDB-Tabelle ein`pending`, um einen Flug zu reservieren.

- Bestätigen des Flugs: Aktualisiert den Datensatz in der DynamoDB-Tabelle, um ihn `transaction_status` auf festzulegen`confirmed`, um den Flug zu bestätigen.
- Reservierung stornieren: Löscht den Datensatz aus der DynamoDB-Tabelle, um den ausstehenden Flug zu stornieren.
- Reservieren eines Autos: Fügt einen Datensatz in die DynamoDB CarRentals -Tabelle mit einem `transaction_status` von ein`pending`, um eine Autoverleih zu reservieren.
- bestätigte Autohärenzen : Aktualisiert den Datensatz in der DynamoDB CarRentals -Tabelle, um `transaction_status` auf festzulegen`confirmed`, um die Autoverleih zu bestätigen.
- Reservierung für stornierte Autos: Löscht den Datensatz aus der DynamoDB CarRentals -Tabelle, um die ausstehende Autoverleihung zu stornieren.
- Zahlung verarbeiten: Fügt einen Datensatz in die DynamoDB-Zahlungstabelle für die Zahlung ein.
- Zahlung abbrechen: Löscht den Datensatz aus der DynamoDB-Tabelle Zahlungen für die Zahlung.

Amazon SNS

Die Beispielanwendung erstellt das folgende Thema und Abonnement für das Senden von SMS-Nachrichten und das Benachrichtigen des Kunden über erfolgreiche oder fehlgeschlagene Reservierungen. Wenn Sie beim Testen der Beispielanwendung Textnachrichten erhalten möchten, aktualisieren Sie das SMS-Abonnement mit Ihrer gültigen Telefonnummer in der Definitionsdatei des Zustandsautomaten.

AWS-CDK-Ausschnitt (Hinzufügen der Telefonnummer in der zweiten Zeile des folgenden Codes):

```
const topic = new  sns.Topic(this, 'Topic');
topic.addSubscription(new subscriptions.SmsSubscription('+11111111111'));
const snsNotificationFailure = new tasks.SnsPublish(this ,'SendingSMSFailure', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation Failed'),
});

const snsNotificationSuccess = new tasks.SnsPublish(this ,'SendingSMSSuccess', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation is Successful'),
});
```

AWS SAM-Ausschnitt (ersetzen Sie die +1111111111 Zeichenfolgen durch Ihre gültige Telefonnummer):

```
  StateMachineTopic11111111111:
    Type: 'AWS::SNS::Subscription'
    Properties:
      Protocol: sms
      TopicArn:
        Ref: StateMachineTopic
      Endpoint: '+11111111111'
    Metadata:
      'aws:sam:path': SamServerlessSagaStack/StateMachine/Topic/+11111111111/Resource
```

Terraform-Ausschnitt (ersetzen Sie die +111111111 Zeichenfolge durch Ihre gültige Telefonnummer):

```
resource "aws_sns_topic_subscription" "sms-target" {
  topic_arn = aws_sns_topic.topic.arn
  protocol  = "sms"
  endpoint  = "+11111111111"
}
```

Erfolgreiche Reservierungen

Der folgende Flow veranschaulicht eine erfolgreiche Reservierung mit „ReserveFlight“, „ReserveCarRental“ und „ProcessPayment“, gefolgt von „ConfirmFlight“ und „ConfirmCarRental“. Der Kunde wird über die erfolgreiche Reservierung per SMS-Nachrichten benachrichtigt, die an den Abonnenten des SNS-Themas gesendet werden.

Fehlgeschlagene Reservierungen

Dieser Flow ist ein Beispiel für einen Fehler im Saga-Muster. Wenn nach der Reservierung von Flug- und Autoverleih „ProcessPayment“ fehlschlägt, werden die Schritte in umgekehrter Reihenfolge storniert. Die Reservierungen werden freigegeben und der Kunde wird über SMS-Nachrichten, die an den Abonnenten des SNS-Themas gesendet werden, über den Fehler informiert.

Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

amazon-ecs-anywhere-cdkQuellcode-Repository: -samples	Umgebung: PoC oder Pilot	Technologien: Modernisierung; Container und Mikroservices; Hybrid Cloud DevOps; Infrastruktur
Arbeitslast: Alle anderen Workloads	AWS-Services: AWS CDK; Amazon ECS; AWS Identity and Access Management	

Übersicht

Amazon ECS Anywhere ist eine Erweiterung des Amazon Elastic Container Service (Amazon ECS). Sie können ECS Anywhere verwenden, um native Amazon ECS-Aufgaben in einer lokalen oder vom Kunden verwalteten Umgebung bereitzustellen. Diese Funktion hilft, Kosten zu senken und komplexe lokale Container-Orchestrierung und Betriebsabläufe zu vereinfachen. Sie können ECS Anywhere verwenden, um Containeranwendungen sowohl in lokalen als auch in Cloud-Umgebungen bereitzustellen und auszuführen. Dadurch entfällt für Ihr Team die Notwendigkeit, mehrere Bereiche und Fähigkeiten zu erlernen oder komplexe Software eigenständig zu verwalten.

Dieses Muster veranschaulicht die Schritte zur Einrichtung von ECS Anywhere mithilfe von AWS Cloud Development Kit (AWS CDK) -Stacks.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. (Weitere Informationen finden Sie unter Installation, Aktualisierung und Deinstallation der AWS-CLI in der AWS-CLI-Dokumentation.)

- AWS CDK Toolkit, installiert und konfiguriert. (Sehen Sie sich das AWS CDK Toolkit in der AWS CDK-Dokumentation an und folgen Sie den Anweisungen, um Version 2 global zu installieren.)
- Node Package Manager (npm), installiert und konfiguriert für das AWS-CDK in. TypeScript (Weitere Informationen finden Sie unter Node.js und npm herunterladen und installieren in der npm-Dokumentation.)

Einschränkungen

- Einschränkungen und Überlegungen finden Sie unter Externe Instances (Amazon ECS Anywhere) in der Amazon ECS-Dokumentation.

Produktversionen

- AWS CDK Toolkit, Version 2
- npm Version 7.20.3 oder höher
- Node.js Version 16.6.1 oder höher

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS-CDK
- Amazon ECS Anywhere
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Systemarchitektur des ECS Anywhere-Setups unter Verwendung des AWS-CDK mit TypeScript, wie in diesem Muster implementiert.

1. Wenn Sie den AWS-CDK-Stack bereitstellen, erstellt er einen CloudFormation Stack auf AWS.
2. Der CloudFormation Stack stellt einen Amazon ECS-Cluster und zugehörige AWS-Ressourcen bereit.

3. Um eine externe Instance bei einem Amazon ECS-Cluster zu registrieren, müssen Sie den AWS Systems Manager Agent (SSM Agent) auf Ihrer virtuellen Maschine (VM) installieren und die VM als von AWS Systems Manager verwaltete Instanz registrieren.
4. Sie müssen auch den Amazon ECS-Container-Agenten und Docker auf Ihrer VM installieren, um sie als externe Instance beim Amazon ECS-Cluster zu registrieren.
5. Wenn die externe Instance registriert und mit dem Amazon ECS-Cluster konfiguriert ist, kann sie mehrere Container auf Ihrer VM ausführen, die als externe Instance registriert ist.

Automatisierung und Skalierung

Das mit diesem Muster bereitgestellte GitHub Repository verwendet das AWS-CDK als IaC-Tool (Infrastructure as Code), um die Konfiguration für diese Architektur zu erstellen. AWS CDK hilft Ihnen bei der Orchestrierung von Ressourcen und der Einrichtung von ECS Anywhere.

Tools

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Code

Der Quellcode für dieses Muster ist im Amazon ECS Anywhere CDK Samples-Repository verfügbar. GitHub Folgen Sie den Anweisungen im nächsten Abschnitt, um das Repository zu klonen und zu verwenden.

Epen

Überprüfen Sie die AWS-CDK-Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-CDK-Version.	Überprüfen Sie die Version des AWS CDK Toolkit, indem	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den folgenden Befehl ausführen: `cdk --version` Für dieses Muster ist AWS CDK Version 2 erforderlich. Wenn Sie eine frühere Version von AWS CDK haben, folgen Sie den Anweisungen in der AWS CDK-Dokumentation, um sie zu aktualisieren.	

Richten Sie AWS-Anmeldeinformationen ein.	Um Anmeldeinformationen einzurichten, führen Sie den `aws configure` Befehl aus und folgen Sie den Anweisungen:
	`$aws configure`
	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`
		DevOps Ingenieur

Bootstrap für die AWS-CDK-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das AWS-CDK-Code-Repository.	Klonen Sie das GitHub Code-Repository für dieses Muster mit dem folgenden Befehl: `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cdk-samples.git`	DevOps Ingenieur
Bootstrapping für die Umwelt.	Führen Sie den folgenden Befehl aus, um die CloudFormation AWS-Vorlage für das Konto und die AWS-Region bereitzustellen, die Sie verwenden möchten: `cdk bootstrap <account-number>/<Region>` Weitere Informationen finden Sie unter Bootstrapping in der AWS CDK-Dokumentation.	DevOps Ingenieur

Erstellen und implementieren Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Paketabhängigkeiten und kompilieren Sie TypeScript Dateien.	Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien, indem Sie die folgenden Befehle ausführen:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$cd amazon-ecs-anywher e-cdk-samples`
	`$npm install`
	`$npm fund`
	
	Mit diesen Befehlen werden alle Pakete aus dem Beispiel-Repository installiert.
	
	Wichtig: Wenn Sie eine Fehlermeldung über fehlende Pakete erhalten, verwenden Sie einen der folgenden Befehle:
	
	`$npm ci`
	
	–oder–
	
	`$npm install -g @aws-cdk/<package_name>`
	
	Weitere Informationen finden Sie unter npm ci und npm install in der npm-Dokum entation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Projekt.	Führen Sie den folgenden Befehl aus, um den Projektcode zu erstellen: `npm run build` Weitere Informationen zum Erstellen und Bereitstellen des Projekts finden Sie unter Ihre erste AWS-CDK-App in der AWS-CDK-Dokumentation.	DevOps Ingenieur
Stellen Sie das Projekt bereit.	Führen Sie den folgenden Befehl aus, um den Projektcode bereitzustellen: `cdk deploy`	DevOps Ingenieur
Überprüfen Sie die Erstellung und Ausgabe des Stacks.	Öffnen Sie die CloudFormation AWS-Konsole unter https://console.aws.amazon.com/cloudformation und wählen Sie den `EcsAnywhereStack` Stack aus. Auf der Registerkarte Ausgaben werden die Befehle angezeigt, die auf Ihrer externen VM ausgeführt werden sollen.	DevOps Ingenieur

Richten Sie einen lokalen Computer ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Ihre VM mithilfe von Vagrant ein.	Zu Demonstrationszwecken können Sie HashiCorp Vagrant verwenden, um eine VM zu erstellen. Vagrant ist ein Open-Source-Hilfsprogramm für den Aufbau und die Wartung portabler virtueller Softwareentwicklungsumgebungen. Erstellen Sie eine Vagrant-VM, indem Sie den `vagrant up` Befehl im Stammverzeichnis ausführen, in dem Vagrantfile gespeichert ist. Weitere Informationen finden Sie in der Vagrant-Dokumentation.	DevOps Ingenieur
Registrieren Sie Ihre VM als externe Instanz.	1. Melden Sie sich mit dem `vagrant ssh` Befehl bei der Vagrant-VM an. Weitere Informationen finden Sie in der Vagrant-Dokumentation. 2. Erstellen Sie einen Aktivierungscode und eine ID, mit denen Sie Ihre VM bei AWS Systems Manager registrieren und Ihre externe Instanz aktivieren können. Die Ausgabe dieses Befehls umfasst `ActivationId` und `ActivationCode` Werte:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws ssm create-activation --iam-role EcsAnywhereInstanceRole | tee ssm-activation.json`
	
	3. Exportieren Sie die Aktivierungs-ID und die Codewerte:
	
	`export ACTIVATION_ID=<activation-ID>`
	`export ACTIVATION_CODE=<activation-code>`
	
	4. Laden Sie das Installationsskript auf Ihren lokalen Server oder Ihre VM herunter:
	
	`curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh" && sudo chmod +x ecs-anywhere-install.sh`
	
	5. Führen Sie das Installationsskript auf Ihrem lokalen Server oder Ihrer VM aus:
	
	`sudo ./ecs-anywhere-install.sh \`
	`--cluster test-ecs-anywhere \`
	`--activation-id $ACTIVATION_ID \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--activation-code $ACTIVATION_CODE \ --region <Region>` Weitere Informationen zum Einrichten und Registrieren Ihrer VM finden Sie unter Registrierung einer externen Instance in einem Cluster in der Amazon ECS-Dokum entation.	

Überprüfen Sie den Status von ECS Anywhere und der externen VM.	Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Ihre virtuelle Box mit der Amazon ECS-Steuerebene verbunden ist und läuft:
	
	`aws ssm describe-instance-information`
	`aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen bereinigen und löschen.	Nachdem Sie dieses Muster durchgegangen sind, sollten Sie die von Ihnen erstellten Ressourcen entfernen, um weitere Kosten zu vermeiden . Führen Sie zum Aufräumen den folgenden Befehl aus:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk destroy`	

Zugehörige Ressourcen

- Dokumentation zu Amazon ECS Anywhere
- Amazon ECS Anywhere Anywhere-Demo
- Beispiele Amazon ECS Anywhere Anywhere-Workshops

Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS

Erstellt von Vijai Anand Ramalingam (AWS) und Sreelaxmi Pai (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; Container und Microservices; Softwareentwicklung und Tests; Web- und mobile Apps	Arbeitslast: Microsoft
AWS-Services: Amazon CloudWatch; Amazon ECS; AWS Systems Manager		

Übersicht

Dieses Muster beschreibt die Schritte zur Modernisierung einer älteren, monolithischen ASP.NET Web Forms-Anwendung durch Portierung auf ASP.NET Core auf AWS.

Durch die Portierung von ASP.NET Web Forms-Anwendungen auf ASP.NET Core können Sie die Leistung, die Kosteneinsparungen und das robuste Ökosystem von Linux nutzen. Dies kann jedoch ein erheblicher manueller Aufwand sein. In diesem Muster wird die Legacy-Anwendung schrittweise mithilfe eines schrittweisen Ansatzes modernisiert und anschließend in der AWS-Cloud containerisiert.

Stellen Sie sich eine ältere, monolithische Anwendung für einen Einkaufswagen vor. Nehmen wir an, dass sie als ASP.NET-Webforms-Anwendung erstellt wurde und aus ASPX-Seiten mit einer Code-Behind () -Datei besteht. `aspx.cs` Der Modernisierungsprozess besteht aus den folgenden Schritten:

1. Teilen Sie den Monolith in Microservices auf, indem Sie die entsprechenden Zerlegungsmuster verwenden. Weitere Informationen finden Sie im Leitfaden Decomposing monoliths into microservices auf der AWS Prescriptive Guidance Guidance-Website.
2. Portieren Sie Ihre ältere ASP.NET Web Forms (.NET Framework) -Anwendung auf ASP.NET Core in .NET 5 oder höher. In diesem Muster verwenden Sie den Portierungsassistenten für .NET, um Ihre ASP.NET Web Forms-Anwendung zu scannen und Inkompatibilitäten mit ASP.NET Core zu identifizieren. Dadurch wird der manuelle Portierungsaufwand reduziert.

3. Entwickeln Sie die Web Forms-Benutzeroberflächenebene mithilfe von React neu. Dieses Muster deckt die Neuentwicklung der Benutzeroberfläche nicht ab. Anweisungen finden Sie unter Neue React-App erstellen in der React-Dokumentation.
4. Entwickeln Sie die Web Forms-Codebehind-Datei (Geschäftsschnittstelle) als ASP.NET Core-Web-API neu. Dieses Muster verwendet NDepend-Berichte, um benötigte Dateien und Abhängigkeiten zu identifizieren.
5. Aktualisieren Sie gemeinsam genutzte Projekte wie Business Logic und Data Access in Ihrer Legacy-Anwendung auf .NET 5 oder höher, indem Sie den Portierungsassistenten für .NET verwenden.
6. Fügen Sie AWS-Services hinzu, um Ihre Anwendung zu ergänzen. Sie können beispielsweise Amazon CloudWatch Logs verwenden, um die Protokolle Ihrer Anwendung zu überwachen, zu speichern und darauf zuzugreifen, und AWS Systems Manager, um Ihre Anwendungseinstellungen zu speichern.
7. Containerisieren Sie die modernisierte ASP.NET Core-Anwendung. Dieses Muster erstellt eine Docker-Datei, die auf Linux in Visual Studio abzielt und Docker Desktop verwendet, um sie lokal zu testen. In diesem Schritt wird davon ausgegangen, dass Ihre Legacy-Anwendung bereits auf einer lokalen Windows-Instance oder einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance ausgeführt wird. Weitere Informationen finden Sie im Muster Einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 EC2-Linux-Instance ausführen.
8. Stellen Sie die modernisierte ASP.NET-Kernanwendung auf Amazon Elastic Container Service (Amazon ECS) bereit. Dieses Muster deckt den Bereitstellungsschritt nicht ab. Anweisungen finden Sie im Amazon ECS-Workshop.

Hinweis: Dieses Muster deckt keine Schritte zur Entwicklung der Benutzeroberfläche, zur Datenbankmodernisierung oder zur Container-Bereitstellung ab.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Visual Studio oder Visual Studio Code, heruntergeladen und installiert.
- Zugriff auf ein AWS-Konto über die AWS-Managementkonsole und die AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2. (Weitere Informationen finden Sie in den Anweisungen zur Konfiguration der AWS-CLI.)
- Das AWS Toolkit for Visual Studio (siehe Anweisungen zur Einrichtung).

- Docker Desktop, heruntergeladen und installiert.
- .NET SDK, heruntergeladen und installiert.
- NDepend-Tool, heruntergeladen und installiert. Um die NDepend-Erweiterung für Visual Studio zu installieren, führen Sie den Befehl aus `NDepend.VisualStudioExtension.Installer` (siehe Anweisungen). Sie können je nach Ihren Anforderungen Visual Studio 2019 oder 2022 auswählen.
- Portierungsassistent für .NET, heruntergeladen und installiert.

Architektur

Modernisierung der Warenkorb-Anwendung

Das folgende Diagramm veranschaulicht den Modernisierungsprozess für eine ältere ASP.NET-Einkaufswagenanwendung.

Zielarchitektur

Das folgende Diagramm veranschaulicht die Architektur der modernisierten Einkaufswagen-Anwendung auf AWS. ASP.NET Core-Web-APIs werden in einem Amazon ECS-Cluster bereitgestellt. Protokollierungs- und Konfigurationsservices werden von Amazon CloudWatch Logs und AWS Systems Manager bereitgestellt.

Tools

AWS-Services

- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Um mehr Kontrolle über Ihre Infrastruktur zu erhalten, können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von EC2-Instances ausführen, die Sie verwalten.
- Amazon CloudWatch Logs — Amazon CloudWatch Logs zentralisiert die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services, die Sie verwenden. Sie können die Protokolle anzeigen und überwachen, sie nach bestimmten Fehlercodes oder Mustern durchsuchen, sie nach bestimmten Feldern filtern oder sie für future Analysen sicher archivieren.

- AWS Systems Manager – AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können. Mithilfe der Systems Manager Manager-Konsole können Sie Betriebsdaten von mehreren AWS-Services anzeigen und betriebliche Aufgaben in Ihren AWS-Ressourcen automatisieren. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem es Ihre verwalteten Instanzen scannt und festgestellte Richtlinienverstöße meldet (oder Korrekturmaßnahmen ergreift).

Tools

- Visual Studio oder Visual Studio Code — Tools zum Erstellen von.NET-Anwendungen, Web-APIs und anderen Programmen.
- AWS Toolkit for Visual Studio — Eine Erweiterung für Visual Studio, die beim Entwickeln, Debuggen und Bereitstellen von.NET-Anwendungen hilft, die AWS-Services verwenden.
- Docker Desktop — Ein Tool, das die Erstellung und Bereitstellung containerisierter Anwendungen vereinfacht.
- NDepend — Ein Analysator, der .NET-Code auf Abhängigkeiten, Qualitätsprobleme und Codeänderungen überwacht.
- Portierungsassistent für .NET — Ein Analysetool, das .NET-Code scannt, um Inkompatibilitäten mit .NET Core zu identifizieren und den Migrationsaufwand abzuschätzen.

Epen

Portieren Sie Ihre Legacy-Anwendung auf .NET 5 oder eine neuere Version

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Ihre.NET Framework-Legacy-Anwendung auf .NET 5.	Sie können den Portierungsassistenten für .NET verwenden, um Ihre ältere ASP.NET Web Forms-Anwendung auf .NET 5 oder höher zu konvertieren. Folgen Sie den Anweisungen in der Dokumentation zu Porting Assistant for .NET.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie NDepend-Berichte.	Wenn Sie Ihre ASP.NET Web Forms-Anwendung modernisieren, indem Sie sie in Microservices zerlegen, benötigen Sie möglicherweise nicht alle .cs-Dateien aus der Legacy-Anwendung. Sie können NDepend verwenden, um einen Bericht für jede Code-Behind (.cs) -Datei zu generieren, um alle Aufrufer und Aufrufer abzurufen. Dieser Bericht hilft Ihnen dabei, nur die benötigten Dateien in Ihren Microservices zu identifizieren und zu verwenden. Nachdem Sie NDepend installiert haben (siehe Abschnitt Voraussetzungen), öffnen Sie die Lösung (.sln-Datei) für Ihre Legacy-Anwendung in Visual Studio und gehen Sie wie folgt vor: 1. Erstellen Sie die Legacy-Anwendung in Visual Studio. 2. Wählen Sie in der Visual Studio-Menüleiste NDepend, Neues NDepend-Projekt an aktuelle VS-Lösung anhängen. 3. Wählen Sie .NET-Assemblys analysieren.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wenn die Analyse abgeschlossen ist, navigieren Sie im Solution Explorer zu dem Projekt. Klicken Sie mit der rechten Maustaste auf eine beliebige Codebehind-Datei (z. B.`listprodu cts.aspx.cs`), für die Sie den Bericht erstellen möchten, und wählen Sie dann Im Abhängigkeitsdiagr amm anzeigen aus. 5. Wählen Sie in der Navigatio nsleiste Anrufer und Anrufer und anschließend Codeabfrage bearbeiten aus. 6. Wählen Sie im Bereich Abfragen und Regeln bearbeiten den Download-Pfeil und dann Nach Excel exportieren aus. Dieser Vorgang generiert einen Bericht für die Code-Behind-Datei, in der alle Anrufer und Anrufer aufgeführ t sind. Weitere Informationen zum Abhängigkeitsdiagramm finden Sie in der NDepend-D okumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue.NET 5-Lösung.	So erstellen Sie eine neue.NET 5-Struktur (oder höher) für Ihre modernisierten ASP.NET Core-Web-APIs: 1. Öffnen Sie Visual Studio. 2. Erstellen Sie eine neue, leere Lösung. 3. Erstellen Sie neue Projekte, die auf .NET 5 (oder höher) abzielen und auf Ihrer Legacy-Anwendung basieren. Beispiele für ältere und neue Projekte für eine Einkaufswagen-Anwendung finden Sie im Abschnitt Zusätzliche Informationen. 4. Verwenden Sie den NDepend-Bericht aus dem vorherigen Schritt, um alle erforderlichen Dateien zu identifizieren. Kopieren Sie diese Dateien aus der Anwendung, die Sie zuvor aktualisiert haben, und fügen Sie sie der neuen Lösung hinzu. 5. Erstellen Sie die Lösung und beheben Sie alle Probleme. Weitere Informationen zum Erstellen von Projekten und	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lösungen finden Sie in der Visual Studio-Dokumentation. Hinweis: Während Sie die Lösung erstellen und die Funktionalität überprüfen, können Sie zusätzlich zu den Dateien, die NDepend identifiziert hat, mehrere zusätzliche Dateien identifizieren, die der Lösung hinzugefügt werden sollen.	

Aktualisieren Sie Ihren Anwendungscode

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie Web-APIs mit ASP.NET Core.	Nehmen wir an, dass es sich bei einem der Microservices, die Sie in Ihrer alten Monolith-Einkaufswagen-Anwendung identifiziert haben, um Produkte handelt. Sie haben im vorherigen Epos ein neues ASP.NET Core-Web-API-Projekt für Produkte erstellt. In diesem Schritt identifizieren und modernisieren Sie alle Webformulare (.aspx-Seiten), die sich auf Produkte beziehen. Gehen wir davon aus, dass Produkte aus vier Webformularen bestehen, wie weiter oben im Abschnitt Architektur dargestellt:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Produkte auflisten • Produkt ansehen • Produkt hinzufügen/bearbeiten • Produkt löschen Sie sollten jedes Webformular analysieren, alle Anfragen identifizieren, die an die Datenbank gesendet werden, um eine gewisse Logik auszuführen, und Antworten erhalten. Sie können jede Anfrage als Web-API-Endpunkt implementieren. Aufgrund ihrer Webformulare können Produkte die folgenden möglichen Endpunkte haben: • `/api/products` • `/api/products/{id}` • `/api/products/add` • `/api/products/update/{id}` • `/api/products/delete/{id}` Wie bereits erwähnt, können Sie auch alle anderen Projekte, die Sie auf .NET 5 aktualisiert haben, wiederverwenden, einschließlich	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Business Logic, Data Access und gemeinsam genutzte/ gemeinsame Projekte.	
Konfigurieren Sie Amazon CloudWatch Logs.	Sie können Amazon CloudWatch Logs verwenden , um die Protokolle Ihrer Anwendung zu überwache n, zu speichern und darauf zuzugreifen. Sie können Daten mithilfe eines AWS-SDK in Amazon CloudWatch Logs protokollieren. Sie können auch.NET-Anwendungen in CloudWatch Logs integrieren, indem Sie gängige .NET-Logg ing-Frameworks wie NLog, Log4Net und das ASP.NET Core-Logging-Framework verwenden. Weitere Informationen zu diesem Schritt finden Sie im Blogbeitrag Amazon CloudWatch Logs and.NET Logging Frameworks.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den AWS Systems Manager Parameter Store.	Sie können den AWS Systems Manager Parameter Store verwenden, um Anwendungseinstellungen wie Verbindungszeichenfolgen getrennt vom Code Ihrer Anwendung zu speichern. Das NuGet Paket Amazon.Extensions.Configuration.SystemsManager vereinfacht, wie Ihre Anwendung diese Einstellungen aus dem AWS Systems Manager Parameter Store in das .NET Core-Konfigurationssystem lädt. Weitere Informationen zu diesem Schritt finden Sie im Blogbeitrag .NET Core-Konfigurationsanbieter für AWS Systems Manager.	App-Developer

Fügen Sie Authentifizierung und Autorisierung hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie ein geteiltes Cookie zur Authentifizierung.	Die Modernisierung einer älteren Monolith-Anwendung ist ein iterativer Prozess, bei dem der Monolith und seine modernisierte Version nebeneinander existieren müssen. Sie können ein geteiltes Cookie verwenden	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, um eine nahtlose Authentif izierung zwischen den beiden Versionen zu erreichen . Die ältere ASP.NET-A nwendung validiert weiterhin die Benutzeranmeldeinf ormationen und gibt das Cookie aus, während die modernisierte ASP.NET Core-Anwendung das Cookie validiert. Anweisungen und Beispielc ode finden Sie im Beispielp rojekt. GitHub	

Erstellen Sie den Container und führen Sie ihn lokal aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Docker-Im age mit Visual Studio.	In diesem Schritt erstellen Sie eine Docker-Datei mithilfe der Visual Studio for .NET Core-Web-API. 1. Öffnen Sie Visual Studio. 2. Wählen Sie im Solution Explorer im Kontextmenü (Rechtsklick) Ihres Projekts die Optionen Hinzufügen, Docker-Unterstützung aus. 3. Wählen Sie Linux als Zielbetriebssystem aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Visual Studio erstellt eine Docker-Datei für Ihr Projekt. Eine Docker-Beispieldatei finden Sie unter Visual Studio Container Tools for Docker auf der Microsoft-Website.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Container mit Docker Desktop und führen Sie ihn aus.	Jetzt können Sie den Container in Docker Desktop erstellen, erstellen und ausführen.
	1. Öffnen Sie ein Befehlszeilenfenster. Navigieren Sie zu dem Lösungsordner, in dem sich die Docker-Datei befindet. Führen Sie den folgenden Befehl aus, um das Docker-Image zu erstellen:
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Führen Sie den folgenden Befehl aus, um alle Docker-Images anzuzeigen:
	`docker images`
	3. Führen Sie den folgenden Befehl aus, um einen Container zu erstellen und auszuführen:
	`docker run -d -p 8080:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
	4. Öffnen Sie Docker Desktop und wählen Sie dann
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Containers/Apps. Sie können einen neuen Container mit dem Namen running sehen. `aspnetcoreewebapicontainer`	

Zugehörige Ressourcen

- Einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 EC2-Linux-Instance ausführen (AWS Prescriptive Guidance)
- Amazon ECS-Workshop
- Führen Sie ECS Blue/Green-Bereitstellungen CodeDeploy mithilfe von AWS durch CloudFormation (AWS-Dokumentation) CloudFormation
- Erste Schritte mit NDepend (NDepend-Dokumentation)
- Portierungsassistent für .NET

Zusätzliche Informationen

Die folgenden Tabellen enthalten Beispiele für Beispielprojekte für eine ältere Warenkorbanwendung und die entsprechenden Projekte in Ihrer modernisierten ASP.NET Core-Anwendung.

Legacy-Lösung:

Project name	Vorlage für ein Projekt	Target framework
Geschäftsschnittstelle	Klassenbibliothek	.NET Framework.
BusinessLogic	Klassenbibliothek	.NET Framework.
WebApplication	ASP.NET Framework-Webanwendung	.NET Framework.
UnitTests	NUnit-Testprojekt	.NET Framework.
Geteilt -> Allgemein	Klassenbibliothek	.NET Framework.

Geteilt -> Framework	Klassenbibliothek	.NET Framework.

Neue Lösung:

Project name	Vorlage für ein Projekt	Target framework
BusinessLogic	Klassenbibliothek	.NET 5.0
<WebAPI>	ASP.NET-Core-Web-API	.NET 5.0
<WebAPI>. UnitTests	NUnit 3-Testprojekt	.NET 5.0
Geteilt -> Allgemein	Klassenbibliothek	.NET 5.0
Geteilt -> Framework	Klassenbibliothek	.NET 5.0

Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus

Erstellt von HARI OHM PRASATH RAJAGOPAL (AWS)

Umgebung: PoC oder Pilot	Technologien: Modernisierung; Serverlos; Betrieb	Arbeitslast: Open Source
AWS-Services: Amazon EC2 EC2-Containerregister; Amazon ECS; AWS CodeCommit; AWS Fargate; AWS Lambda; Amazon SNS		

Übersicht

Dieses Muster beschreibt, wie geplante und ereignisgesteuerte Workloads mithilfe von AWS Fargate in großem Umfang in der Amazon Web Services (AWS) -Cloud ausgeführt werden.

In dem Anwendungsfall, den dieses Muster einrichtet, wird der Code immer dann nach sensiblen AWS-Informationen wie der AWS-Kontonummer und den Anmeldeinformationen durchsucht, wenn eine Pull-Anfrage eingereicht wird. Die Pull-Anfrage initiiert eine Lambda-Funktion. Die Lambda-Funktion ruft eine Fargate-Aufgabe auf, die sich um den Codescan kümmert. Lambda wird immer dann initiiert, wenn eine neue Pull-Anfrage gestellt wird. Wenn beim Scan vertrauliche Informationen gefunden werden, sendet Amazon Simple Notification Service (Amazon SNS) die Scanergebnisse in einer E-Mail-Nachricht.

Dieses Muster ist in den folgenden Geschäftsanwendungsfällen hilfreich:

- Wenn Ihr Unternehmen viele geplante und ereignisgesteuerte Workloads ausführen muss, die aufgrund von Einschränkungen in Bezug auf Laufzeit (15-Minuten-Limit) oder Arbeitsspeicher nicht von AWS Lambda ausgeführt werden können
- Wenn Sie möchten, dass AWS die für diese Workloads bereitgestellten Instances verwaltet

Wenn Sie dieses Muster verwenden, haben Sie die Möglichkeit, eine neue Virtual Private Cloud (VPC) zu erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS CodeCommit für das Hosten der Codebasis und das Erstellen von Pull-Requests
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows
- Workloads, die in Containern ausgeführt werden
- Ausführbare Apache Maven-Datei, die im Klassenpfad eingerichtet ist

Architektur

Der gesamte Ablauf umfasst die folgenden Schritte.

1. Immer wenn eine neue Pull-Anfrage eingereicht wird CodeCommit, wird eine Lambda-Funktion initiiert. Die Lambda-Funktion überwacht das `CodeCommit Pull Request State Change` Ereignis über Amazon. EventBridge
2. Die Lambda-Funktion sendet eine neue Fargate-Aufgabe mit den folgenden Umgebungsparametern zum Auschecken und Scannen des Codes.

   ```
   RUNNER # <<TaskARN>>
   SNS_TOPIC # <<SNSTopicARN>>
   SUBNET # <<Subnet in which Fargate task gets launched>>
   ```

   Findet der Scan vertrauliche Informationen im Code, leitet Fargate eine neue Nachricht an das Amazon SNS SNS-Thema weiter.
3. Ein SNS-Abonnent liest die Nachricht aus dem Thema und sendet eine E-Mail-Nachricht.

Technologie

- AWS CodeCommit
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)

- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon SNS
- Docker

Tools

Tools

- AWS CLI — Die AWS-Befehlszeilenschnittstelle (CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services.
- AWS CodeCommit — AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet. Auf diese CodeCommit Weise können Teams in einer sicheren und hochgradig skalierbaren Umgebung gemeinsam an Code arbeiten.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Registry, die Entwickler zum Speichern, Verwalten und Bereitstellen von Docker-Container-Images verwenden können.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service. Sie können Amazon ECS verwenden, um Container in einem Cluster auszuführen, zu stoppen und zu verwalten.
- AWS Fargate — AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen, ohne Server oder Cluster von Amazon EC2 EC2-Instances verwalten zu müssen.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht. Herausgeber kommunizieren asynchron mit Abonnenten, indem sie eine Nachricht erstellen und an ein Thema senden, bei dem es sich um einen logischen Zugriffspunkt und Kommunikationskanal handelt. Kunden, die das SNS-Thema abonnieren, erhalten veröffentlichte Nachrichten über ein unterstütztes Protokoll wie Lambda, E-Mail, mobile Push-Benachrichtigungen und mobile Textnachrichten (SMS).

- Docker — Docker unterstützt Sie beim Erstellen, Testen und Bereitstellen von Anwendungen in Paketen, die als Container bezeichnet werden.
- Git-Client — Befehlszeilen- oder Desktop-Tool zum Auschecken der benötigten Artefakte
- Maven — Apache Maven ist ein Projektmanagement-Tool zur zentralen Verwaltung des Builds, der Berichterstattung und der Dokumentation eines Projekts.

Epen

Richten Sie das lokale Repository ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code herunter.	Laden Sie im Bereich Anlagen die ZIP-Datei herunter und extrahieren Sie die Dateien.	Entwickler, AWS-Syste madministrator
Richten Sie das Repo ein.	Führen Sie es `mvn clean install` im Stammordner aus.	Entwickler, AWS-Syste madministrator

Erstellen Sie ein Amazon ECR-Image und übertragen Sie das Image

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon ECR-Repository und melden Sie sich an.	Öffnen Sie die Amazon ECR-Konsole. Wählen Sie im Navigationsbereich Repositor ies und dann Create repositor y aus. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt Verwandte Ressourcen.	Entwickler, AWS-Syste madministrator
Pushen Sie Ihr Container-Image.	Öffnen Sie das Repositor y, wählen Sie Push-Befehle anzeigen und melden Sie sich	Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bei Docker an. Nachdem Sie angemeldet sind, führen Sie die Befehle mit den erforderl ichen Ersetzungen aus, die sich unter Push the container image im Abschnitt Zusätzlic he Informationen befinden. Dadurch wird das Docker-Co ntainer-Image hochgeladen, das zum Scannen von Code verwendet wird. Nachdem der Upload abgeschlossen ist, kopieren Sie die URL des neuesten Builds in das Amazon ECR-Repository.	

Erstellen Sie das CodeCommit Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das CodeCommi t Repository.	Um ein neues CodeCommit AWS-Repository zu erstellen , führen Sie den Befehl unter CodeCommit Repositor y erstellen im Abschnitt Zusätzliche Informationen aus.	Entwickler, AWS-Syste madministrator

Erstellen Sie die VPC (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Wenn Sie eine neue VPC anstelle einer vorhanden en verwenden möchten,	Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	führen Sie die Befehle unter VPC erstellen im Abschnitt Zusätzliche Informationen aus. Das AWS Cloud Developme nt Kit (AWS CDK) -Skript gibt die IDs der erstellten VPC und des Subnetzes aus.	

Erstellen Sie den Amazon ECS-Cluster und die Fargate-Aufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Cluster und die Aufgabe.	Um einen Amazon ECS-Cluster und eine Fargate-A ufgabendefinition zu erstellen , führen Sie die Befehle unter Cluster und Aufgabe erstellen im Abschnitt Zusätzliche Informationen aus. Stellen Sie sicher, dass bei der Ausführun g des Shell-Skripts die richtige VPC-ID und der Amazon ECR-Repo-URI als Parameter übergeben werden. Das Skript erstellt eine Fargate-A ufgabendefinition, die auf das Docker-Image (verantwortlich für das Scannen) verweist. Das Skript erstellt dann einen Job und eine zugehörige Ausführungsrolle.	Entwickler, AWS-Syste madministrator
Überprüfen Sie den Amazon ECS-Cluster.	Öffnen Sie die Amazon-EC S-Konsole. Wählen Sie im Navigationsbereich Clusters	Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und dann den neu erstellten Amazon ECS-Cluster mit dem Namen Fargate-Job-Cluste r aus. Wählen Sie anschließ end im Navigationsbereich Aufgabendefinition aus und vergewissern Sie sich, dass es eine neue Aufgabend efinition mit dem Präfix gibt. `awscdkfargateecsTa skDef`	

Erstellen Sie das SNS-Thema und den Abonnenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Um ein SNS-Thema zu erstellen, führen Sie den Befehl unter SNS-Thema erstellen im Abschnitt Zusätzliche Informationen aus. Notieren Sie sich nach erfolgreicher Erstellung den`SNS ARN`, der im nächsten Schritt verwendet wird.	Entwickler, AWS-Syste madministrator
Erstellen Sie den SNS-Abonn enten.	Um einen E-Mail-Abonnenten für das SNS-Thema zu erstellen, führen Sie den Befehl unter SNS-Abonn ent erstellen im Abschnitt Zusätzliche Informationen aus. Stellen Sie sicher, dass Sie den Befehl ersetzen `TopicARN` und `Email`	Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`address` im CLI-Befehl verwenden. Um E-Mail-Be nachrichtigungen zu erhalten, stellen Sie sicher, dass Sie die E-Mail-Adresse bestätigen, die als Abonnent verwendet wird.	

Lambda-Funktion erstellen und auslösen CodeCommit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Funktion und den Auslöser.	Um eine Lambda-Funktion mit einem CodeCommit Trigger zu erstellen, führen Sie den Befehl unter Lambda-Funktion und CodeCommit Trigger im Abschnitt Zusätzliche Informati onen aus. Stellen Sie sicher, dass Sie die Parameter durch die entsprechenden Werte ersetzen, bevor Sie den Befehl ausführen. Das Skript erstellt die Lambda-Funktion und konfiguriert sie so, dass sie aufgerufen wird, wenn eine neue Pull-Anfrage gestellt wird.	Entwickler, AWS-Syste madministrator

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendung.	Wenn Sie vertrauliche AWS-Informationen in das	Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommit Repo einchecken, sollte die Lambda-Funktion initiiert werden. Die Lambda-Funktion initiiert die Fargate-Aufgabe, die den Code scannt und die Scanergebnisse in einer E-Mail-Benachrichtigung sendet.	

Zugehörige Ressourcen

- Erstellen eines Amazon ECR-Repositorys
- Docker-Images auf Amazon ECR übertragen

Zusätzliche Informationen

Übertragen Sie das Container-Image

```
> cd 1-ecr-image-push
> ./run.sh <<ecr-repository>>
```

Erstellen Sie das CodeCommit Repository

```
aws codecommit create-repository --repository-name test-repo --repository-description
 "My Test repository"
```

Erstellen einer VPC

```
> cd 2-create-vpc
> ./run.sh
```

Ausgabe

```
aws-batch-cdk-vpc-efs-launch-template.privatesubnet = subnet-<<id>>
```

```
aws-batch-cdk-vpc-efs-launch-template.publicsubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.vpcid = vpc-<<id>>
```

Erstellen Sie den Cluster und die Aufgabe

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 3-create-ecs-task
> ./run.sh <<vpc-id>> <<ecr-repo-uri>>
```

Ausgabe

```
aws-cdk-fargate-ecs.CLUSTERNAME = Fargate-Job-Cluster
aws-cdk-fargate-ecs.ClusterARN = <<cluster_arn>>
aws-cdk-fargate-ecs.ContainerARN = Fargate-Container
aws-cdk-fargate-ecs.TaskARN = <<task_arn>>
aws-cdk-fargate-ecs.TaskExecutionRole = <<execution_role_arn>>
aws-cdk-fargate-ecs.TaskRole = <<task_role_arn>>
```

Erstellen Sie das SNS-Thema

```
aws sns create-topic --name code-commit-topic
```

Erstellen Sie den SNS-Abonnenten

```
aws sns subscribe \
    --topic-arn <<topic_arn>> \
    --protocol email \
    --notification-endpoint <<email_address>>
```

Lambda-Funktion und Trigger CodeCommit

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 5-Lambda-CodeCommit-Trigger
> ./run.sh <<taskarn>> <<snstopicarn>> subnet-<<id>> <<codecommitarn>>
```

Ausgabe

```
aws-cdk-fargate-lambda-event.Cloudwatchrule = <<cloudwatchrule>>
```

```
aws-cdk-fargate-lambda-event.CodeCommitLambda = AWS-Code-Scanner-Function
aws-cdk-fargate-lambda-event.LambdaRole = <<lambdaiamrole>>
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Mandanten-Onboarding in SaaS-Architektur für das Silomodell mit C# und AWS CDK

Erstellt von Tabby Ward (AWS), Susmitha Reddy Gankidi (AWS) und Vijai Anand Ramalingam (AWS)

Code-Repository: Tennat Onboarding Silo	Umgebung: PoC oder Pilotprojekt	Technologien: Modernisierung; Cloudnativ; SaaS DevOps;
Workload: Open-Source	AWS-Services: AWS CloudFormation; Amazon DynamoDB ; Amazon DynamoDB Streams; AWS Lambda ; Amazon API Gateway	

Übersicht

Software as a Service (SaaS)-Anwendungen können mit einer Vielzahl verschiedener Architekturmodelle erstellt werden. Das Silomodell bezieht sich auf eine Architektur, in der Mandanten dedizierte Ressourcen zur Verfügung gestellt werden.

SaaS-Anwendungen verlassen sich auf ein reibungsloses Modell, um neue Mandanten in ihre Umgebung einzuführen. Dies erfordert häufig die Orchestrierung einer Reihe von Komponenten, um alle Elemente, die zum Erstellen eines neuen Mandanten erforderlich sind, erfolgreich bereitzustellen und zu konfigurieren. Dieser Prozess wird in der SaaS-Architektur als Mandanten-On-Boarding bezeichnet. Das Onboarding sollte für jede SaaS-Umgebung vollständig automatisiert werden, indem Infrastruktur als Code in Ihrem Onboarding-Prozess verwendet wird.

Dieses Muster führt Sie durch ein Beispiel für die Erstellung eines Mandanten und die Bereitstellung einer grundlegenden Infrastruktur für den Mandanten in Amazon Web Services (AWS). Das Muster verwendet C# und das AWS Cloud Development Kit (AWS CDK).

Da dieses Muster einen Abrechnungsalarm auslöst, empfehlen wir, den Stack in der AWS-Region USA Ost (Nord-Virginia) oder us-east-1 bereitzustellen. Weitere Informationen finden Sie in der AWS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein AWS Identity and Access Management (IAM)-Prinzipal mit ausreichendem IAM-Zugriff zum Erstellen von AWS-Ressourcen für dieses Muster. Weitere Informationen finden Sie unter IAM-Rollen.
- Installieren Sie Amazon Command Line Interface (AWS CLI) und konfigurieren Sie AWS CLI für die AWS-CDK-Bereitstellung.
- Visual Studio 2022 wurde heruntergeladen und installiert oder Visual Studio Code wurde heruntergeladen und installiert.
- AWS Toolkit for Visual Studio einrichten.
- .NET Core 3.1 oder höher (erforderlich für C#-AWS-CDK-Anwendungen)
- Amazon.Lambda.Tools installiert.

Einschränkungen

- AWS CDK verwendet AWS CloudFormation, sodass AWS-CDK-Anwendungen CloudFormation Service Quotas unterliegen. Weitere Informationen finden Sie unter AWS- CloudFormation Kontingente.
- Der Tenant- CloudFormation Stack wird mit einer CloudFormation Servicerolle `infra-cloudformation-role` mit Platzhalterzeichen für Aktionen (`sns*` und `sqs*`) erstellt, jedoch mit Ressourcen, die auf das `tenant-cluster` Präfix beschränkt sind. Bewerten Sie für einen Produktionsanwendungsfall diese Einstellung und gewähren Sie nur den erforderlichen Zugriff auf diese Servicerolle. Die `InfrastructureProvision` Lambda-Funktion verwendet auch ein Platzhalterzeichen (`cloudformation*`), um den CloudFormation Stack bereitzustellen, jedoch mit Ressourcen, die auf das `tenant-cluster` Präfix beschränkt sind.
- Der Docker-Build dieses Beispielcodes verwendet `--platform=linux/amd64`, um `linux/amd64` basierte Images zu erzwingen. Dadurch soll sichergestellt werden, dass die endgültigen Image-Artefakte für Lambda geeignet sind, das standardmäßig x86-64-Architektur verwendet.

Wenn Sie die Lambda-Zielarchitektur ändern müssen, müssen Sie sowohl die Dockerfiles als auch die AWS-CDK-Codes ändern. Weitere Informationen finden Sie im Blogbeitrag Migrieren von AWS Lambda-Funktionen zu Arm-basierten AWS Graviton2-Prozessoren.

- Der Stack-Löschvorgang bereinigt keine CloudWatch Protokolle (Protokollgruppen und Protokolle), die vom Stack generiert wurden. Sie müssen die Protokolle manuell über die Amazon- CloudWatch Konsole der AWS-Managementkonsole oder die über die API bereinigen.

Dieses Muster ist als Beispiel eingerichtet. Bewerten Sie für den Produktionseinsatz die folgenden Einstellungen und nehmen Sie Änderungen auf der Grundlage Ihrer Geschäftsanforderungen vor:

- Für den AWS Simple Storage Service (Amazon S3)-Bucket in diesem Beispiel ist die Versionsverwaltung der Einfachheit halber nicht aktiviert. Bewerten und aktualisieren Sie die Einrichtung nach Bedarf.
- In diesem Beispiel werden der Einfachheit halber Amazon API Gateway-REST-API-Endpunkte ohne Authentifizierung, Autorisierung oder Drosselung eingerichtet. Für den Produktionseinsatz empfehlen wir, das System in die Geschäftssicherheitsinfrastruktur zu integrieren. Bewerten Sie diese Einstellung und fügen Sie nach Bedarf die erforderlichen Sicherheitseinstellungen hinzu.
- Für dieses Beispiel für eine Tenant-Infrastruktur haben Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Queue Service (Amazon SQS) nur minimale Einstellungen. Der AWS Key Management Service (AWS KMS) für jeden Mandanten wird für Amazon CloudWatch- und Amazon SNS-Services im Konto geöffnet, die auf der Grundlage der AWS KMS-Schlüsselrichtlinie verwendet werden sollen. Die Einrichtung ist nur ein Beispiel für einen Platzhalter. Passen Sie die Einrichtung nach Bedarf an Ihren geschäftlichen Anwendungsfall an.
- Das gesamte Setup, das unter anderem API-Endpunkte und die Bereitstellung und Löschung von Backend-Tenants mithilfe von AWS umfasst CloudFormation, deckt nur den grundlegenden zufriedenen Pfadfall ab. Bewerten und aktualisieren Sie die Einrichtung mit der erforderlichen Wiederholungslogik, zusätzlicher Logik zur Fehlerbehandlung und Sicherheitslogik basierend auf Ihren Geschäftsanforderungen.
- Der Beispielcode wird mit up-to-date cdk-nag getestet, um zum Zeitpunkt dieses Schreibens nach Richtlinien zu suchen. Neue Richtlinien können in Zukunft durchgesetzt werden. Diese neuen Richtlinien erfordern möglicherweise, dass Sie den Stack basierend auf den Empfehlungen manuell ändern, bevor der Stack bereitgestellt werden kann. Überprüfen Sie den vorhandenen Code, um sicherzustellen, dass er Ihren Geschäftsanforderungen entspricht.
- Der Code basiert darauf, dass das AWS-CDK ein zufälliges Suffix generiert, anstatt sich auf statische zugewiesene physische Namen für die am häufigsten erstellten Ressourcen zu verlassen.

Diese Einrichtung soll sicherstellen, dass diese Ressourcen eindeutig sind und nicht mit anderen Stacks in Konflikt stehen. Weitere Informationen finden Sie in der AWS-CDK-Dokumentation. Passen Sie dies an Ihre Geschäftsanforderungen an.

- In diesem Beispielcode werden .NET-Lambda-Artefakte in Docker-basierte Images verpackt und mit der von Lambda bereitgestellten Container-Image-Laufzeit ausgeführt. Die Container-Image-Laufzeit bietet Vorteile für standardmäßige Übertragungs- und Speichermechanismen (Container-Registrys) und genauere lokale Testumgebungen (über das Container-Image). Sie können das Projekt auf die Verwendung von Lambda bereitgestellten .NET-Laufzeiten umstellen, um die Build-Zeit der Docker-Images zu verkürzen. Anschließend müssen Sie jedoch Übertragungs- und Speichermechanismen einrichten und sicherstellen, dass die lokale Einrichtung mit der Lambda-Einrichtung übereinstimmt. Passen Sie den Code an die Geschäftsanforderungen der Benutzer an.

Produktversionen

- AWS-CDK-Version 2.45.0 oder höher
- Visual Studio 2022

Architektur

Technologie-Stack

- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon DynamoDB
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS

Architektur

Das folgende Diagramm zeigt den Erstellungsablauf des Tenant-Stacks. Weitere Informationen zu den Stacks Steuerebene und Mandantentechnologie finden Sie im Abschnitt Zusätzliche Informationen.

Ablauf der Erstellung von Tenant-Stacks

1. Der Benutzer sendet eine POST-API-Anforderung mit neuer Mandantennutzlast (Tenant-Name, Mandantenbeschreibung) in JSON an eine von Amazon API Gateway gehostete REST-API. Das API Gateway verarbeitet die Anforderung und leitet sie an die Backend-Lambda-Tenant-On-boarding-Funktion weiter. In diesem Beispiel gibt es keine Autorisierung oder Authentifizierung. In einer Produktionseinrichtung sollte diese API in das SaaS-Infrastruktur-Sicherheitssystem integriert werden.
2. Die Mandanten-On-Boarding-Funktion überprüft die Anforderung. Anschließend wird versucht, den Mandantendatensatz, der den Mandantennamen, den generierten Mandanten Universally Unique Identifier (UUID) und die Mandantenbeschreibung enthält, in der Tabelle Amazon DynamoDB Tenant On-boarding zu speichern.
3. Nachdem DynamoDB den Datensatz gespeichert hat, initiiert ein DynamoDB-Stream die nachgelagerte Lambda-Tenant-Infrastruktur-Funktion.
4. Die Lambda-Funktion Tenant Infrastructure agiert basierend auf dem empfangenen DynamoDB-Stream. Wenn der Stream für das INSERT-Ereignis bestimmt ist, verwendet die Funktion den NewImage Abschnitt des Streams (aktueller Aktualisierungsdatensatz, Mandantenname-Feld), um aufzurufen und eine neue Tenant-Infrastruktur mithilfe der Vorlage CloudFormation zu erstellen, die im S3-Bucket gespeichert ist. Die CloudFormation Vorlage erfordert den Parameter Tenant Name.
5. AWS CloudFormation erstellt die Tenant-Infrastruktur basierend auf den CloudFormation Vorlagen- und Eingabeparametern.
6. Jede Einrichtung der Tenant-Infrastruktur verfügt über einen CloudWatch Alarm, einen Abrechnungsalarm und ein Alarmereignis.
7. Das Alarmereignis wird zu einer Nachricht an ein SNS-Thema, das mit dem AWS KMS-Schlüssel des Mandanten verschlüsselt wird.
8. Das SNS-Thema leitet die empfangene Alarmmeldung an die SQS-Warteschlange weiter, die mit dem AWS KMS des Mandanten für den Verschlüsselungsschlüssel verschlüsselt wird.

Andere Systeme können in Amazon SQS integriert werden, um Aktionen basierend auf Nachrichten in der Warteschlange auszuführen. Um den Code generisch zu halten, verbleiben eingehende Nachrichten in der Warteschlange und müssen manuell gelöscht werden.

Ablauf der Löschung des Tenant-Stacks

1. Der Benutzer sendet eine DELETE-API-Anfrage mit neuer Mandantennutzlast (Tenant-Name, Mandantenbeschreibung) in JSON an die von Amazon API Gateway gehostete REST-API, die die Anfrage verarbeitet und an die Mandanten-On-On-On-On-boarding-Funktion weiterleitet. In diesem Beispiel gibt es keine Autorisierung oder Authentifizierung. In einer Produktionseinrichtung wird diese API in das SaaS-Infrastruktur-Sicherheitssystem integriert.
2. Die Mandanten-On-Boarding-Funktion überprüft die Anforderung und versucht dann, den Mandantendatensatz (Tenant-Name) aus der Mandanten-On-Boarding-Tabelle zu löschen.
3. Nachdem DynamoDB den Datensatz erfolgreich gelöscht hat (der Datensatz ist in der Tabelle vorhanden und wird gelöscht), initiiert ein DynamoDB-Stream die nachgelagerte Lambda-Tenant-Infrastruktur-Funktion.
4. Die Lambda-Funktion Tenant Infrastructure agiert basierend auf dem empfangenen DynamoDB-Stream-Datensatz. Wenn der Stream für das REMOVE-Ereignis bestimmt ist, verwendet die Funktion den OldImage Abschnitt des Datensatzes (Datensatzinformationen und Mandantennamefeld vor der letzten Änderung, die gelöscht wird), um das Löschen eines vorhandenen Stacks basierend auf diesen Datensatzinformationen zu initiieren.
5. AWS CloudFormation löscht den Ziel-Tenant-Stack entsprechend der Eingabe.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie beim Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST-, HTTP- und - WebSocket APIs in jeder Größenordnung.
- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, mit dem Sie mit Ihrer AWS Cloud Development Kit (AWS CDK)-App interagieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Toolkit for Visual Studio ist ein Plugin für die integrierte Entwicklungsumgebung (IDE) von Visual Studio. Das Toolkit for Visual Studio unterstützt die Entwicklung, das Debuggen und die Bereitstellung von .NET-Anwendungen, die AWS-Services verwenden.

Andere Tools

- Visual Studio ist eine IDE, die Compiler, Codevervollständigungstools, grafische Designer und andere Funktionen umfasst, die die Softwareentwicklung unterstützen.

Code

Der Code für dieses Muster befindet sich im Beispiel-Repository Mandanten-Onboarding in SaaS Architecture für Silo Model APG.

Sekunden

AWS-CDK einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Node.js-Installation.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Node.js auf Ihrem lokalen Computer installiert ist. `node --version`	AWS-Administrator, AWS DevOps
Installieren Sie AWS CDK Toolkit.	Führen Sie den folgenden Befehl aus, um AWS CDK Toolkit auf Ihrem lokalen Computer zu installieren. `npm install -g aws-cdk` Wenn npm nicht installiert ist, können Sie es von der Node.js-Website aus installieren.	AWS-Administrator, AWS DevOps
Überprüfen Sie die AWS CDK Toolkit-Version.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die AWS CDK Toolkit-Version auf Ihrem Computer korrekt installiert ist. `cdk --version`	AWS-Administrator, AWS DevOps

Überprüfen des Codes für die Mandanten-Onboarding-Steuerebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository und navigieren Sie zum `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example` Ordner. Öffnen Sie in Visual Studio 2022 die `\src\TenantOnboardingInfra.sln` Lösung. Öffnen Sie die `TenantOnboardingInfraStack.cs` Datei und überprüfen Sie den Code. Die folgenden Ressourcen werden als Teil dieses Stacks erstellt: • DynamoDB-Tabelle • S3-Bucket (Laden Sie die CloudFormation Vorlage in den S3-Bucket hoch.) • Lambda-Ausführungsrolle • Lambda-Funktion • API Gateway-API • Ereignisquelle zur Lambda-Funktion	AWS-Administrator, AWS DevOps
Überprüfen Sie die CloudFormation Vorlage.	Öffnen Sie im `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-exam`	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ple\template` Ordner `infra.yaml` und überprüfen Sie die CloudFormation Vorlage. Diese Vorlage wird mit dem Mandantennamen verkettet, der aus der DynamoDB-Tabelle für das Mandanten-Onboarding abgerufen wird. Die Vorlage stellt die Tenant-spezifische Infrastruktur bereit. In diesem Beispiel werden der AWS KMS-Schlüssel, Amazon SNS, Amazon SQS und der CloudWatch Alarm bereitgestellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Mandanten -Onboarding-Funktion.	Öffnen Sie `Function.cs` und überprüfen Sie den Code für die Mandanten -Onboarding-Funktion, die mit der Vorlage Visual Studio AWS Lambda Project (.NET Core- C#) mit der Vorlage .NET 6 (Container Image) erstellt wird. Öffnen Sie die `Dockerfile` und überprüfen Sie den Code. ist `Dockerfile` eine Textdatei, die aus Anweisungen zum Erstellen des Lambda-Container-Images besteht. Beachten Sie, dass die folgenden NuGet Pakete dem `TenantOnboardingFunction` Projekt als Abhängigkeiten hinzugefügt werden: • `Amazon.Lambda.APIGatewayEvents` • `AWSSDK.DynamoDBv2` • `Newtonsoft.Json`	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Tenant-InfraProvisioning Funktion.	Navigieren Sie zu `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\InfraProvisioningFunction` . Öffnen Sie `Function.cs` und überprüfen Sie den Code für die Mandanten infrastruktur-Bereitstellungsfunktion, die mit der Vorlage Visual Studio AWS Lambda Project (.NET Core- C#) mit der Vorlage .NET 6 (Container Image) erstellt wird. Öffnen Sie die `Dockerfile` und überprüfen Sie den Code. Beachten Sie, dass die folgenden NuGet Pakete dem `InfraProvisioningFunction` Projekt als Abhängigkeiten hinzugefügt werden: • `Amazon.Lambda.DynamoDBEvents` • `AWSSDK.DynamoDBv2` • `AWSSDK.Cloudformation`	App-Entwickler, AWS DevOps

Bereitstellen der AWS-Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lösung.	Führen Sie die folgenden Schritte aus, um die Lösung zu erstellen: 1. Öffnen Sie in Visual Studio 2022 die `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra.sln` Lösung. 2. Öffnen Sie das Kontextmenü (rechte Maustaste) für die Lösung und wählen Sie Lösung erstellen aus. Hinweis: Stellen Sie sicher, dass Sie das `Amazon.CDK.Lib NuGet` Paket auf die neueste Version im `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra` Projekt aktualisieren, bevor Sie die Lösung erstellen.	App-Developer
Bootstrappen Sie die AWS-CDK-Umgebung.	Öffnen Sie die Windows-Eingabeaufforderung und navigieren Sie zum Stammordner der AWS-CDK-	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	App, in dem die `cdk.json` Datei verfügbar ist (`\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example`). Führen Sie den folgenden Befehl für Bootstrapping aus.
	`cdk bootstrap`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk bootstrap --profile <profile name>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Listen Sie die AWS-CDK-S tacks auf.	Führen Sie den folgenden Befehl aus, um alle Stacks aufzulisten, die im Rahmen dieses Projekts erstellt werden sollen.
	`cdk ls`
	`cdk ls --profile`
	`<profile name>`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk ls --profile`
	`<profile name>`
		AWS-Administrator, AWS DevOps

Überprüfen Sie, welche AWS-Ressourcen erstellt werden.	Führen Sie den folgenden Befehl aus, um alle AWS-Ressourcen zu überprüfen, die im Rahmen dieses Projekts erstellt werden.
	`cdk diff`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk diff --profile`
	`<profile name>`
		AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie alle AWS-Ressourcen mithilfe von AWS CDK bereit.	Führen Sie den folgenden Befehl aus, um alle AWS-Ressourcen bereitzustellen.
	`cdk deploy --all --require-approval never`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk deploy --all --require-approval never --profile <profile name>`
	Nachdem die Bereitstellung abgeschlossen ist, kopieren Sie die API-URL aus dem Abschnitt Outputs in der Eingabeaufforderung, wie im folgenden Beispiel gezeigt.
	`Outputs: TenantOnboardingInfraStack.TenantOnboardingAPIEndpoint42E526D7 = https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/`
		AWS-Administrator, AWS DevOps

Überprüfen der Funktionalität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen neuen Mandanten.	Senden Sie die folgende curl-Anforderung, um den neuen Mandanten zu erstellen.
	`curl -X POST <TenantOnboardingAPIEndpoint* from CDK Output>tenant -d '{"Name":"Tenant123", "Description":"Stack for Tenant123"}'`
	Ändern Sie den Platzhalter `<TenantOnboardingAPIEndpoint* from CDK Output>` in den tatsächlichen Wert von AWS CDK, wie im folgenden Beispiel gezeigt.
	`curl -X POST https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant -d '{"Name": "Tenant123", "Description":"test12"}'`
	Das folgende Beispiel zeigt die Ausgabe.
	`{"message": "A new tenant added - 5/4/2022 7:11:30 AM"}`
		App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die neu erstellten Mandantendetails in DynamoDB .	Führen Sie die folgenden Schritte aus, um die neu erstellten Mandantendetails in DynamoDB zu überprüfen. 1. Öffnen Sie die AWS-Managementkonsole und navigieren Sie zum Amazon DynamoDB-Service. 2. Wählen Sie in der linken Navigation Elemente erkunden und wählen Sie die `TenantOnboarding` Tabelle aus. Hinweis: Dem Mandanten namen wird vorangest ellt`tenantcluster-` . Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen. 3. Stellen Sie sicher, dass ein neues Element mit den Mandantendetails erstellt wurde.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Stack-Erstellung für den neuen Mandanten.	Stellen Sie sicher, dass der neue Stack gemäß der CloudFormation Vorlage erfolgreich erstellt und mit Infrastruktur für den neu erstellten Mandanten bereitgestellt wurde. 1. Öffnen Sie die - CloudFormation Konsole. 2. Wählen Sie in der linken Navigation Stacks und überprüfen Sie, ob ein Stack mit dem Mandantennamen erfolgreich erstellt wurde. 3. Wählen Sie den neu erstellten Tenant-Stack und dann die Registerkarte Ressourcen aus. Notieren Sie sich die Alarmressource und die Amazon SQS-Ressource. 4. Öffnen Sie ein neues Terminal mit konfigurierten AWS-Anmeldeinformationen und zeigen Sie auf die richtige Region. Um einen Testalarm auszulösen, geben Sie den folgenden Code ein und ersetzen Sie durch `<alarm resource name>` den in Schritt 3	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	notierten Namen der Alarmressource.
	
	`aws cloudwatch set-alarm-state --alarm-name <alarm resource name> --state-value ALARM --state-reason 'Test setup'`
	
	Das folgende Beispiel zeigt den Code mit einem Alarmressourcennamen.
	
	`aws cloudwatch set-alarm-state --alarm-name tenantcluster-tenant123-alarm --state-value ALARM --state-reason 'Test setup'`
	
	5. Öffnen Sie die -Konsole und navigieren Sie zur Amazon SQS-Konsole. Wählen Sie den in Schritt 3 identifizierten Amazon SQS-Ressourcennamen aus. Folgen Sie den Anweisungen in der AWS-Dokumentation, um die Testnachricht zu empfangen und aus dem Alarm zu löschen, der in Schritt 4 ausgelöst wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie den Tenant-Stack.	Senden Sie die folgende curl-Anforderung, um den Tenant-Stack zu löschen.
	`curl -X DELETE <TenantOnboardingAPIEndpoint* from CDK Output>tenant/<Tenant Name from previous step>`
	Ändern Sie den Platzhalter `<TenantOnboardingAPIEndpoint* from CDK Output>` in den tatsächlichen Wert von AWS CDK und in den tatsächlichen Wert aus dem vorherigen Schritt `<Tenant Name from previous step>` zur Erstellung des Mandanten, wie im folgenden Beispiel gezeigt.
	`curl -X DELETE https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant/Tenant123`
	Das folgende Beispiel zeigt die Ausgabe.
	`{"message": "Tenant destroyed - 5/4/2022 7:14:48 AM"}`
		App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Stack-Lös chvorgang für den vorhanden en Mandanten.	Führen Sie die folgenden Schritte aus, um zu überprüfe n, ob der vorhandene Tenant-Stack gelöscht wurde: 1. Öffnen Sie die -Konsole und navigieren Sie zur - CloudFormation Konsole. 2. Stellen Sie in der linken Navigation sicher, dass sich der vorhandene Stack mit dem Mandanten namen nicht mehr in der Konsole befindet (wenn die CloudFormation Konsole so eingerichtet ist, dass nur aktive Stacks angezeigt werden) oder gerade gelöscht wird. Wenn sich der Stack nicht mehr in der CloudFormation Konsole befindet, verwenden Sie die Dropdown-Liste, um die Einstellung der Konsole von Aktiv in Gelöscht zu ändern, um den gelöschte n Stack anzuzeigen und zu überprüfen, ob der Stack erfolgreich gelöscht wurde.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zerstören Sie die Umgebung.	Bevor Sie den Stack bereinigen, stellen Sie Folgendes sicher: • Alle Datensätze in DynamoDB werden entweder über den vorherigen Löschvorgang des Mandanten oder über die DynamoDB-Konsole oder API entfernt. Jede Löschung von Tenant-Datensätzen initiiert die Bereinigung ihres AWS-CloudFormation Gegenstücks. • Alle mandantenbasierten AWS- CloudFormation Stacks werden in der AWS- CloudFormation Konsole bereinigt (falls die DynamoDB-Trigger-Bereinigungslogik fehlschlägt). Nachdem das Testen abgeschlossen ist, kann AWS CDK verwendet werden, um alle Stacks und zugehörigen Ressourcen zu löschen, indem der folgende Befehl ausgeführt wird.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk destroy --all;` Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie das Profil . Bestätigen Sie die Stack-Lös chaufforderung, um den Stack zu löschen.	
Bereinigen von Amazon CloudWatch Logs.	Der Stack-Löschvorgang bereinigt keine CloudWatch Protokolle (Protokollgruppen und Protokolle), die vom Stack generiert wurden. Bereinigen Sie die CloudWatc h Ressourcen manuell mithilfe der CloudWatch Konsole oder der API.	App-Entwickler, AWS DevOps, AWS-Administrator

Zugehörige Ressourcen

- AWS-CDK-.NET-Workshop
- Arbeiten mit dem AWS-CDK in C#
- CDK-.NET-Referenz

Zusätzliche Informationen

Technologie-Stack auf Steuerebene

Der in .NET geschriebene CDK-Code wird verwendet, um die Infrastruktur auf Steuerebene bereitzustellen, die aus den folgenden Ressourcen besteht:

1. API Gateway

Dient als REST-API-Einstiegspunkt für den Stack auf Steuerebene.

2. Lambda-Funktion für das Onboarding des Mandanten

   Diese Lambda-Funktion wird von API Gateway mit der Methode m initiiert.

   Eine POST-Methoden-API-Anforderung führt dazu, dass (`tenant name`, `tenant description`) in die DynamoDB-`Tenant Onboarding`Tabelle eingefügt wird.

   In diesem Codebeispiel wird der Mandantenname auch als Teil des Mandanten-Stack-Namens und der Namen der Ressourcen innerhalb dieses Stacks verwendet. Dies soll die Identifizierung dieser Ressourcen erleichtern. Dieser Mandantenname muss in der gesamten Einrichtung eindeutig sein, um Konflikte oder Fehler zu vermeiden. Die detaillierte Einrichtung der Eingabevalidierung wird in der Dokumentation zu IAM-Rollen und im Abschnitt Einschränkungen erläutert.

   Der Persistenzprozess für die DynamoDB-Tabelle ist nur erfolgreich, wenn der Mandantenname in keinem anderen Datensatz in der Tabelle verwendet wird.

   Der Mandantenname ist in diesem Fall der Partitionsschlüssel für diese Tabelle, da nur der Partitionsschlüssel als `PutItem` Bedingungsausdruck verwendet werden kann.

   Wenn der Mandantenname noch nie aufgezeichnet wurde, wird der Datensatz erfolgreich in der Tabelle gespeichert.

   Wenn der Mandantenname jedoch bereits von einem vorhandenen Datensatz in der Tabelle verwendet wird, schlägt der Vorgang fehl und löst eine DynamoDB-`ConditionalCheckFailedException`Ausnahme aus. Die Ausnahme wird verwendet, um eine Fehlermeldung (`HTTP BadRequest`) zurückzugeben, die angibt, dass der Mandantenname bereits vorhanden ist.

   Eine `DELETE` Methoden-API-Anforderung entfernt den Datensatz für einen bestimmten Mandantennamen aus der `Tenant Onboarding`-Tabelle.

   Das Löschen des DynamoDB-Datensatzes in diesem Beispiel ist auch dann erfolgreich, wenn der Datensatz nicht existiert.

   Wenn der Zieldatensatz vorhanden ist und gelöscht wird, wird ein DynamoDB-Stream-Datensatz erstellt. Andernfalls wird kein Downstream-Datensatz erstellt.

3. Onboarding von DynamoDB mit aktivierten Amazon-DynamoDB-Streams für Mandanten

Dadurch werden die Mandantenmetadateninformationen aufgezeichnet, und jedes Speichern oder Löschen von Datensätzen sendet einen Stream nachgelagert zur `Tenant Infrastructure` Lambda-Funktion.

4. Lambda-Funktion für die Tenant-Infrastruktur

   Diese Lambda-Funktion wird vom DynamoDB-Stream-Datensatz aus dem vorherigen Schritt initiiert. Wenn der Datensatz für ein `INSERT` Ereignis bestimmt ist, ruft er AWS auf, CloudFormation um eine neue Tenant-Infrastruktur mit der CloudFormation Vorlage zu erstellen, die in einem S3-Bucket gespeichert ist. Wenn der Datensatz für ist`REMOVE`, initiiert er das Löschen eines vorhandenen Stacks basierend auf dem -`Tenant Name`Feld des Stream-Datensatzes.

5. S3 bucket

   Dies dient zum Speichern der CloudFormation Vorlage.

6. IAM-Rollen für jede Lambda-Funktion und eine Servicerolle für CloudFormation

   Jede Lambda-Funktion verfügt über ihre eindeutige IAM-Rolle mit den geringsten Berechtigungen, um ihre Aufgabe zu erfüllen. Beispielsweise hat die `Tenant On-boarding` Lambda-Funktion Lese-/Schreibzugriff auf DynamoDB und die `Tenant Infrastructure` Lambda-Funktion kann nur den DynamoDB-Stream lesen.

   Für die Bereitstellung von Tenant-Stacks wird eine benutzerdefinierte CloudFormation Servicerolle erstellt. Diese Servicerolle enthält zusätzliche Berechtigungen für die CloudFormation Stack-Bereitstellung (z. B. den AWS KMS-Schlüssel). Dadurch werden Rollen zwischen Lambda und aufgeteilt CloudFormation , um alle Berechtigungen für eine einzelne Rolle (Infrastruktur-Lambda-Rolle) zu vermeiden.

   Berechtigungen, die leistungsstarke Aktionen ermöglichen (z. B. das Erstellen und Löschen von CloudFormation Stacks), sind gesperrt und nur für Ressourcen zulässig, die mit beginnen`tenantcluster-`. Die Ausnahme ist AWS KMS aufgrund seiner Ressourcennamenskonvention. Dem aufgenommenen Mandantennamen aus der API werden `tenantcluster-` zusammen mit anderen Validierungsprüfungen vorangestellt (alphanumerisch nur mit Bindestrichen und auf weniger als 30 Zeichen begrenzt, um in die meisten AWS-Ressourcennamen zu passen). Dadurch wird sichergestellt, dass der Mandantenname nicht versehentlich zu einer Unterbrechung der Kerninfrastruktur-Stacks oder -Ressourcen führt.

Tenant-Technologie-Stack

Eine CloudFormation Vorlage wird im S3-Bucket gespeichert. Die Vorlage stellt den mandantenspezifischen AWS KMS-Schlüssel, einen CloudWatch Alarm, ein SNS-Thema, eine SQS-Warteschlange und eine SQS-Richtlinie bereit.

Der AWS KMS-Schlüssel wird für die Datenverschlüsselung durch Amazon SNS und Amazon SQS für ihre Nachrichten verwendet. Die Sicherheitsmethoden für AwsSolutions-SNS2 und AwsSolutions-SQS2 empfehlen, Amazon SNS und Amazon SQS mit Verschlüsselung einzurichten. CloudWatch Alarme funktionieren jedoch nicht mit Amazon SNS, wenn Sie einen von AWS verwalteten Schlüssel verwenden, daher müssen Sie in diesem Fall einen vom Kunden verwalteten Schlüssel verwenden. Weitere Informationen finden Sie im AWS Knowledge Center .

Die SQS-Richtlinie wird in der Amazon SQS-Warteschlange verwendet, damit das erstellte SNS-Thema die Nachricht an die Warteschlange senden kann. Ohne die SQS-Richtlinie wird der Zugriff verweigert. Weitere Informationen finden Sie in der Amazon SNS-Dokumentation.

Zerlegen von Monolithen in Microservices mithilfe von CQRS und Event Sourcing

Erstellt von Bololfo Jr. Cerrada (AWS), Dmitry G (AWS) und Tabby Ward (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Monolith-CRUD-Modell	Ziel: Microservices
R-Typ: Neuarchitektur	Workload: Open-Source	Technologien: Modernisierung; Messaging und Kommunikation; Serverless
AWS-Services: Amazon DynamoDB ;AWS Lambda ;Amazon SNS		

Übersicht

Dieses Muster kombiniert zwei Muster und verwendet sowohl das CQRS-Muster (Command Query Responsibility Separatention) als auch das Ereignis-Sourcing-Muster. Das CQRS-Muster trennt die Verantwortlichkeiten der Befehls- und Abfragemodelle. Das Ereignis-Sourcing-Muster nutzt die asynchrone ereignisgesteuerte Kommunikation, um das allgemeine Benutzererlebnis zu verbessern.

Sie können CQRS- und Amazon Web Services (AWS)-Services verwenden, um jedes Datenmodell unabhängig zu verwalten und zu skalieren und gleichzeitig Ihre monolithe Anwendung in eine Microservices-Architektur umzugestalten. Anschließend können Sie das Ereignis-Sourcing-Muster verwenden, um Daten aus der Befehlsdatenbank mit der Abfragedatenbank zu synchronisieren.

Dieses Muster verwendet Beispielcode, der eine Lösungsdatei (*.sln) enthält, die Sie mit der neuesten Version von Visual Studio öffnen können. Das Beispiel enthält Bol-API-Code, um zu demonstrieren, wie CQRS und Event Sourcing in serverlosen und herkömmlichen oder On-Premises-Anwendungen von AWS funktionieren.

Weitere Informationen zu CQRS und Ereignis-Sourcing finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon CloudWatch
- Amazon-DynamoDB-Tabellen
- Amazon DynamoDB Streams
- AWS Identity and Access Management (IAM)-Zugriffsschlüssel und geheimer Schlüssel; weitere Informationen finden Sie im Video im Abschnitt Verwandte Ressourcen
- AWS Lambda
- Vertrautheit mit Visual Studio
- Vertrautheit mit AWS Toolkit for Visual Studio; weitere Informationen finden Sie im Demo-Video zum AWS Toolkit for Visual Studio im Abschnitt Verwandte Ressourcen

Produktversionen

- Visual Studio 2019 Community Edition .
- AWS Toolkit for Visual Studio 2019.
- .NET Core 3.1. Diese Komponente ist eine Option in der Visual Studio-Installation. Um .NET Core während der Installation einzuschließen, wählen Sie plattformübergreifende -Entwicklung aus.

Einschränkungen

- Der Beispielcode für eine herkömmliche On-Premises-Anwendung (ASP.NET Core Web API und Datenzugriffsobjekte) enthält keine Datenbank. Es wird jedoch mit dem `CustomerData` In-Memory-Objekt geliefert, das als Mock-Datenbank fungiert. Der bereitgestellte Code reicht aus, damit Sie das Muster testen können.

Architektur

Quelltechnologie-Stack

- ASP.NET Core Web API-Projekt
- IIS-Webserver

- Datenzugriffsobjekt
- CRUD-Modell

Quellarchitektur

In der Quellarchitektur enthält das CRUD-Modell sowohl Befehls- als auch Abfrageschnittstellen in einer Anwendung. Beispielcode finden Sie unter `CustomerDAO.cs` (angefügt).

Zieltechnologie-Stack

- Amazon DynamoDB
- Amazon DynamoDB Streams
- AWS Lambda
- (Optional) Amazon API Gateway
- (Optional) Amazon Simple Notification Service (Amazon SNS)

Zielarchitektur

In der Zielarchitektur werden die Befehls- und Abfrageschnittstellen getrennt. Die im folgenden Diagramm gezeigte Architektur kann mit API Gateway und Amazon SNS erweitert werden. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

1. Befehls-Lambda-Funktionen führen Schreibvorgänge wie Erstellen, Aktualisieren oder Löschen in der Datenbank aus.
2. Abfragen von Lambda-Funktionen führen Leseoperationen wie Abrufen oder Auswählen in der Datenbank aus.
3. Diese Lambda-Funktion verarbeitet die DynamoDB-Streams aus der Befehlsdatenbank und aktualisiert die Abfragedatenbank für die Änderungen.

Tools

Tools

- Amazon DynamoDB – Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der eine schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Amazon DynamoDB Streams – DynamoDB Streams erfasst eine zeitlich geordnete Abfolge von Änderungen auf Elementebene in jeder DynamoDB-Tabelle. Anschließend werden diese Informationen bis zu 24 Stunden lang in einem Protokoll gespeichert. Die Verschlüsselung ruhender Daten verschlüsselt die Daten in DynamoDB Streams.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- AWS-Managementkonsole – Die AWS-Managementkonsole ist eine Webanwendung, die eine breite Sammlung von Servicekonsolen für die Verwaltung von AWS-Services umfasst.
- Visual Studio 2019 Community Edition – Visual Studio 2019 ist eine integrierte Entwicklungsumgebung (IDE). Die Community Edition ist für Open-Source-Mitwirkende kostenlos. In diesem Muster verwenden Sie Visual Studio 2019 Community Edition, um Beispielcode zu öffnen, zu kompilieren und auszuführen. Nur zur Anzeige können Sie einen beliebigen Texteditor oder Visual Studio Code verwenden.
- AWS Toolkit for Visual Studio – Das AWS Toolkit for Visual Studio ist ein Plugin für die Visual Studio IDE. Das AWS Toolkit for Visual Studio erleichtert Ihnen das Entwickeln, Debuggen und Bereitstellen von .NET-Anwendungen, die AWS-Services nutzen.

Code

Der Beispielcode ist angehängt. Anweisungen zur Bereitstellung des Beispielcodes finden Sie im Abschnitt Telefonie.

Polen

Öffnen und entwickeln Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie die Lösung.	1. Laden Sie den Beispiel-Quellcode (`CQRS-ES`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Code.zip`) aus dem Abschnitt Anhänge herunter und extrahieren Sie die Dateien. 2. Wählen Sie in der Visual Studio-IDE Datei , Öffnen , Projektlösung aus und navigieren Sie zu dem Ordner, in den Sie den Quellcode extrahiert haben. 3. Wählen Sie AWS.APG.CQRSES.sln und dann Öffnen aus. Die gesamte Lösung wird in Visual Studio geladen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lösung.	Öffnen Sie das Kontextmenü (rechte Maustaste) für die Lösung und wählen Sie dann Lösung erstellen aus. Dadurch werden alle Projekte in der Lösung erstellt und kompiliert. Es sollte erfolgreich kompiliert werden. Visual Studio Solution Explorer sollte die Verzeichnisstruktur anzeigen. • `CQRS On-Premises Code Sample` enthält ein Beispiel für die Verwendung von CQRS On-Premises. • `CQRS AWS Serverless` enthält den gesamten CQRS- und Ereignis-Sourcing-Beispielcode mithilfe von AWS Serverless-Services.	App-Developer

Erstellen der DynamoDB-Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie Anmeldeinformationen an.	Wenn Sie noch keinen Zugriffsschlüssel haben, sehen Sie sich das Video im Abschnitt Verwandte Ressourcen an.	App-Entwickler, Dateningenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Erweitern Sie im Lösungs-Explorer CQRS AWS Serverless und erweitern Sie dann den Ordner Lösung erstellen. 2. Erweitern Sie das Projekt AwS.APG.CQRSES.Build und zeigen Sie die `Program.cs` Datei an. 3. Scrollen Sie zum Anfang von `Program.cs` und suchen Sie nach `Program()` . 4. Ersetzen Sie `YOUR ACCESS KEY` durch Ihren Kontozugriffsschlüssel und ersetzen Sie durch Ihren `YOUR SECRET KEY`geheimen Kontoschlüssel. Beachten Sie, dass Sie in einer Produktionsumgebung Ihre Schlüssel nicht fest codieren würden. Stattdessen könnten Sie AWS Secrets Manager verwenden, um die Anmeldeinformationen zu speichern und abzurufen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Projekt.	Um das Projekt zu erstellen , öffnen Sie das Kontextme nü (rechte Maustaste) für das Projekt AwS.APG.C QRSES.Build und wählen Sie dann Erstellen aus.	App-Entwickler, Dateninge nieur, DBA
Erstellen Sie die Tabellen und füllen Sie sie aus.	Um die Tabellen zu erstellen und sie mit Seed-Date n zu füllen, öffnen Sie das Kontextmenü (rechte Maustaste) für das Projekt AwS.APG.CQRSES.Build und wählen Sie dann Debuggen, Neue Instance starten aus.	App-Entwickler, Dateninge nieur, DBA
Überprüfen Sie die Tabellene rstellung und die Daten.	Navigieren Sie zur Überprüfu ng zu AWS Explorer und erweitern Sie Amazon DynamoDB . Es sollte die Tabellen anzeigen. Öffnen Sie jede Tabelle, um die Beispield aten anzuzeigen.	App-Entwickler, Dateninge nieur, DBA

Ausführen lokaler Tests

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das CQRS-Proj ekt.	1. Öffnen Sie die Lösung und navigieren Sie zum Lösungsordner CQRS AWS Services/CQRS/Tests. 2. Öffnen Sie im Projekt AWS.APG.CQRSES.CQR	App-Entwickler, Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SLambda.Tests BaseFunct ionTest.cs und ersetzen Sie AccessKeyund durch SecretKey die von Ihnen erstellten IAM-Schlüssel. 3. Speichern Sie die Änderungen. 4. Um das Testprojekt zu kompilieren und zu erstellen , öffnen Sie das Kontextme nü (rechte Maustaste) für das Projekt und wählen Sie dann Erstellen aus.	
Erstellen Sie das Event-Sou rcing-Projekt.	1. Navigieren Sie zum Lösungsordner CQRS AWS Services/Event Source/Te sts. 2. In AWS.APG.C QRSESEventSourceLa mbda.Testet das Projekt, öffnen Sie BaseFunct ionTest.cs und ersetzen Sie AccessKeyund SecretKey durch die von Ihnen erstellten IAM-Schlüssel. 3. Speichern Sie die Änderungen. 4. Um das Testprojekt zu kompilieren und zu erstellen , öffnen Sie das Kontextme nü (rechte Maustaste) für das Projekt und wählen Sie dann Erstellen aus.	App-Entwickler, Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Tests aus.	Um alle Tests auszuführen, wählen Sie Anzeigen, Test-Explorer und dann Alle Tests in Ansicht ausführen aus. Alle Tests sollten erfolgreich sein, was durch ein grünes Häkchensymbol angezeigt wird.	App-Entwickler, Testingenieur

Veröffentlichen der CQRS-Lambda-Funktionen in AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Veröffentlichen Sie die erste Lambda-Funktion.	1. Öffnen Sie im Lösungs-Explorer das Kontextmenü (rechte Maustaste) für das AWS.APG.CQRSES.CommandCreateLambda project und wählen Sie dann In AWS Lambda veröffentlichen aus. 2. Wählen Sie das Profil aus, das Sie verwenden möchten, und die AWS-Region, in der Sie die Lambda-Funktion bereitstellen möchten, sowie den Funktionsnamen. 3. Behalten Sie für die verbleibenden Felder die Standardwerte bei und wählen Sie Weiter aus.	App-Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie in der Dropdownliste Rollenname die Option ausAWSLambda FullAccess. 5. Um Ihre Kontoschlüssel bereitzustellen, wählen Sie Hinzufügen und geben Sie `AcessKey` als Variable und Ihren Zugriffsschlüssel als Wert ein. Wählen Sie dann erneut Hinzufügen und geben Sie `SecretKey` als Variable und Ihren geheimen Schlüssel als Wert ein. 6. Behalten Sie für die verbleibenden Felder die Standardwerte bei und wählen Sie Hochladen aus. Nachdem die Lambda-Te stfunktion hochgeladen wurde, wird sie automatisch in Visual Studio angezeigt. 7. Wiederholen Sie die Schritte 1-6 für die folgenden Projekte: • AWS.APG.C QRSES.CommandDelet eLambda • AWS.APG.C QRSES.CommandUpdat eLambda	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• AWS.APG.CQRSES.CommandAddRewardLambda • AWS.APG.CQRSES.CommandRedeemRewardLambda • AWS.APG.CQRSES.QueryCustomerListLambda • AWS.APG.CQRSES.QueryRewqardLambda	
Überprüfen Sie den Funktions-Upload.	(Optional) Sie können überprüfen, ob die Funktion erfolgreich geladen wurde, indem Sie zu AWS Explorer navigieren und AWS Lambda erweitern. Um das Testfenster zu öffnen, wählen Sie die Lambda-Funktion aus (doppelter Klick).	App-Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lambda-Funktion.	1. Geben Sie die Anforderungsdaten ein oder kopieren Sie ein Beispiel für Anforderungsdaten aus Testdaten im Abschnitt Zusätzliche Informationen. Stellen Sie sicher, dass Sie Daten auswählen, die für die Funktion bestimmt sind, die Sie testen. 2. Um den Test durchzuführen, wählen Sie Invoke (Aufrufen) aus. Die Antwort und alle Fehler werden im Textfeld Antwort angezeigt, und Protokolle werden im Textfeld Protokolle oder in CloudWatch Protokollen angezeigt. 3. Um die Daten zu überprüfen, wählen Sie in AWS Explorer die DynamoDB-Tabelle aus (doppelter Klick). Alle CQRS-Lambda-Projekte finden Sie unter den Lösungsordnern `CQRS AWS Serverless\CQRS\Command Microservice` und `CQRS AWS Serverless\CQRS\Command Microservice` . Informationen zum Lösungsverzeichnis	App-Entwickler, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und zu Projekten finden Sie unter Quellcodeverzeichnis im Abschnitt Zusätzliche Informationen.	
Veröffentlichen Sie die verbleibenden Funktionen.	Wiederholen Sie die vorherigen Schritte für die folgenden Projekte: • AWS.APG.CQRSES.CommandDeleteLambda • AWS.APG.CQRSES.CommandUpdateLambda • AWS.APG.CQRSES.CommandAddRewardLambda • AWS.APG.CQRSES.CommandRedeemRewardLambda • AWS.APG.CQRSES.QueryCustomerListLambda • AWS.APG.CQRSES.QueryRewqardLambda	App-Entwickler, DevOps Techniker

Einrichten der Lambda-Funktion als Ereignis-Listener

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Veröffentlichen Sie die Lambda-Ereignishandler Customer und Bol.	Um jeden Ereignis-Handler zu veröffentlichen, führen Sie die Schritte im vorherigen Epos aus. Die Projekte befinden sich unter den `CQRS AWS`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Serverless\Event Source\Reward Event` Lösungsordnern `CQRS AWS Serverless\Event Source\Customer Event` und . Weitere Informationen finden Sie unter Quellcode verzeichnis im Abschnitt Zusätzliche Informationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den Ereignis-Sourcing-Lambda-Ereignis-Listener an.	1. Melden Sie sich bei der AWS-Managementkonsole mit demselben Konto an, das Sie bei der Veröffentlichung der Lambda-Projekte verwenden. 2. Wählen Sie für die Region USA Ost 1 oder die Region aus, in der Sie die Lambda-Funktionen im vorherigen Epi bereitgestellt haben. 3. Navigieren Sie zum Lambda-Service. 4. Wählen Sie die `EventSourceCustomer` Lambda-Funktion aus. 5. Wählen Sie Add Trigger aus. 6. Wählen Sie in der Dropdownliste Auslöserkonfiguration die Option DynamoDB aus. 7. Wählen Sie in der Dropdown-Liste DynamoDB-Tabelle die Option auscqrses-customer-cmd. 8. Wählen Sie in der Dropdownliste Startposition die Option Horizont trimmen aus. Horizont trimmen bedeutet, dass der DynamoDB-Auslöser	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	am letzten (unrimierten) Stream-Datensatz beginnt zu lesen, der der älteste Datensatz im Shard ist. 9. Aktivieren Sie das Kontrollk ästchen Auslöser aktivieren. 10. Behalten Sie für die verbleibenden Felder die Standardwerte bei und wählen Sie Hinzufügen aus. Nachdem der Listener erfolgreich an die DynamoDB-Tabelle angefügt wurde, wird er auf der Lambda-De signerseite angezeigt.	
Veröffentlichen Sie die EventSourceReward Lambda-Funktion und fügen Sie sie an.	Um die `EventSour ceReward` Lambda-Fu nktion zu veröffentlichen und anzufügen, wiederhol en Sie die Schritte in den beiden vorherigen Artikeln und wählen Sie cqrses-reward-cmd aus der Dropdown-Liste DynamoDB-Tabelle aus.	App-Developer

Testen und Validieren der DynamoDB-Streams und des Lambda-Auslösers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Stream und den Lambda-Auslöser.	1. Navigieren Sie in Visual Studio zu AWS Explorer.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erweitern Sie AWS Lambda und wählen Sie die CommandRedeemRewardFunktion aus (doppelter Klick). Im sich öffnenden Funktionsfenster können Sie die Funktion testen. 3. Geben Sie im Textfeld Anforderung die Anforderungsdaten im JSON-Format (JavaScript Object Notation) ein. Eine Beispielanforderung finden Sie unter Testdaten im Abschnitt Zusätzliche Informationen. 4. Wählen Sie aufrufen aus.	
Validieren Sie mithilfe der DynamodDB-Berechtigungsabfragetabelle.	1. Öffnen Sie die -cqrses-reward-queryTabelle. 2. Überprüfen Sie die Punkte des Kunden, der die Belohnung eingetauscht hat. Die eingelösten Punkte sollten vom aggregierten Gesamtpunkt des Kunden abgezogen werden.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie mithilfe von - CloudWatch Protokollen.	1. Navigieren Sie zu CloudWatch und wählen Sie Protokollgruppen aus. 2. Die /aws/lambda/EventSourceRewardlog-Gruppe enthält die Protokolle für den `EventSourceReward` Auslöser. Alle Lambda-Aufrufe werden protokolliert, einschließlich der Nachrichten, die Sie in `context.Logger.LogLine` und `Console.WriteLine` im Lambda-Code platziert haben.	App-Developer
Validieren Sie den EventSourceCustomer Auslöser.	Wiederholen Sie zum Validieren des `EventSourceCustomer` Auslösers die Schritte in diesem Epics unter Verwendung der jeweiligen Kundentabelle und CloudWatch Protokolle des `EventSourceCustomer` Auslösers.	App-Developer

Zugehörige Ressourcen

Referenzen

- Downloads der Community Edition von Visual Studio 2019
- AWS Toolkit for Visual Studio herunterladen
- AWS Toolkit for Visual Studio-Benutzerhandbuch
- Serverless auf AWS

- DynamoDB-Anwendungsfälle und Designmuster
- CQRS für Italien Fowler
- Ereignisbereitstellung in Italien Fowler

Videos

- AWS Toolkit for Visual Studio-Demo
- Wie erstelle ich eine Zugriffsschlüssel-ID für einen neuen IAM-Benutzer?

Zusätzliche Informationen

CQRS und Ereignis-Sourcing

CQRS

Das CQRS-Muster trennt ein einzelnes konzeptionelles Operationsmodell, z. B. ein einzelnes CRUD-Modell (Erstellen, Lesen, Aktualisieren, Löschen) für Datenzugriffsobjekte, in Befehls- und Abfrageoperationsmodelle. Das Befehlsmodell bezieht sich auf jede Operation, z. B. Erstellen, Aktualisieren oder Löschen, die den Status ändert. Das Abfragemodell bezieht sich auf jede Operation, die einen Wert zurückgibt.

1. Das CRUD-Modell des Kunden umfasst die folgenden Schnittstellen:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`

Wenn Ihre Anforderungen komplexer werden, können Sie von diesem Einzelmodell-Ansatz ausgehen. CQRS verwendet ein Befehlsmodell und ein Abfragemodell, um die Verantwortung für

das Schreiben und Lesen von Daten zu trennen. Auf diese Weise können die Daten unabhängig voneinander verwaltet werden. Bei einer klare Trennung der Verantwortlichkeiten wirken sich Verbesserungen an jedem Modell nicht auf das andere aus. Diese Trennung verbessert Wartung und Leistung und reduziert die Komplexität der Anwendung, wenn sie wächst.

1. Schnittstellen im Customer Command-Modell:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
2. Schnittstellen im Kundenabfragemodell:
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`
   - `GetMonthlyStatement()`

Beispielcode finden Sie unter Quellcodeverzeichnis .

Das CQRS-Muster entkoppelt dann die Datenbank. Diese Entkopplung führt zu der Gesamtheit der einzelnen Services, was die wichtigste Einheit der Microservice-Architektur ist.

Mit CQRS in der AWS Cloud können Sie jeden Service weiter optimieren. Sie können beispielsweise verschiedene Recheneinstellungen festlegen oder zwischen einem Serverless- oder einem Container-basierten Microservice wählen. Sie können Ihr On-Premises-Caching durch Amazon ersetzen ElastiCache. Wenn Sie über ein On-Premises-Nachrichten zum Veröffentlichen/Abonnement verfügen, können Sie es durch Amazon Simple Notification Service (Amazon SNS) ersetzen. Darüber hinaus können Sie die - pay-as-you-go Preise und die breite Palette von AWS-Services nutzen, die Sie nur für das zahlen, was Sie tatsächlich nutzen.

CQRS bietet die folgenden Vorteile:

- Unabhängige Skalierung – Bei jedem Modell kann seine Skalierungsstrategie an die Anforderungen und den Bedarf des Services angepasst werden. Ähnlich wie bei Hochleistungsanwendungen kann das Modell durch die Trennung von Lese- und Schreibvorgängen unabhängig skaliert werden, um jeden Bedarf zu erfüllen. Sie können auch Rechenressourcen hinzufügen oder reduzieren, um den Skalierbarkeitsbedarf eines Modells zu bewältigen, ohne das andere zu beeinträchtigen.
- Unabhängige Wartung – Die Trennung von Abfrage- und Befehlsmodellen verbessert die Wartungsbarkeit der Modelle. Sie können Codeänderungen und -verbesserungen an einem Modell vornehmen, ohne das andere zu beeinträchtigen.
- Sicherheit – Es ist einfacher, die Berechtigungen und Richtlinien anzuwenden, um Modelle zum Lesen und Schreiben zu trennen.
- Optimierte Lesevorgänge – Sie können ein Schema definieren, das für Abfragen optimiert ist. Sie können beispielsweise ein Schema für die aggregierten Daten und ein separates Schema für die Faktentabellen definieren.
- Integration – CQRS eignet sich gut für ereignisbasierte Programmiermodelle.
- Verwaltete Komplexität – Die Trennung in Abfrage- und Befehlsmodelle eignet sich für komplexe Domains.

Beachten Sie bei der Verwendung von CQRS die folgenden Einschränkungen:

- Das CQRS-Muster gilt nur für einen bestimmten Teil einer Anwendung und nicht für die gesamte Anwendung. Wenn sie in einer Domain implementiert ist, die nicht dem Muster entspricht, kann sie die Produktivität verringern, das Risiko erhöhen und Komplexität mit sich bringen.
- Das Muster eignet sich am besten für häufig verwendete Modelle mit unausgewogenen Lese- und Schreibvorgängen.
- Bei leseintensiven Anwendungen wie großen Berichten, deren Verarbeitung einige Zeit in Anspruch nimmt, bietet Ihnen CQRS die Möglichkeit, die richtige Datenbank auszuwählen und ein Schema zum Speichern Ihrer aggregierten Daten zu erstellen. Dies verbessert die Reaktionszeit beim Lesen und Anzeigen des Berichts, indem die Berichtsdaten nur einmal verarbeitet und in der aggregierten Tabelle abgelegt werden.
- Für die schreibintensiven Anwendungen können Sie die Datenbank für Schreibvorgänge konfigurieren und dem Befehls-Microservice erlauben, unabhängig zu skalieren, wenn der Schreibbedarf steigt. Beispiele finden Sie unter `AWS.APG.CQRSES.CommandRedeemRewardLambda` und `AWS.APG.CQRSES.CommandAddRewardLambda` Microservices.

Ereignis-Sourcing

Der nächste Schritt besteht darin, die Ereignis-Sourcing zu verwenden, um die Abfragedatenbank zu synchronisieren, wenn ein Befehl ausgeführt wird. Betrachten Sie beispielsweise die folgenden Ereignisse:

- Es wird ein Kundenbindungspunkt hinzugefügt, bei dem die Gesamtzahl der oder aggregierten Belohnungspunkte des Kunden in der Abfragedatenbank aktualisiert werden müssen.
- Der Nachname eines Kunden wird in der Befehlsdatenbank aktualisiert, was erfordert, dass die Ersatzkundeninformationen in der Abfragedatenbank aktualisiert werden.

Im herkömmlichen CRUD-Modell stellen Sie die Konsistenz der Daten sicher, indem Sie die Daten sperren, bis eine Transaktion abgeschlossen ist. Bei der Ereignis-Sourcing werden die Daten synchronisiert, indem eine Reihe von Ereignissen veröffentlicht wird, die von einem Subscriber verwendet werden, um seine jeweiligen Daten zu aktualisieren.

Das Ereignis-Sourcing-Muster stellt sicher und zeichnet eine vollständige Reihe von Aktionen auf, die für die Daten durchgeführt wurden, und veröffentlicht sie über eine Abfolge von Ereignissen. Diese Ereignisse stellen eine Reihe von Änderungen an den Daten dar, die Abonnenten dieses Ereignisses verarbeiten müssen, um ihren Datensatz auf dem neuesten Stand zu halten. Diese Ereignisse werden vom Abonnenten verarbeitet und synchronisieren die Daten in der Datenbank des Abonnenten. In diesem Fall ist dies die Abfragedatenbank.

Das folgende Diagramm zeigt die Ereignis-Sourcing, die mit CQRS in AWS verwendet wird.

1. Befehls-Lambda-Funktionen führen Schreibvorgänge wie Erstellen, Aktualisieren oder Löschen in der Datenbank aus.
2. Abfragen von Lambda-Funktionen führen Leseoperationen wie Abrufen oder Auswählen in der Datenbank aus.
3. Diese Lambda-Funktion verarbeitet die DynamoDB-Streams aus der Befehlsdatenbank und aktualisiert die Abfragedatenbank für die Änderungen. Sie können diese Funktion auch verwenden, um eine Nachricht in Amazon SNS zu veröffentlichen, damit ihre Abonnenten die Daten verarbeiten können.
4. (Optional) Der Lambda-Ereignisabonnent verarbeitet die von Amazon SNS veröffentlichte Nachricht und aktualisiert die Abfragedatenbank.
5. (Optional) Amazon SNS sendet eine E-Mail-Benachrichtigung über den Schreibvorgang.

In AWS kann die Abfragedatenbank von DynamoDB Streams synchronisiert werden. DynamoDB erfasst eine zeitlich geordnete Abfolge von Änderungen auf Elementebene in einer DynamobDB-Tabelle nahezu in Echtzeit und speichert die Informationen innerhalb von 24 Stunden dauerhaft.

Durch die Aktivierung von DynamoDB Streams kann die Datenbank eine Abfolge von Ereignissen veröffentlichen, die das Ereignis-Sourcing-Muster ermöglicht. Das Ereignis-Sourcing-Muster fügt den Ereignisabonnenten hinzu. Die Ereignisabonnentenanwendung verarbeitet das Ereignis je nach Verantwortung des Abonnenten. Im vorherigen Diagramm überträgt der Ereignis-Subscriber die Änderungen an die Abfrage-DynamoDB-Datenbank, um die Daten synchronisiert zu halten. Die Verwendung von Amazon SNS , dem Message Broker und der Ereignis-Subscriber-Anwendung hält die Architektur entkoppelt.

Das Event-Sourcing bietet die folgenden Vorteile:

- Konsistenz für Transaktionsdaten
- Ein zuverlässiger Audit-Trail und der Verlauf der Aktionen, die zur Überwachung der in den Daten durchgeführten Aktionen verwendet werden können
- Ermöglicht verteilten Anwendungen wie Microservices, ihre Daten in der gesamten Umgebung zu synchronisieren
- Zuverlässige Veröffentlichung von Ereignissen, wenn sich der Status ändert
- Rekonstruieren oder Wiedergeben vergangener Status
- Gekoppelte Entitäten, die Ereignisse zur Migration von einer monolithischen Anwendung zu Microservices austauschen
- Reduzierung von Konflikten, die durch gleichzeitige Updates verursacht werden; Ereignis-Sourcing vermeidet die Notwendigkeit, Objekte direkt im Datenspeicher zu aktualisieren
- Flexibilität und Erweiterbarkeit durch Entkopplung der Aufgabe und des Ereignisses
- Externe Systemaktualisierungen
- Verwaltung mehrerer Aufgaben in einem einzigen Ereignis

Beachten Sie bei der Verwendung von Event Sourcing die folgenden Einschränkungen:

- Da es eine gewisse Verzögerung beim Aktualisieren von Daten zwischen den Quell-Subscriber-Datenbanken gibt, besteht die einzige Möglichkeit, eine Änderung rückgängig zu machen, darin, dem Ereignisspeicher ein Ausgleichsereignis hinzuzufügen.
- Die Implementierung von Ereignis-Sourcing hat seit seinem anderen Programmierstil eine Lernkurve.

Testdaten

Verwenden Sie die folgenden Testdaten, um die Lambda-Funktion nach erfolgreicher Bereitstellung zu testen.

CommandCreate Kunde

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Done",  "CompanyName":"AnyCompany",
 "Address": "USA",  "VIP":true }
```

CommandUpdate Kunde

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Doe",  "CompanyName":"Example Corp.",
 "Address": "Seattle, USA",  "VIP":true }
```

CommandDelete Kunde

Geben Sie die Kunden-ID als Anforderungsdaten ein. Wenn die Kunden-ID beispielsweise 151 lautet, geben Sie 151 als Anforderungsdaten ein.

```
151
```

QueryCustomerList

Dies ist leer. Wenn es aufgerufen wird, werden alle Kunden zurückgegeben.

CommandAddReward

Dadurch werden Kunden mit der ID 1 (Richard) 40 Punkte hinzugefügt.

```
{
  "Id":10101,
  "CustomerId":1,
  "Points":40
}
```

CommandRedeemReward

Dadurch werden 15 Punkte für den Kunden mit der ID 1 (Richard) abgezogen.

```
{
  "Id":10110,
```

```
  "CustomerId":1,
  "Points":15
}
```

QueryReward

Geben Sie die ID des Kunden ein. Geben Sie beispielsweise 1 für Richard, 2 für Arnav und 3 für Shirley ein.

```
2
```

Quellcodeverzeichnis

Verwenden Sie die folgende Tabelle als Leitfaden für die Verzeichnisstruktur der Visual Studio-Lösung.

CQRS On-Premises-Code-Beispiellösungsverzeichnis

CRUD-Modell des Kunden

CQRS On-Premises-Codebeispiel\CRUD Model\AWS.APG.CQRSES.DAL-Projekt

CQRS-Version des Kunden-CRUD-Modells

- Kundenbefehl: `CQRS On-Premises Code Sample\CQRS Model\Command Microservice \AWS.APG.CQRSES.Command`Projekt
- Kundenabfrage: `CQRS On-Premises Code Sample\CQRS Model\Query Microservice \AWS.APG.CQRSES.Query` Projekt

Befehls- und Abfrage-Microservices

Der Command Microservice befindet sich im Lösungsordner `CQRS On-Premises Code Sample \CQRS Model\Command Microservice`:

- `AWS.APG.CQRSES.CommandMicroservice` Das ASP.NET Core API-Projekt fungiert als Eintrittspunkt, an dem Verbraucher mit dem Service interagieren.
- `AWS.APG.CQRSES.Command` Das .NET Core-Projekt ist ein Objekt, das befehlsbezogene Objekte und Schnittstellen hostet.

Der Abfrage-Microservice befindet sich im Lösungsordner `CQRS On-Premises Code Sample \CQRS Model\Query Microservice`:

- `AWS.APG.CQRSES.QueryMicroservice` Das ASP.NET Core API-Projekt fungiert als Eintrittspunkt, an dem Verbraucher mit dem Service interagieren.
- `AWS.APG.CQRSES.Query` Das .NET Core-Projekt ist ein Objekt, das abfragebezogene Objekte und Schnittstellen hostet.

CQRS-AWS Serverless-Codelösungsverzeichnis

Dieser Code ist die AWS-Version des On-Premises-Codes unter Verwendung von AWS Serverless-Services.

In C# .NET Core wird jede Lambda-Funktion durch ein .NET Core-Projekt dargestellt. Im Beispielcode dieses Musters gibt es ein separates Projekt für jede Schnittstelle in den Befehls- und Abfragemodellen.

CQRS unter Verwendung von AWS-Services

Sie finden das Stammlösungsverzeichnis für CQRS mithilfe von AWS Serverless-Services im `CQRS AWS Serverless\CQRS`Ordner . Das Beispiel umfasst zwei Modelle: Kunde und Bol.

Die Lambda-Funktionen für Customer und Bol befinden sich unter den `CQRS\Command Microservice\Reward` Ordnern `CQRS\Command Microservice\Customer` und . Sie enthalten die folgenden Lambda-Projekte:

- Kundenbefehl: `CommandCreateLambda`, `CommandDeleteLambda`, und `CommandUpdateLambda`
- -Befehl: `CommandAddRewardLambda` und `CommandRedeemRewardLambda`

Die Abfrage-Lambda-Funktionen für Customer und Bol finden Sie unter den `CQRS \QueryMicroservice\Reward`Ordnern `CQRS\Query Microservice\Customer` und . Sie enthalten die Lambda-Projekte `QueryCustomerListLambda` und `QueryRewardLambda` .

CQRS-Testprojekt

Das Testprojekt befindet sich im `CQRS\Tests` Ordner . Dieses Projekt enthält ein Testskript zur Automatisierung des Tests der CQRS-Lambda-Funktionen.

Ereignis-Sourcing mit AWS-Services

Die folgenden Lambda-Ereignis-Handler werden von den DynamoDB-Streams „Customer“ und „Admin“ initiiert, um die Daten in Abfragetabellen zu verarbeiten und zu synchronisieren.

- Die `EventSourceCustomer` Lambda-Funktion ist dem DynamoDB-Stream der Kundentabelle (`cqrses-customer-cmd`) zugeordnet.
- Die `EventSourceReward` Lambda-Funktion ist dem DynamoDB-Stream der Bol-Tabelle (`cqrses-reward-cmd`) zugeordnet.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Mehr Muster

- ???
- Automatisieren des Hinzufügens oder Aktualisierens von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- Automatisieren Sie die Identifizierung und Planung von Migrationsstrategien mithilfe von AppScore
- Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mit AWS CDK
- Sichern und Archivieren von Mainframe-Daten in Amazon S3 mithilfe von AMI-Cloud-Daten
- Verketten von AWS-Services mithilfe eines Serverless-Ansatzes
- Containerisieren Sie Mainframe-Workloads, die von Clari Age modernisiert wurden
- Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertieren von Mainframe-Datendateien mit komplexen Datensatzlayouts mit Micro Focus
- ???
- Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale EC2-Instances bereit mit CodePipeline
- Bereitstellen und Debuggen von Amazon-EKS-Clustern
- Bereitstellen von Containern mithilfe von Elastic Beanstalk
- Emulieren von Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Inkrementelle Migration von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL mit Oracle SQL Developer und AWS SCT
- Integrieren Sie Stonebranch Universal Controller in AWS Mainframe Modernization
- Verwalten von AWS Service Catalog-Produkten in mehreren AWS-Konten und AWS-Regionen
- Migrieren eines AWS-Mitgliedskontos von AWS Organizations zu AWS Control Tower

- Migrieren und replizieren Sie VSAM-Dateien zu Amazon RDS oder Amazon MSK mithilfe von Connect from Precisely
- Migrieren von SAP ASE zu Amazon RDS for SQL Server mit AWS DMS
- Migrieren externer Oracle-Tabellen zu Amazon Aurora PostgreSQL – kompatibel
- Modernisieren Sie Mainframe-Batchdruck-Workloads in AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI
- ???
- Modernisieren Sie die Mainframe-Ausgabeverwaltung in AWS mithilfe von OpenText Micro Focus Enterprise Server und LRS PageCenterX
- ???
- Von AWS App2Container generierte Docker-Images optimieren
- Replizieren von Mainframe-Datenbanken in AWS mithilfe von Precisely Connect
- Ausführen von Amazon-ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere
- Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein
- Richten Sie die CloudFormation AWS-Drift-Erkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein
- Strukturieren eines Python-Projekts in hexaffinaler Architektur mit AWS Lambda
- Upgrade von SAP-Pacemaker-Clustern von ENSA1 auf ENSA2
- Verwenden von CloudEndure für die Notfallwiederherstellung einer On-Premises-Datenbank
- Lokales Validieren des Codes Account Factory für Terraform (AFT)

Netzwerk

Themen

Automatisieren der Einrichtung von regionsübergreifendem Peering mit AWS Transit Gateway

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Netzwerk; Hybrid Cloud	AWS-Services: AWS Transit Gateway ;AWS Step Functions ;AWS Lambda

Übersicht

AWS Transit Gateway verbindet Virtual Private Clouds (VPCs) und On-Premises-Netzwerke über einen zentralen Hub. Transit Gateway-Datenverkehr verbleibt immer im globalen Amazon Web Services (AWS)-Backbone und durchläuft nicht das öffentliche Internet, wodurch Bedrohungsvektoren wie häufige Exploits und DDoSDDoSAngriffe (Distributed Denial of Service) reduziert werden.

Wenn Sie zwischen zwei oder mehr AWS-Regionen kommunizieren müssen, können Sie regionsübergreifendes Transit Gateway-Peering verwenden, um Peering-Verbindungen zwischen Transit Gateways in verschiedenen Regionen herzustellen. Die manuelle Konfiguration des interregionalen Peerings mit Transit Gateway kann jedoch ein zeitaufwändiger Prozess sein, der mehrere Schritte umfasst. Dieses Muster bietet einen automatisierten Prozess zum Entfernen dieser manuellen Schritte mithilfe von Code für das Peering. Sie können diesen Ansatz verwenden, wenn Sie während einer Einrichtung einer Organisation mit mehreren Regionen mehrere Regionen und AWS-Konten wiederholt konfigurieren müssen.

Dieses Muster verwendet einen AWS- CloudFormation Stack, der den AWS Step Functions-Workflow, AWS Lambda-Funktionen, AWS Identity and Access Management (IAM)-Rollen und Protokollgruppen in Amazon CloudWatch Logs enthält. Anschließend können Sie eine Step-Functions-Ausführung starten und die interregionale Peering-Verbindung für Ihre Transit-Gateways erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3)-Bucket.
- Transit-Gateways, die in der Region des Anforderers und der Region des Annehmers erstellt und konfiguriert wurden. Die Anfordererregion ist der Ort, an dem eine Peering-Anforderung stammt, und die Annehmerregionen akzeptieren die Peering-Anforderung. Weitere Informationen dazu finden Sie unter Erstellen und Akzeptieren einer VPC-Peering-Verbindung in der Amazon-VPC-Dokumentation.
- VPCs , installiert und konfiguriert in den Regionen Annehmer und Anforderer. Schritte zum Erstellen einer VPC finden Sie unter Erstellen der VPC von Erste Schritte mit Amazon VPC in der Amazon-VPC-Dokumentation.
- Die VPCs müssen das `addToTransitGateway` Tag und den `true` Wert verwenden.
- Sicherheitsgruppen und Netzwerkzugriffssteuerungslisten (ACLs) für Ihre VPCs , konfiguriert gemäß Ihren Anforderungen. Weitere Informationen dazu finden Sie unter Sicherheitsgruppen für Ihre VPC und Netzwerk-ACLs in der Amazon-VPC-Dokumentation.

AWS-Regionen und -Einschränkungen

- Nur bestimmte AWS-Regionen unterstützen regionsübergreifendes Peering. Eine vollständige Liste der Regionen, die regionsübergreifendes Peering unterstützen, finden Sie in den FAQs AWS Transit Gateway.
- Im angehängten Beispielcode wird davon ausgegangen, dass die Region des Anforderers ist`us-east-2`, und die Region des Annehmers wird als angenommen`us-west-2`. Wenn Sie verschiedene Regionen konfigurieren möchten, müssen Sie diese Werte in allen Python-Dateien bearbeiten. Um eine komplexere Einrichtung zu implementieren, die mehr als zwei Regionen umfasst, können Sie die Step Function so ändern, dass die Regionen als Parameter an die Lambda-Funktion übergeben und die Funktion für jede Kombination ausführen.

Architektur

Das Diagramm zeigt einen Workflow mit den folgenden Schritten:

1. Der Benutzer erstellt einen AWS- CloudFormation Stack.

2. AWS CloudFormation erstellt einen Step Functions-Zustandsautomaten, der eine Lambda-Funktion verwendet. Weitere Informationen dazu finden Sie unter Erstellen eines Step Functions-Zustandsautomaten, der Lambda verwendet in der AWS Step Functions-Dokumentation.
3. Step Functions ruft eine Lambda-Funktion für Peering auf.
4. Die Lambda-Funktion erstellt eine Peering-Verbindung zwischen Transit-Gateways.
5. Step Functions ruft eine Lambda-Funktion für Änderungen der Routing-Tabelle auf.
6. Die Lambda-Funktion ändert die Routing-Tabellen, indem der CIDR-Block (Classless Inter-Domain Routing) der VPCs hinzugefügt wird.

Step-Functions-Workflow

Das Diagramm zeigt den folgenden Step Functions-Workflow:

1. Der Step-Functions-Workflow ruft die Lambda-Funktion für das Transit-Gateway-Peering auf.
2. Es gibt einen Timer-Aufruf, um eine Minute zu warten.
3. Der Peering-Status wird abgerufen und an den Bedingungsblock gesendet. Der Block ist für die Schleife verantwortlich.
4. Wenn die Erfolgsbedingung nicht erfüllt ist, wird der Workflow so codiert, dass er in die Timer-Phase eintritt.
5. Wenn die Erfolgsbedingung erfüllt ist, wird eine Lambda-Funktion aufgerufen, um die Routing-Tabellen zu ändern. Nach diesem Aufruf endet der Step-Functions-Workflow.

Tools

- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt.
- Amazon CloudWatch Logs – CloudWatch Mit Protokollen können Sie die Protokolle aller Ihrer Systeme, Anwendungen und AWS-Services, die Sie verwenden, zentralisieren.
- AWS Identity and Access Management (IAM) – IAM ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services.
- AWS Lambda – Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und übernimmt die gesamte Verwaltung der Rechenressourcen.

- AWS Step Functions – Step Functions erleichtert die Koordination der Komponenten verteilter Anwendungen als eine Reihe von Schritten in einem visuellen Workflow.

Polen

Automatisieren von Peering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die angehängten Dateien in Ihren S3-Bucket hoch.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3-Konsole und laden Sie dann die `get-transit-gateway-peering-status.zip` Dateien `modify-transit-gateway-routes.zip` `peer-transit-gateway.zip` , und (angefügt) in Ihren S3-Bucket hoch.	Allgemeines AWS
Erstellen Sie den AWS-CloudFormation Stack.	Führen Sie den folgenden Befehl aus, um einen AWS-CloudFormation Stack mit der `transit-gateway-peering.json` Datei (angefügt) zu erstellen: `aws cloudformation create-stack --stack-name myteststack --template-body file://sampletemplate.json` Der AWS- CloudFormation Stack erstellt den Step	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Functions-Workflow, die Lambda-Funktionen, IAM-Rollen und CloudWatch Protokollgruppen. Stellen Sie sicher, dass sich die AWS- CloudFormation Vorlage auf den S3-Bucket bezieht, der die zuvor hochgeladenen Dateien enthält. Hinweis: Sie können einen Stack auch mithilfe der AWS-CloudFormation Konsole erstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Stacks in der AWS- CloudFormation Konsole in der AWS-CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine neue Ausführung in Step Functions.	Öffnen Sie die Step Functions -Konsole und starten Sie eine neue Ausführung. Step Functions ruft die Lambda-Funktion auf und erstellt die Peering-Verbindung für die Transit-Gateways. Sie benötigen keine JSON-Eing abedatei. Stellen Sie sicher, dass eine Anfügung verfügbar ist und dass der Verbindun gstyp Peering ist. Weitere Informationen dazu finden Sie unter Starten einer neuen Ausführung ab Erste Schritte mit AWS Step Functions in der AWS Steps Functions-Dokumentation.	DevOps Techniker, Allgemein es AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Routen in den Routing-Tabellen.	Zwischen den Transit-Gateways wird ein interregionales Peering eingerichtet. Die Routing-Tabellen werden mit dem IPv4-CIDR-Blockbereich der Peer-Region-VPC aktualisiert. Öffnen Sie die Amazon-VPC-Konsole und wählen Sie die Registerkarte Zuordnungen in der Routing-Tabelle aus, die der Transit-Gateway-Anfügung entspricht. Überprüfen Sie den VPC-CIDR-Blockbereich der per Peering verbundenen Regionen. Ausführliche Schritte und Anweisungen finden Sie unter Zuordnen einer Transit-Gateway-Routing-Tabelle in der Amazon-VPC-Dokumentation.	Netzwerkadministrator

Zugehörige Ressourcen

- Ausführungen in Step Functions
- Transit-Gateway-Peering-Anfügungen
- Verbinden von VPCs über AWS-Regionen hinweg mithilfe von AWS Transit Gateway – Demo (Video)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Zentralisieren der Netzwerkkonnektivität mit AWS Transit Gateway

Erstellt von Mydhili (AWS) und Nikhil Marrapu (AWS)

Umgebung: Produktion	Technologien: Netzwerk	AWS-Services: AWS Transit Gateway; Amazon VPC

Übersicht

Dieses Muster beschreibt die einfachste Konfiguration, in der AWS Transit Gateway verwendet werden kann, um ein On-Premises-Netzwerk mit Virtual Private Clouds (VPCs) in mehreren AWS-Konten innerhalb einer AWS-Region zu verbinden. Mit dieser Einrichtung können Sie ein Hybrid-Netzwerk einrichten, das mehrere VPC-Netzwerke in einer Region und ein On-Premises-Netzwerk miteinander verbindet. Dies wird durch die Verwendung eines Transit-Gateways und einer Virtual Private Network (VPN)-Verbindung zum On-Premises-Netzwerk erreicht.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Konto für das Hosten von Netzwerkservices, das als Mitgliedskonto einer Organisation in AWS Organizations verwaltet wird
- VPCs in mehreren AWS-Konten, ohne sich überschneidende CIDR-Blöcke (Classless Inter-Domain Routing)

Einschränkungen

Dieses Muster unterstützt nicht die Isolierung des Datenverkehrs zwischen bestimmten VPCs oder dem On-Premises-Netzwerk. Alle an das Transit Gateway angeschlossenen Netzwerke können sich gegenseitig erreichen. Um den Datenverkehr zu isolieren, müssen Sie benutzerdefinierte Routing-Tabellen auf dem Transit-Gateway verwenden. Dieses Muster verbindet die VPCs und das On-Premises-Netzwerk nur mithilfe einer einzigen standardmäßigen Transit-Gateway-Routing-Tabelle, was die einfachste Konfiguration ist.

Architektur

Zieltechnologie-Stack

- AWS Transit Gateway
- AWS Site-to-Site-VPN
- VPC
- AWS Resource Access Manager (AWS RAM)

Zielarchitektur

Tools

AWS-Services

- AWS Resource Access Manager (AWS RAM) hilft Ihnen, Ihre Ressourcen sicher über Ihre AWS-Konten, Organisationseinheiten oder Ihre gesamte Organisation von AWS Organizations freizugeben.
- AWS Transit Gateway ist ein zentraler Hub, der Virtual Private Clouds (VPCs) und On-Premises-Netzwerke miteinander verbindet.

Polen

Erstellen eines Transit-Gateways im Netzwerkdienstkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Transit-Gateway.	Erstellen Sie in dem AWS-Konto, in dem Sie Netzwerkservices hosten möchten, ein Transit-Gateway in der AWS-Zielregion. Anweisungen finden Sie unter Erstellen eines Transit-Gateways. Beachten Sie Folgendes:	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie Standard-Routing-Tabellenzuordnung aus. • Wählen Sie Standard-Verbreitung von Routing-Tabellen aus.	

Verbinden des Transit-Gateways mit Ihrem On-Premises-Netzwerk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie ein Kunden-Gateway-Gerät für die VPN-Verbindung ein.	Das Kunden-Gateway-Gerät ist auf der On-Premises-Seite der Site-to-Site-VPN-Verbindung zwischen dem Transit-Gateway und Ihrem On-Premises-Netzwerk angeschlossen. Weitere Informationen finden Sie unter Ihr Kunden-Gateway-Gerät in der AWS Site-to-Site VPN-Dokumentation. Identifizieren oder starten Sie ein unterstütztes On-Premises-Kundengerät und notieren Sie sich dessen öffentliche IP-Adresse. Die VPN-Konfiguration wird später in diesem Epos abgeschlossen.	Netzwerkadministrator
Erstellen Sie im Netzwerkdienstkonto eine VPN-Anfügung an das Transit-Gateway.	Um eine Verbindung einzurichten, erstellen Sie eine VPN-Anfügung für das Transit-Gateway. Anweisungen finden	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie unter Transit-Gateway-VPN-Anfügungen.	
Konfigurieren Sie das VPN auf dem Kunden-Gateway-Gerät in Ihrem On-Premises-Netzwerk.	Laden Sie die Konfigurationsdatei für die Site-to-Site-VPN-Verbindung herunter, die dem Transit-Gateway zugeordnet ist, und konfigurieren Sie VPN-Einstellungen auf dem Kunden-Gateway-Gerät. Anweisungen finden Sie unter Herunterladen der Konfigurationsdatei .	Netzwerkadministrator

Freigeben des Transit-Gateways im Netzwerkdienstkonto für andere AWS-Konten oder Ihre Organisation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie im AWS Organizations-Verwaltungskonto die Freigabe.	Um das Transit Gateway für Ihre Organisation oder für bestimmte Organisationseinheiten freizugeben, aktivieren Sie die Freigabe in AWS Organizations . Andernfalls müssten Sie das Transit-Gateway für jedes Konto einzeln freigeben. Anweisungen finden Sie unter Aktivieren der Ressourcenfreigabe in AWS Organizations.	AWS-Systemadministrator
Erstellen Sie die Transit-Gateway-Ressourcenfreigabe im Netzwerkdienstkonto.	Damit VPCs in anderen AWS-Konten innerhalb Ihrer Organisation eine Verbindung	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zum Transit-Gateway herstelle n können, verwenden Sie im Konto der Netzwerks ervices die AWS RAM-Konso le, um die Transit-Gateway-Ressource freizugeben. Anweisungen finden Sie unter Erstellen einer Ressource nfreigabe.	

Verbinden von VPCs mit dem Transit Gateway

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie VPC-Anhänge in einzelnen Konten.	Erstellen Sie in den Konten, für die das Transit-Gateway freigegeben wurde, Transit-Gateway-VPC-Anhänge . Anweisungen finden Sie unter Erstellen einer Transit-Gateway-Anfügung an eine VPC.	Netzwerkadministrator
Akzeptieren Sie die VPC-Anfügungsanforderungen.	Akzeptieren Sie im Netzwerkd ienstkonto die Transit-Gateway-VPC-Anfügun gsanforderungen. Anweisung en finden Sie unter Akzeptier en eines freigegebenen Anhangs.	Netzwerkadministrator

Routing konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Routen in einzelnen Konto-VPCs.	Fügen Sie in jeder einzelnen Konto-VPC Routen zum On-Premises-Netzwerk und zu anderen VPC-Netzwerken hinzu, wobei Sie das Transit-Gateway als Ziel verwenden. Anweisungen finden Sie unter Hinzufügen und Entfernen von Routen aus einer Routing-Tabelle.	Netzwerkadministrator
Konfigurieren Sie Routen in der Transit-Gateway-Routing-Tabelle.	Routen von VPCs und der VPN-Verbindung sollten propagiert werden und in der Transit-Gateway-Standard-Routing-Tabelle angezeigt werden. Erstellen Sie bei Bedarf alle statischen Routen (ein Beispiel sind statische Routen für die statische VPN-Verbindung) in der Transit-Gateway-Standard-Routing-Tabelle. Anweisungen finden Sie unter Erstellen einer statischen Route.	Netzwerkadministrator
Fügen Sie Regeln für Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACL) hinzu.	Stellen Sie für die EC2-Instances und andere Ressourcen in der VPC sicher, dass die Sicherheitsgruppenregeln und die Netzwerk-ACL-Regeln Datenverkehr zwischen VPCs sowie dem On-Premis	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	es-Netzwerk zulassen. Anweisungen finden Sie unter Steuern des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen und Hinzufügen und Löschen von Regeln aus einer ACL.	

Testen der Konnektivität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Konnektivität zwischen VPCs.	Stellen Sie sicher, dass Netzwerk-ACL und Sicherheitsgruppen Internet Control Message Protocol (ICMP)-Datenverkehr zulassen und dann von Instances in einer VPC zu einer anderen VPC pingen, die ebenfalls mit dem Transit Gateway verbunden ist.	Netzwerkadministrator
Testen Sie die Konnektivität zwischen VPCs und dem On-Premises-Netzwerk.	Stellen Sie sicher, dass Netzwerk-ACL-Regeln, Sicherheitsgruppenregeln und alle Firewalls ICMP-Datenverkehr zulassen und dann zwischen dem On-Premises-Netzwerk und den EC2-Instances in den VPCs pingen. Die Netzwerkkommunikation muss zuerst vom On-Premises-Netzwerk initiiert werden,	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um die VPN-Verbindung in den -UPStatus zu versetzen.	

Zugehörige Ressourcen

- Aufbau einer skalierbaren und sicheren Multi-VPC-AWS-Netzwerkinfrastruktur (AWS-Whitepaper)
- Arbeiten mit freigegebenen Ressourcen (AWS-RAM-Dokumentation)
- Arbeiten mit Transit Gateways (AWS Transit Gateway-Dokumentation)

Konfigurieren Sie die HTTPS-Verschlüsselung für Oracle JD Edwards EnterpriseOne auf Oracle WebLogic mithilfe eines Application Load Balancer

Umgebung: Produktion	Technologien: Netzwerke ; Sicherheit, Identität, Compliance	Arbeitslast: Oracle
AWS-Services: AWS Certificate Manager (ACM); Elastic Load Balancing (ELB); Amazon Route 53		

Übersicht

Dieses Muster erklärt, wie die HTTPS-Verschlüsselung für SSL-Offloading in Oracle JD Edwards EnterpriseOne auf Oracle-Workloads konfiguriert wird. WebLogic Bei diesem Ansatz wird der Datenverkehr zwischen dem Browser des Benutzers und einem Load Balancer verschlüsselt, um die Server von der Verschlüsselungslast zu entlasten. EnterpriseOne

Viele Benutzer skalieren die Stufe der EnterpriseOne JAVA Virtual Machine (JVM) horizontal, indem sie einen AWS Application Load Balancer verwenden.Der Load Balancer dient als zentrale Anlaufstelle für Kunden und verteilt den eingehenden Datenverkehr auf mehrere JVMs. Optional kann der Load Balancer den Datenverkehr auf mehrere Availability Zones verteilen und die Verfügbarkeit von erhöhen. EnterpriseOne

Der in diesem Muster beschriebene Prozess konfiguriert die Verschlüsselung zwischen dem Browser und dem Load Balancer, anstatt den Verkehr zwischen dem Load Balancer und den JVMs zu verschlüsseln. EnterpriseOne Dieser Ansatz wird als SSL-Offloading bezeichnet. Die Auslagerung des SSL-Entschlüsselungsprozesses vom EnterpriseOne Web- oder Anwendungsserver auf den Application Load Balancer reduziert die Belastung der Anwendungsseite. Nach der SSL-Terminierung am Load Balancer wird der unverschlüsselte Datenverkehr an die Anwendung auf AWS weitergeleitet.

Oracle JD Edwards EnterpriseOne ist eine ERP-Lösung (Enterprise Resource Planning) für Unternehmen, die Produkte oder Sachanlagen herstellen, konstruieren, vertreiben, warten oder verwalten. JD Edwards EnterpriseOne unterstützt verschiedene Hardware, Betriebssysteme und Datenbankplattformen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM) -Rolle, die berechtigt ist, AWS-Serviceanrufe zu tätigen und AWS-Ressourcen zu verwalten
- Ein SSL-Zertifikat

Produktversionen

- Dieses Muster wurde mit Oracle WebLogic 12c getestet, Sie können aber auch andere Versionen verwenden.

Architektur

Es gibt mehrere Ansätze, um SSL-Offloading durchzuführen. Dieses Muster verwendet einen Application Load Balancer und einen Oracle HTTP Server (OHS), wie in der folgenden Abbildung dargestellt.

Das folgende Diagramm zeigt das JVM-Layout von JD Edwards EnterpriseOne, Application Load Balancer und Java Application Server (JAS).

Tools

AWS-Services

- Application Load Balancer verteilen den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (Amazon EC2 EC2-Instances), in mehreren Availability Zones.

- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Bewährte Methoden

- Bewährte Methoden für ACM finden Sie in der ACM-Dokumentation.

Epen

Einrichtung WebLogic und Arbeitsschutz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie Oracle-Komponenten.	1. Installieren Sie Fusion Middleware Infrastructure, indem Sie dem Standardinstallationsprozess folgen. Dieses Programm hilft Ihnen bei der Installation und Konfiguration einer WebLogic Domain. Anweisungen finden Sie in der Oracle-Dokumentation. 2. Installieren Sie OHS, indem Sie dem Standardinstallationsprozess folgen. Anweisungen finden Sie in der Oracle-Dokumentation. 3. Wenn die Installation abgeschlossen ist, starten Sie den Konfigurationsassistenten (`config.sh`	JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei), um OHS zu konfigurieren. • Sie können eine bestehende Domain aktualisieren oder eine neue Domain erstellen. Bei diesem Muster wird davon ausgegangen, dass Sie eine bestehende Domain aktualisieren. • Wählen Sie für Verfügbare Vorlagen Oracle Enterprise Manager-Restricted JRF und Oracle HTTP Server (Restricted JRF). Wenn Sie diese Optionen für Java Required Files (JRF) auswählen, entfällt die Verbindung zu einer externen Datenbank. • Akzeptieren Sie für Verwaltete Server, Cluster, Servervorlagen, Coherence Clusters, Machines, Assign Servers to Machines, Virtuelle Ziele und Partitionen die Standardkonfigurationswerte und wählen Sie Weiter, um zur nächsten Kategorie zu wechseln.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Vervollständigen Sie die Konfigurationsdetails (z. B. Administratorhost und Port, Listenadresse und Port, Servername) für die OHS-Instanz (z. B.`ohs1`).	
Aktivieren Sie das WebLogic Plugin auf Domainebene.	Das WebLogic Plugin ist für den Lastenausgleich erforderl ich. Um das Plugin zu aktiviere n: 1. Melden Sie sich über den WebLogic folgenden Link bei der Verwaltungskonsole an: `http://<WeblogicSe rver>:<Adminport>/ console` 2. Wählen Sie Sperren und Bearbeiten und anschließend Konfiguration, Webanwendungen. 3. Wählen Sie das WebLogic Plugin aktiviert (Kontroll kästchen oder Drop-down-Option). 4. Wählen Sie Änderungen speichern und aktivieren.	JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bearbeiten Sie die Konfigurationsdatei.	Die `mod_wl_ohs.conf` Datei konfiguriert Proxy-Anfragen von OHS an. WebLogic
	1. Bearbeiten Sie diese Datei. Sie befindet sich in:
	`$ORACLE_HOME/user_projects/domains/`
	Beispielsweise:
	`/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1`
	2. Fügen Sie die Werte WebLogic host (`WebLogicHost`) und port (`WebLogicPort`) hinzu (Dieses Muster geht von localhost und Port 8000 aus.)
	3. Fügen Sie die `WLProxySSLPassThrough` Werte `WLProxySSL` und wie folgt hinzu:
	`<VirtualHost *:8000>`
	`<Location /jde>`
	`WLSRequest On`
		JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>SetHandler weblogic-
	handler
	WebLogicHost
	 localhost
	WebLogicPort 8000
	WLProxySSL On
	WLProxySSLPassThrough
	 On
	</Location>
	</VirtualHost></pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie OHS mit dem Enterprise Manager.	1. Melden Sie sich über den folgenden Link bei Enterprise Manager Fusion Middleware an: `http://<WeblogicServer>:<Adminport>/em/` 2. Wählen Sie in Target Navigation unter HTTP-Server die OHS-Instanz aus (z. B.). `ohs1` 3. Wählen Sie Herunterfahren und Starten, um die OHS-Instanz neu zu starten. 4. Wenn das OHS-Setup abgeschlossen ist, können Sie eine Verbindung zum EnterpriseOne HTML-Client herstellen, indem Sie Ihren HTTP-Server-Hostnamen mit Port 8000 anstelle des EnterpriseOne Server-Hostnamens verwenden. • Alter Link: `http://<Webserver>:80/jde/owhtml` • Neuer Link: `http://<HTTP server or web server>:8000/jde/owhtml` Wenn Sie einen anderen Port als den standardm	JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	äßigen Oracle-HTTP-Port verwenden, bearbeiten Sie die `httpd.conf` Datei, um an zwei Stellen einen Listener für diesen Port hinzuzufügen:
	`#[Listen] OHS_LISTEN_PORT`
	`Listen 8000`
	und:
	`#`
	`ServerName <Weblogic Server1>:8000`	

Den Application Load Balancer konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine Zielgruppe ein.	1. Erstellen Sie eine Zielgruppe für den HTTP-Server-Port 8000. 2. Registrieren Sie die Ziele unter der Zielgruppe mit demselben Port. 3. Überprüfen Sie den Status der Ziele, um sicherzustellen, dass sie fehlerfrei sind. 4. Konfigurieren Sie die Einstellungen für die	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Integritätsprüfung nach Bedarf. Eine ausführliche Anleitung finden Sie in der Elastic Load Balancing Balancing-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Load Balancer ein.	1. Erstellen Sie einen Application Load Balancer mit Standardattributen und der erforderlichen Virtual Private Cloud (VPC), Sicherheitsgruppen und Subnetzen. Anweisungen finden Sie in der Elastic Load Balancing Balancing-Dokumentation. 2. Fügen Sie einen Listener-Eintrag für HTTPS 443 hinzu und leiten Sie ihn an die Zielgruppe weiter, die Sie im vorherigen Schritt erstellt haben. (Anweisungen finden Sie in der Elastic Load Balancing Balancing-Dokumentation.) Ein HTTPS-Listener benötigt ein SSL-Zertifikat. Sie können ein Zertifikat von ACM auswählen oder eines hochladen. 3. Aktivieren Sie für beide Listener Stickiness, indem Sie den Anweisungen in der Elastic Load Balancing Balancing-Dokumentation folgen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Route 53 53-Eintrag (DNS) hinzu.	(Optional) Sie können einen Amazon Route 53 53-DNS-Eintrag für die Subdomain hinzufügen. Dieser Datensatz würde auf Ihren Application Load Balancer verweisen. Anweisungen finden Sie in der Dokumentation zu Route 53	AWS-Administrator

Fehlerbehebung

Problem	Lösung
Der HTTP-Server wird nicht angezeigt.	Wenn der HTTP-Server nicht in der Zielnavigationsliste der Enterprise Manager-Konsole erscheint, gehen Sie wie folgt vor: 1. Wählen Sie unter WebLogic Domain, Administration die Option OHS-Instances aus. 2. Wählen Sie Create, um eine neue OHS-Instanz zu erstellen. 3. Geben Sie einen Instanznamen ein und wählen Sie dann OK, um die Instanz zu erstellen. Wenn die Instanz erstellt und die Änderungen aktiviert wurden, können Sie den HTTP-Server im Zielnavigationsbereich sehen.

Zugehörige Ressourcen

AWS-Dokumentation

- Application Load Balancer
- Arbeiten mit öffentlich gehosteten Zonen
- Arbeiten mit privaten Hosting-Zonen

Oracle-Dokumentation:

- Überblick über das Oracle WebLogic Server Proxy Plug-In
- WebLogic Server mit dem Infrastructure Installer installieren
- Installation und Konfiguration des Oracle HTTP-Servers

Herstellen einer Verbindung mit Application Migration Service-Daten- und Steuerebenen über ein privates Netzwerk

Erstellt von Dipin Jain (AWS) und Bol Kuznetsov (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Netzwerk; Migration	AWS-Services: AWS Application Migration Service; Amazon EC2; Amazon VPC; Amazon S3

Übersicht

Dieses Muster erklärt, wie Sie mithilfe von Schnittstellen-VPC-Endpunkten eine Verbindung zu einer AWS Application Migration Service (AWS MGN)-Datenebene und Steuerebene in einem privaten, gesicherten Netzwerk herstellen können.

Application Migration Service ist eine hoch automatisierte lift-and-shift (Hostwechsel-)Lösung, die die Kosten für die Migration von Anwendungen zu AWS vereinfacht, beschleunigt und senkt. Es ermöglicht Unternehmen, eine große Anzahl physischer, virtueller oder Cloud-Server ohne Kompatibilitätsprobleme, Leistungsunterbrechungen oder lange Cutover-Fenster neu zu hosten. Application Migration Service ist über die AWS-Managementkonsole verfügbar. Dies ermöglicht eine nahtlose Integration mit anderen AWS-Services wie AWS CloudTrail, Amazon CloudWatchund AWS Identity and Access Management (IAM).

Sie können eine Verbindung von einem Quell-Rechenzentrum zu einer Datenebene herstellen, d. h. zu einem Subnetz, das als Staging-Bereich für die Datenreplikation in der Ziel-VPC dient, über eine private Verbindung, indem Sie AWS VPN-Services, AWS Direct Connect oder VPC-Peering in Application Migration Service verwenden. Sie können auch Schnittstellen-VPC-Endpunkte verwenden, die von AWS unterstützt werden PrivateLink , um über ein privates Netzwerk eine Verbindung zu einer Application Migration Service-Steuerebene herzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Subnetz des Bereitstellungsbereichs – Bevor Sie Application Migration Service einrichten, erstellen Sie ein Subnetz, das als Bereitstellungsbereich für Daten verwendet werden soll, die von Ihren

Quellservern zu AWS (d. h. einer Datenebene) repliziert werden. Sie müssen dieses Subnetz in der Vorlage für Replikationseinstellungen angeben, wenn Sie zum ersten Mal auf die Application Migration Service-Konsole zugreifen. Sie können dieses Subnetz für bestimmte Quellserver in der Vorlage mit den Replikationseinstellungen überschreiben. Obwohl Sie ein vorhandenes Subnetz in Ihrem AWS-Konto verwenden können, empfehlen wir Ihnen, zu diesem Zweck ein neues dediziertes Subnetz zu erstellen.

- Netzwerkanforderungen – Die Replikationsserver, die von Application Migration Service in Ihrem Staging-Bereich-Subnetz gestartet werden, müssen in der Lage sein, Daten an den Application Migration Service-API-Endpunkt unter zu sendenhttps://mgn.<region>.amazonaws.com/, wobei der Code für die AWS-Region <region> ist, in die Sie replizieren (z. B. https://mgn.us-east-1.amazonaws.com). Amazon Simple Storage Service (Amazon S3)-Service-URLs sind zum Herunterladen von Application Migration Service-Software erforderlich.
  - Das AWS Replication Agent-Installationsprogramm sollte Zugriff auf die S3-Bucket-URL der AWS-Region haben, die Sie mit Application Migration Service verwenden.
  - Das Subnetz des Staging-Bereichs sollte Zugriff auf Amazon S3 haben.
  - Die Quellserver, auf denen der AWS Replication Agent installiert ist, müssen in der Lage sein, Daten an die Replikationsserver im Subnetz des Staging-Bereichs und an den API-Endpunkt des Application Migration Service unter zu sendenhttps://mgn.<region>.amazonaws.com/.

In der folgenden Tabelle sind die erforderlichen Ports aufgeführt.

Quelle	Zieladresse	Port	Weitere Informationen finden Sie unter
Quell-Rechenzentrum	Amazon S3-Service-URLs	443 (TCP)	Kommunikation über TCP-Port 443
Quell-Rechenzentrum	AWS-regionsspezifische Konsolenadresse für Application Migration Service	443 (TCP)	Kommunikation zwischen den Quellservern und dem Application Migration Service über TCP-Port 443
Quell-Rechenzentrum	Subnetz des Staging-Bereichs	1 500 (TCP)	Kommunikation zwischen den

			Quellservern und dem Subnetz des Staging-Bereichs über TCP-Port 1500
Subnetz des Staging-Bereichs	AWS-regionsspezifische Konsolenadresse für Application Migration Service	443 (TCP)	Kommunikation zwischen dem Subnetz des Staging-Bereichs und dem Application Migration Service über TCP-Port 443
Subnetz des Staging-Bereichs	Amazon S3-Service-URLs	443 (TCP)	Kommunikation über TCP-Port 443
Subnetz des Staging-Bereichs	Amazon EC2-Endpunkt der AWS-Region des Subnetzes	443 (TCP)	Kommunikation über TCP-Port 443

Einschränkungen

Application Migration Service ist derzeit nicht in allen AWS-Regionen und -Betriebssystemen verfügbar.

- Unterstützte AWS-Regionen
- Unterstützte Betriebssysteme

Architektur

Das folgende Diagramm veranschaulicht die Netzwerkarchitektur für eine typische Migration. Weitere Informationen zu dieser Architektur finden Sie in der Dokumentation zum Application Migration Service und im Video zur Architektur und Netzwerkarchitektur des Application Migration Service.

Die folgende Detailansicht zeigt die Konfiguration von Schnittstellen-VPC-Endpunkten in der Staging-Bereich-VPC, um Amazon S3 und Application Migration Service zu verbinden.

Tools

- AWS Application Migration Service ist ein AWS-Service, der das Hostwechsel von Anwendungen in AWS vereinfacht, beschleunigt und senkt.
- Schnittstellen-VPC-Endpunkte ermöglichen es Ihnen, eine Verbindung zu Services herzustellen, die von AWS betrieben werden, PrivateLink ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung erforderlich sind. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit den Ressourcen in dem Service zu kommunizieren. Der Datenverkehr zwischen Ihrer VPC und dem anderen Service verlässt das Amazon-Netzwerk nicht.

Polen

Erstellen von Endpunkten für Application Migration Service, Amazon EC2 und Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Schnittstellenendpunkt für Application Migration Service.	Die VPC des Quellrech enzentrums und des Staging-Bereichs stellt über den Schnittstellenendpunkt, den Sie in der Ziel-Staging-Berei ch-VPC erstellen, eine private Verbindung zur Application Migration Service-Steuereben e her. So erstellen Sie den Endpunkt: 1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/. 2. Wählen Sie im Navigatio nsbereich Endpoints und	Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	klicken Sie auf Create Endpoint. 3. Wählen Sie für Service category die Option AWS services. 4. Geben Sie für Servicena me ein `com.amazo naws.<region>.mgn` . Wählen Sie für Typ die Option Schnittstelle aus. 5. Wählen Sie für VPC eine Ziel-Stagingbereich-VPC aus, um den Endpunkt zu erstellen. 6. Für Subnets wählen Sie die Subnetze (Availabi lity Zones) aus, in denen die Endpunktnetzwerksc hnittstellen erstellt werden sollen. 7. Um ein privates DNS für den Schnittstellenendpunkt zu aktivieren, wählen Sie im Abschnitt Zusätzliche Einstellungen die Option DNS-Namen aktivieren aus. 8. Wählen Sie eine Sicherhei tsgruppe aus, die eingehenden Datenverkehr aus dem VPC-Subnetz des Staging-Bereichs über TCP 443 zulässt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Endpunkt erstellen aus. Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte in der Amazon-VPC-Dokumentation.	
Konfigurieren Sie den Schnittstellenendpunkt für Amazon EC2.	Die VPC des Staging-Bereichs stellt über den Schnittstellenendpunkt, den Sie in der VPC des Ziel-Staging-Bereichs erstellen, eine private Verbindung zur Amazon EC2-API her. Um den Endpunkt zu erstellen, folgen Sie den Anweisungen in der vorherigen Geschichte. • Geben Sie für Servicename ein `com.amazonaws.<region>.ec2` . Wählen Sie für Typ die Option Schnittstelle aus. • Die Sicherheitsgruppe muss eingehenden HTTPS-Datenverkehr vom Stagingbereich-VPC-Subnetz über Port 443 zulassen. • Wählen Sie im Abschnitt Zusätzliche Einstellungen die Option DNS-Namen aktivieren aus.	Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Schnittstellenendpunkt für Amazon S3.	Die VPC des Quell-Rechenzentrums und des Staging-Bereichs stellt über den Schnittstellenendpunkt, den Sie in der Ziel-Staging-Bereich-VPC erstellen, eine private Verbindung zur Amazon S3-API her. Um den Endpunkt zu erstellen, folgen Sie den Anweisungen in der ersten Geschichte. • Geben Sie für Servicename ein `com.amazonaws.<region>.s3` . Wählen Sie für Typ die Option Schnittstelle aus. • Die VPC-Sicherheitsgruppe muss eingehenden HTTPS-Datenverkehr vom Stagingbereich-VPC-Subnetz über Port 443 zulassen. • Deaktivieren Sie im Abschnitt Zusätzliche Einstellungen die Option DNS-Namen aktivieren . Amazon S3-Schnittstellenendpunkte unterstützen keine privaten DNS-Namen. Hinweis: Sie verwenden einen Schnittstellenendpunkt, da Gateway-Endpunktve	Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rbindungen nicht aus einer VPC erweitert werden können. (Details finden Sie in der Amazon-VPC-Dokumentation.)	
Konfigurieren Sie den Amazon S3-Gateway-Endpunkt.	Während der Konfigurationsphase muss sich der Replikationsserver mit einem S3-Bucket verbinden, um die Softwareupdates des AWS Replication Servers herunterzuladen. Amazon-S3-Schnittstellenendpunkte unterstützen jedoch keine privaten DNS-Namen und es gibt keine Möglichkeit, einem Replikationsserver einen DNS-Namen für einen Amazon S3-Endpunkt bereitzustellen. Um dieses Problem zu beheben, erstellen Sie einen Amazon S3-Gateway-Endpunkt in der VPC, zu der das Subnetz des Staging-Bereichs gehört, und aktualisieren die Routing-Tabellen des Staging-Subnetzes mit den relevanten Routen. Weitere Informationen finden Sie unter Erstellen eines Gateway-Endpunkts in der AWS-PrivateLink Dokumentation.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie On-Premises-DNS, um private DNS-Namen für Endpunkte aufzulösen.	Die Schnittstellenendpunkte für Application Migration Service und Amazon EC2 haben private DNS-Namen, die in der VPC aufgelöst werden können. Sie müssen jedoch auch On-Premises-Server konfigurieren, um private DNS-Namen für diese Schnittstellenendpunkte aufzulösen. Es gibt mehrere Möglichkeiten, diese Server zu konfigurieren. In diesem Muster haben wir diese Funktionalität getestet, indem wir On-Premises-DNS-Abfragen an den eingehenden Endpunkt von Amazon Route 53 Resolver in der Staging-Bereich-VPC weiterleiten. Weitere Informationen finden Sie unter Auflösen von DNS-Abfragen zwischen VPCs und Ihrem Netzwerk in der Route 53-Dokumentation.	Migrationsingenieur

Herstellen einer Verbindung mit der Application Migration Service-Steuerebene über einen privaten Link

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS Replication Agent mithilfe von AWS PrivateLink.	1. Laden Sie den AWS Replication Agent in einen privaten S3-Bucket in der Zielregion herunter. 2. Melden Sie sich bei den Quellservern an, die migriert werden sollen. Das AWS Replication Agent-Installationsprogramm benötigt Netzwerkzugriff auf den Application Migration Service und Amazon S3-Endpunkte. Da Ihr On-Premises-Netzwerk nicht für den Application Migration Service und öffentliche Amazon S3-Endpunkte geöffnet ist, müssen Sie den Agent mithilfe der Schnittstellenendpunkte installieren, die Sie in den vorherigen Schritten mithilfe von AWS erstellt haben PrivateLink. Hier ist ein Beispiel für Linux: 1. Laden Sie den Agent mit dem Befehl herunter:	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-<aws_region>.bucket.<s3-endpoint-DNS-name>/latest/linux/aws-replication-installer-init.py`
	
	Hinweis: `bucket` ist ein statisches Schlüsselwort, das Sie vor dem DNS-Namen des Amazon S3-Schnittstellenendpunkts hinzufügen müssen. Weitere Informationen finden Sie in der Amazon S3-Dokumentation.
	
	Wenn der DNS-Name des Amazon S3-Schnittstellenendpunkts beispielsweise lautet `vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com` und die AWS-Region lautet `us-west-1`, verwenden Sie den Befehl :
	
	`wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-us-west-1.bucket.vpce-009c8b`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	07adb052a11-qgf8q5 0y.s3.us-west-1.vp ce.amazonaws.com/l atest/linux/aws-re plication-installer- init.py 2. Installieren Sie den Agent: • Wenn Sie beim Erstellen eines Schnittstellenendp unkts für Applicati on Migration Service DNS-Namen aktivieren ausgewählt haben, führen Sie den Befehl aus: sudo python3 aws- replication-installer- init.py \ --region <aws_regi on> \ --aws-access-key-i d <access-key> \ --aws-secret-acces s-key <secret-key> \ --no-prompt \ --s3-endpoint <s3- endpoint-DNS-name> • Wenn Sie beim Erstellen des Schnittstellenendpunkts für Application Migration Service nicht DNS-Namen aktivieren ausgewählt haben, führen Sie den Befehl aus:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sudo python3 aws-replication-installer-init.py \ --region <aws_region> \ --aws-access-key-id <access-key> \ --aws-secret-access-key <secret-key> \ --no-prompt \ --s3-endpoint <s3-endpoint-DNS-name> \ --endpoint <mgn-endpoint-DNS-name>` Weitere Informationen finden Sie in der AWS Replication Agent-Installationsanleitung in der Dokumentation zum Application Migration Service. Nachdem Sie Ihre Verbindung mit Application Migration Service hergestellt und den AWS Replication Agent installiert haben, folgen Sie den Anweisungen in der Application Migration Service-Dokumentation, um Ihre Quellserver zu Ihrer Ziel-VPC und Ihrem Subnetz zu migrieren.	

Zugehörige Ressourcen

Dokumentation zum Application Migration Service

- Konzepte
- Migrationsworkflow
- Schnellstartanleitung
- HÄUFIG GESTELLTE FRAGEN
- Fehlersuche

Weitere Ressourcen

- AWS Application Migration Service – Eine technische Einführung (Anleitung für AWS Training and Certification)
- AWS Application Migration Service-Architektur und Netzwerkarchitektur (Video)

Zusätzliche Informationen

Fehlerbehebung bei AWS Replication Agent-Installationen auf Linux-Servern

Wenn Sie einen gcc-Fehler auf einem Amazon Linux-Server erhalten, konfigurieren Sie das Paket-Repository und verwenden Sie den folgenden Befehl:

```
## sudo yum groupinstall "Development Tools"
```

Erstellen von Infoblox-Objekten mit CloudFormation benutzerdefinierten AWS-Ressourcen und Amazon SNS

Erstellt von Tim Sutton (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Netzwerk	Workload: Alle anderen Workloads
AWS-Services: Amazon SNS; AWS CloudFormation; AWS KMS; AWS Lambda ;AWS Organizations		

Übersicht

Infoblox Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) und IP Address Management (Infoblox DDI) ermöglichen es Ihnen, eine komplexe Hybrid-Umgebung zu zentralisieren und effizient zu steuern. Mit Infoblox DDI können Sie alle Netzwerkressourcen in einer autoritativen IP-Adressmanagement (IPAM)-Datenbank erkennen und aufzeichnen. Darüber hinaus können Sie DNS On-Premises und in der Amazon Web Services (AWS) Cloud mithilfe derselben Appliances verwalten.

Dieses Muster beschreibt, wie Sie eine CloudFormation benutzerdefinierte AWS-Ressource verwenden, um Infoblox-Objekte (z. B. DNS-Datensätze oder IPAM-Objekte) zu erstellen, indem Sie die Infoblox-WAPI aufrufen. Weitere Informationen zur Infoblox WAPI finden Sie in der WAPI-Dokumentation in der Infoblox-Dokumentation.

Durch die Verwendung dieses Musters können Sie eine einheitliche Ansicht der DNS-Datensätze und IPAM-Konfigurationen für Ihre AWS- und On-Premises-Umgebungen erhalten, zusätzlich zum Entfernen manueller Prozesse, die Datensätze erstellen und Ihre Netzwerke bereitstellen. Sie können den Ansatz dieses Musters für die folgenden Anwendungsfälle verwenden:

- Hinzufügen eines A-Datensatzes nach dem Erstellen einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance
- Hinzufügen eines CNAME-Datensatzes nach dem Erstellen eines Application Load Balancers

- Hinzufügen eines Netzwerkobjekts nach dem Erstellen einer Virtual Private Cloud (VPC)
- Bereitstellung des nächsten Netzwerkbereichs und Verwendung dieses Bereichs zum Erstellen von Subnetzen

Sie können dieses Muster auch erweitern und andere Infoblox-Gerätefunktionen wie das Hinzufügen verschiedener DNS-Datensatztypen oder das Konfigurieren von Infoblox vDiscovery verwenden.

Das Muster verwendet ein hub-and-spoke Design, in dem der Hub Konnektivität zur Infoblox-Appliance in der AWS Cloud oder On-Premises erfordert und AWS Lambda verwendet, um die Infoblox-API aufzurufen. Der Spoke befindet sich in demselben oder einem anderen Konto in derselben Organisation in AWS Organizations und ruft die Lambda-Funktion mithilfe einer CloudFormation benutzerdefinierten AWS-Ressource auf.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene Infoblox-Appliance oder ein vorhandenes Infoblox-Raster, die/das in der AWS Cloud, On-Premises oder beidem installiert und mit einem Administratorbenutzer konfiguriert ist, der IPAM- und DNS-Aktionen verwalten kann. Weitere Informationen dazu finden Sie unter Informationen zu Administratorkonten in der Infoblox-Dokumentation.
- Eine vorhandene autoritative DNS-Zone, die Sie Datensätze auf der Infoblox-Appliance hinzufügen möchten. Weitere Informationen dazu finden Sie unter Konfigurieren autoritativer Zonen in der Infoblox-Dokumentation.
- Zwei aktive AWS-Konten in AWS Organizations. Ein Konto ist das Hub-Konto und das andere Konto ist das Spoke-Konto.
- Die Hub- und Spoke-Konten müssen sich in derselben AWS-Region befinden.
- Die VPC des Hub-Kontos muss sich mit der Infoblox-Appliance verbinden, z. B. mithilfe von AWS Transit Gateway oder VPC-Peering.
- AWS Serverless Application Model (AWS SAM), lokal installiert und konfiguriert mit AWS Cloud9 oder AWS CloudShell.
- Die `ClientTest.yaml` Dateien `Infoblox-Hub.zip` und (angefügt), die in die lokale Umgebung heruntergeladen wurden, die AWS SAM enthält.

Einschränkungen

- Das Service-Token der CloudFormation benutzerdefinierten AWS-Ressource muss aus derselben Region stammen, in der der Stack erstellt wird. Wir empfehlen Ihnen, in jeder Region ein Hub-Konto zu verwenden, anstatt ein Amazon Simple Notification Service (Amazon SNS)-Thema in einer Region zu erstellen und die Lambda-Funktion in einer anderen Region aufzurufen.

Produktversionen

- Infoblox WAPI Version 2.7

Architektur

Die folgenden Diagramme zeigen den Workflow dieses Musters.

Das Diagramm zeigt die folgenden Komponenten für die Lösung dieses Musters:

1. Mit CloudFormation benutzerdefinierten AWS-Ressourcen können Sie benutzerdefinierte Bereitstellungslogik in Vorlagen schreiben, die AWS beim Erstellen, Aktualisieren oder Löschen von Stacks CloudFormation ausführt. Wenn Sie einen Stack erstellen, CloudFormation sendet AWS eine `create` Anforderung an ein SNS-Thema, das von einer Anwendung überwacht wird, die auf einer EC2-Instance ausgeführt wird.
2. Die Amazon SNS-Benachrichtigung der CloudFormation benutzerdefinierten AWS-Ressource wird mit einem bestimmten AWS Key Management Service (AWS KMS)-Schlüssel verschlüsselt und der Zugriff ist auf Konten in Ihrer Organisation in Organizations beschränkt. Das SNS-Thema initiiert die Lambda-Ressource, die die Infoblox-WAPI aufruft.
3. Amazon SNS ruft die folgenden Lambda-Funktionen auf, die die Infoblox WAPI-URL, den Benutzernamen und das Passwort AWS Secrets Manager Amazon Resource Names (ARNs) als Umgebungsvariablen verwenden:
   - `dnsapi.lambda_handler` – empfängt die `DNSValue` Werte `DNSNameDNSType`, und von der CloudFormation benutzerdefinierten AWS-Ressource und verwendet diese zum Erstellen von DNS A-Datensätzen und CNAMES.
   - `ipaddr.lambda_handler` – empfängt die `Network Name` Werte `VPCCIDR`, `Type`, und von der CloudFormation benutzerdefinierten AWS-Ressource und verwendet dieses`SubnetPrefix`, um die Netzwerkdaten zur Infoblox IPAM-Datenbank hinzuzufügen oder der benutzerdefinierten Ressource das nächste verfügbare Netzwerk zur Verfügung zu stellen, das zum Erstellen neuer Subnetze verwendet werden kann.

- `describeprefixes.lambda_handler` – Ruft die `describe_managed_prefix_lists` AWS-API mithilfe des `"com.amazonaws."+Region+".s3"` Filters auf, um die erforderliche abzurufen`prefix ID`.

  Wichtig: Diese Lambda-Funktionen sind in Python geschrieben und ähneln einander, rufen aber unterschiedliche APIs auf.

4. Sie können das Infoblox-Raster als physische, virtuelle oder cloudbasierte Netzwerkgeräte bereitstellen. Es kann On-Premises oder als virtuelle Appliance mit einer Reihe von Hypervisoren bereitgestellt werden, darunter VMware ESXi , Microsoft Hyper-V, Linux KVM und Xen. Sie können das Infoblox-Raster auch mit einem Amazon Machine Image (AMI) in der AWS Cloud bereitstellen.
5. Das Diagramm zeigt eine Hybridlösung für das Infoblox-Raster, die DNS und IPAM für Ressourcen in der AWS Cloud und On-Premises bereitstellt.

Technologie-Stack

- AWS CloudFormation
- IAM
- AWS KMS
- AWS Lambda
- AWS SAM
- AWS Secrets Manager
- Amazon SNS
- Amazon VPC

Tools

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie zentral erstellen und verwalten.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie Serverless-Anwendungen in der AWS Cloud erstellen können.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Code

Sie können die AWS-`ClientTest.yaml`Beispiel CloudFormation vorlage (angefügt) verwenden, um den Infoblox-Hub zu testen. Sie können die AWS- CloudFormation Vorlage so anpassen, dass sie die benutzerdefinierten Ressourcen aus der folgenden Tabelle enthält.

Erstellen eines A-Datensatzes mit der benutzerdefinierten Infoblox-Spoke-Ressource	Rückgabewerte:
	`infobloxref` – Infoblox-Referenzen
	Beispielressource :
	`ARECORDCustomResource:`
	`  Type: "Custom::InfobloxAPI"`
	`  Properties:`

```
    ServiceToken: !Sub  arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfobloxDNSFunction

    DNSName: 'arecordtest.compa
ny.com'

    DNSType: 'ARecord'

    DNSValue: '10.0.0.1'
```

Erstellen eines CNAME-Datensatzes mit der benutzerdefinierten Infoblox-Spoke-Ressource

Rückgabewerte:

`infobloxref` – Infoblox-Referenzen

Beispielressource :

```
CNAMECustomResource:

  Type: "Custom::InfobloxAPI"

  Properties:

    ServiceToken: !Sub arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfoblox

    DNSFunction

    DNSName: 'cnametest.company.com'

    DNSType: 'cname'

    DNSValue: 'aws.amazon.com'
```

Erstellen eines Netzwerkobjekts mit der benutzerdefinierten Infoblox-Spoke-Ressource	Rückgabewerte:
	`infobloxref` – Infoblox-Referenzen
	`network` – Netzwerkbereich (wie `VPCCIDR`)
	Beispielressource:
	`VPCCustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: VPC`
	`  NetworkName: My-VPC`

Rufen Sie das nächste verfügbare Subnetz mit der benutzerdefinierten Infoblox-Spoke-Res source ab	Rückgabewerte:
	`infobloxref` – Infoblox-Referenzen
	`network` – Der Netzwerkbereich des Subnetzes
	Beispielressource:
	`Subnet1CustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  DependsOn: VPCCustomResource`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: Subnet`
	`  SubnetPrefix: !Ref SubnetPrefix`
	`NetworkName: My-Subnet`

Polen

Erstellen und Konfigurieren der VPC des Hub-Kontos

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC mit einer Verbindung zur Infoblox-Appliance.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Hub-Konto an und erstellen Sie eine VPC, indem Sie die	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schritte in der Amazon VPC in der AWS Cloud Quick Start-Referenzbereitstellung von AWS Quick Starts ausführen. Wichtig: Die VPC muss über HTTPS-Konnektivität mit der Infoblox-Appliance verfügen, und wir empfehlen, für diese Verbindung ein privates Subnetz zu verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erstellen Sie die VPC-Endpunkte für private Subnetze.	VPC-Endpunkte bieten Konnektivität zu öffentlichen -Services für Ihre privaten Subnetze. Die folgenden Endpunkte sind erforderlich: • Ein Gateway-Endpunkt für Amazon Simple Storage Service (Amazon S3), um Lambda die Kommunikation mit AWS zu ermöglichen CloudFormation • Ein Schnittstellenendpunkt für Secrets Manager, um die Konnektivität mit Secrets Manager zu ermöglichen • Ein Schnittstellenendp unkt für AWS KMS, um die Verschlüsselung des SNS-Themas und Secrets-Manager-Secrets zu ermöglichen Weitere Informationen zum Erstellen von Endpunkten für private Subnetze finden Sie unter VPC-Endpunkte in der Amazon-VPC-Dokumentation.	Netzwerkadministrator, Systemadministrator

Bereitstellen des Infoblox-Hubs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS SAM-Vorlage.	1. Führen Sie den `unzip Infoblox-Hub.zip` Befehl in der Umgebung aus, die AWS SAM enthält. 2. Führen Sie den `cd Hub/` Befehl aus, um Ihr Verzeichnis in das Hub Verzeichnis zu ändern. 3. Führen Sie den `sam build` Befehl aus, um die AWS SAM-Vorlagendatei, den Anwendungscode und alle sprachspezifischen Dateien und Abhängigkeiten zu verarbeiten. Der `sam build` Befehl kopiert auch Build-Artefakte im Format und an der Stelle, die für die folgende Geschichte erwartet werden.	Entwickler, Systemadministrator
Stellen Sie die AWS SAM-Vorlage bereit.	Der `sam deploy` Befehl nimmt die erforderlichen Parameter und speichert sie in der `samconfig.toml` Datei , speichert die AWS-CloudFormation Vorlage und die Lambda-Funktionen in einem S3-Bucket und stellt die AWS- CloudFormation	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Vorlage dann in Ihrem Hub-Konto bereit.
	
	Der folgende Beispielcode zeigt, wie Sie die AWS SAM-Vorlage bereitstellen:
	
	`$ sam deploy --guided`
	
	`Configuring SAM deploy`
	`==========`
	`==`
	`Looking for config file [samconfig.toml] : Found`
	`Reading default arguments : Success`
	`Setting default arguments for 'sam deploy'`
	`==========`
	`==========`
	`Stack Name [Infoblox-Hub]:`
	`AWS Region [eu-west-1]:`
	`Parameter InfobloxUsername:`
	`Parameter InfobloxPassword:`
	`Parameter InfobloxIPAddress [xxx.xxx.xx.xxx]:`
	`Parameter AWSOrganisationID [o-xxxxxxxxx]:`
	`Parameter VPCID [vpc-xxxxxxxxx]:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Parameter VPCCIDR [xxx.xxx.xxx.xxx/16]: Parameter VPCSubnetID1 [subnet-xxx]: Parameter VPCSubnetID2 [subnet-xxx]: Parameter VPCSubnetID3 [subnet-xxx]: Parameter VPCSubnetID4 []: #Shows you resources changes to be deployed and require a 'Y' to initiate deploy Confirm changes before deploy [Y/n]: y #SAM needs permission to be able to create roles to connect to the resources in your template Allow SAM CLI IAM role creation [Y/n]: n Capabilities [['CAPABILITY_NAMED_IAM']]: Save arguments to configuration file [Y/n]: y SAM configuration file [samconfig.toml]: SAM configuration environment [default]:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wichtig: Sie müssen die `--guided` Option jedes Mal verwenden, da die Anmeldeinformationen für Infoblox nicht in der `samconfig.toml` Datei gespeichert sind.	

Zugehörige Ressourcen

- Erste Schritte mit WAPIs unter Verwendung von Postman (Infoblox-Blog)
- Bereitstellen von vNIOS für AWS unter Verwendung des BYOL-Modells (Infoblox-Dokumentation)
- quickstart-aws-vpc (GitHub Repository)
- describe_managed_prefix_lists (Dokumentation zum AWS SDK für Python)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Anpassen von Amazon- CloudWatch Warnungen für AWS Network Firewall

Erstellt von Jason Owens (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Netzwerk, Sicherheit, Identität, Compliance	Workload: Open-Source
AWS-Services: Amazon CloudWatch Logs; AWS Network Firewall; AWS CLI		

Übersicht

Das Muster hilft Ihnen dabei, die Amazon- CloudWatch Warnungen anzupassen, die von der Amazon Web Services (AWS) Network Firewall generiert werden. Sie können vordefinierte Regeln verwenden oder benutzerdefinierte Regeln erstellen, die die Nachricht, Metadaten und den Schweregrad der Warnungen bestimmen. Sie können dann auf diese Warnungen reagieren oder Antworten von anderen Amazon-Services wie Amazon automatisieren EventBridge.

In diesem Muster generieren Sie Suricata-kompatible Firewall-Regeln. Suricata ist eine Open-Source-Engine zur Bedrohungserkennung. Sie erstellen zunächst einfache Regeln und testen sie dann, um zu bestätigen, dass die CloudWatch Warnungen generiert und protokolliert werden. Sobald Sie die Regeln erfolgreich getestet haben, ändern Sie sie, um benutzerdefinierte Nachrichten, Metadaten und Schweregrade zu definieren, und testen Sie dann erneut, um die Aktualisierungen zu bestätigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI) ist auf Ihrer Linux-, macOS- oder Windows-Workstation installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren oder Aktualisieren der neuesten Version der AWS CLI.

- AWS Network Firewall installiert und für die Verwendung von - CloudWatch Protokollen konfiguriert. Weitere Informationen finden Sie unter Protokollieren des Netzwerkverkehrs von AWS Network Firewall.
- Eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance in einem privaten Subnetz einer Virtual Private Cloud (VPC), die durch Network Firewall geschützt ist.

Produktversionen

- Verwenden Sie für Version 1 der AWS CLI 1.18.180 oder höher. Verwenden Sie für Version 2 der AWS CLI 2.1.2 oder höher.
- Die Datei classification.config aus Suricata Version 5.0.2. Eine Kopie dieser Konfigurationsdatei finden Sie im Abschnitt Zusätzliche Informationen.

Architektur

Zieltechnologie-Stack

- Network Firewall
- Amazon CloudWatch -Protokolle

Zielarchitektur

Das Architekturdiagramm zeigt den folgenden Workflow:

1. Eine EC2-Instance in einem privaten Subnetz stellt eine -Anforderung, indem sie entweder curl oder Wget verwendet.
2. Network Firewall verarbeitet den Datenverkehr und generiert eine Warnung.
3. Network Firewall sendet die protokollierten Warnungen an CloudWatch Logs.

Tools

AWS-Services

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.

- Amazon CloudWatch Logs hilft Ihnen, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, damit Sie sie überwachen und sicher archivieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Network Firewall ist eine zustandsbehaftete, verwaltete Netzwerk-Firewall sowie ein Service zur Erkennung und Verhinderung von Eindringlingen für Virtual Private Clouds (VPCs) in der AWS Cloud.

Andere Tools und Services

- curl – curl ist ein Open-Source-Befehlszeilentool und eine Bibliothek.
- Wget – GNU Wget ist ein kostenloses Befehlszeilen-Tool.

Polen

Erstellen der Firewall-Regeln und Regelgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen von Regeln.	1. Erstellen Sie in einem Texteditor eine Liste von Regeln, die Sie der Firewall hinzufügen möchten. Jede Regel muss sich in einer separaten Zeile befinden. Der Wert im `classtype` Parameter stammt aus der standardm äßigen Suricata-Klassifiz ierungskonfigurationsdatei. Den vollständigen Inhalt der Konfigurationsdate i finden Sie im Abschnitt Zusätzliche Informationen. Im Folgenden finden Sie zwei Beispiele für -Regeln.	AWS-Systemadministrator, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>alert http any
	 any -> any any
	 (content:"badstuff
	"; classtype:misc-
	activity; sid:3;
	 rev:1;)
	alert http any any
	 -> any any (content:
	"morebadstuff";
	 classtype:bad-unkn
	own; sid:4; rev:1;)</pre>
	2. Speichern Sie die Regeln in einer Datei mit dem Namen `custom.rules` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Regelgruppe.	Geben Sie in der AWS CLI den folgenden Befehl ein. Dadurch wird die Regelgruppe erstellt.
	`# aws network-firewall create-rule-group \ --rule-group-name custom --type STATEFUL \ --capacity 10 --rules file://custom.rules \ --tags Key=environment,Value=development`
	Im Folgenden finden Sie eine Beispielausgabe. Notieren Sie sich die `RuleGroupArn` , die Sie in einem späteren Schritt benötigen.
	`{ "UpdateToken": "4f998d72-973c-490a-bed2-fc3460547e23", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b",`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Type": "STATEFUL",
	"Capacity": 10,
	"RuleGroupStatus": "ACTIVE",
	"Tags": [
	{
	"Key": "environment",
	"Value": "development"
	}
	]
	}</pre>	

Aktualisieren der Firewall-Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie den ARN der Firewall-Richtlinie ab.	Geben Sie in der AWS CLI den folgenden Befehl ein. Dadurch wird der Amazon-Ressourcenname (ARN) der Firewall-Richtlinie zurückgegeben. Notieren Sie den ARN zur Verwendung später in diesem Muster.
	<pre># aws network-firewall describe-firewall \
	--firewall-name aws-network-firewall-anfw \
	--query 'Firewall.FirewallPolicyArn'</pre>
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Im Folgenden finden Sie ein Beispiel für einen ARN, der von diesem Befehl zurückgeg eben wird. `"arn:aws:network-firewall:us-east-2:1234567890:firewall-policy/firewall-policy-anfw"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Firewall-Richtlinie.	Kopieren Sie in einem Texteditor den folgenden Code. Ersetzen Sie durch `<RuleGroupArn>` den Wert, den Sie im vorherige n Epi aufgezeichnet haben. Speichern Sie die Datei als `firewall-policy-an fw.json` . `{ "StatelessDefaultA ctions": [ "aws:forw ard_to_sfe" ], "StatelessFragment DefaultActions": [ "aws:forw ard_to_sfe" ], "StatefulRuleGroup References": [ { "Resource Arn": "<RuleGroupArn>" } ] }` Geben Sie den folgenden Befehl in die AWS CLI ein. Dieser Befehl erfordert ein Aktualisierungstoken, um die neuen Regeln hinzuzufügen. Das Token wird verwendet, um zu bestätigen, dass sich	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die Richtlinie seit dem letzten Abruf nicht geändert hat.
	
	`UPDATETOKEN=(`aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --output text --query UpdateToken`)`
	
	`aws network-firewall update-firewall-policy \ --update-token $UPDATETOKEN \ --firewall-policy-name firewall-policy-anfw \ --firewall-policy file://firewall-policy-anfw.json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bestätigen Sie die Richtlini enaktualisierungen.	(Optional) Wenn Sie bestätige n möchten, dass die Regeln hinzugefügt wurden, und das Richtlinienformat anzeigen möchten, geben Sie den folgenden Befehl in die AWS CLI ein.
	`# aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --query FirewallPolicy`
	Im Folgenden finden Sie eine Beispielausgabe.
	`{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "arn:aws:network-firewall:us-east-2:123456789`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>0:stateful-rulegroup/
	custom"
	        }
	    ]
	}</pre>	

Testen der Warnfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Generieren Sie Warnungen zum Testen.	1. Melden Sie sich im Firewall-Subnetz an einer Testarbeitsstation an.
	2. Geben Sie Befehle ein, die Warnungen generieren sollen. Sie können beispielsweise `wget` oder verwenden`curl`.
	<pre>wget -U "badstuff"
	 http://www.amazon.
	com -o /dev/null</pre>
	<pre>curl -A "morebads
	tuff" http://ww
	w.amazon.com -o /
	dev/null</pre>
		AWS-Systemadministrator

Überprüfen Sie, ob die Warnungen protokolliert werden.	1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/ 2. Navigieren Sie zur richtigen Protokollgruppe und zum richtigen Stream. Weitere	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Informationen finden Sie unter An - CloudWatch Protokolle gesendete Protokolldaten anzeigen (CloudWatch Protokoll dokumentation).
	3. Vergewissern Sie sich, dass die protokollierten Ereignisse den folgenden Beispielen ähneln. Die Beispiele zeigen nur den relevanten Teil der Warnung.
	
	Beispiel 1
	
	`"alert": { "action": "allowed", "signature_id": 3, "rev": 1, "signature": "", "category": "Misc activity", "severity": 3 }`
	
	Beispiel 2
	
	`"alert": { "action": "allowed", "signature_id": 4, "rev": 1,`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"signatur
	e": "",
	"category
	": "Potentially Bad
	 Traffic",
	"severity
	": 2
	}</pre>	

Aktualisieren der Firewall-Regeln und Regelgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die Firewall-Regeln.	1. Öffnen Sie die Datei `custom.rules` in einem Texteditor.
	2. Ändern Sie die erste Regel so, dass sie der folgenden ähnelt. Diese Regel muss in einer einzelnen Zeile in der Datei eingegeben werden.
	<pre>alert http any any ->
	 any any (msg:"Watch
	 out - Bad Stuff!!";
	 content:"badstuff"
	; classtype:misc-
	activity; priority:
	2; sid:3; rev:2;
	 metadata:custom-
	field-2 Danger!,
	 custom-field More
	 Info;)</pre>
	Dadurch werden die folgenden Änderungen an der Regel vorgenommen:
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Fügt eine msg-Zeichenfolge (Suricata-Website) hinzu, die Textinformationen über die Signatur oder Warnung bereitstellt. In der generierten Warnung entspricht dies der Signatur. • Passt die Standardpriorität (Suricata-Website) von `misc-activity` von von 3 auf 2 an. Die Standardwerte der verschiedenen `classtypes` finden Sie im Abschnitt Zusätzliche Informationen. • Fügt der Warnung benutzerdefinierte Metadaten (Suricata-Website) hinzu. Dies sind zusätzliche Informationen, die der Signatur hinzugefügt werden. Es wird empfohlen, Schlüssel-Wert-Paare zu verwenden. • Ändert die Version (Suricata-Website) von 1 auf 2. Dies stellt die Version der Signatur dar.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Regelgruppe.	Führen Sie in der AWS CLI die folgenden Befehle aus. Verwenden Sie den ARN Ihrer Firewall-Richtlinie. Diese Befehle rufen ein Aktualisierungstoken ab und aktualisieren die Regelgruppe mit den Regeländerungen. `# UPDATETOKEN=(`aws network-firewall \ describe-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:123457890:stateful-rulegroup/custom \ --output text --query UpdateToken`)` `# aws network-firewall update-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom \ --rules file://custom.rules \ --update-token $UPDATETOKEN` Im Folgenden finden Sie eine Beispielausgabe. `{`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"UpdateToken": "7536939f-6a1d-414c-96d1-bb28110996ed", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] } }	

Testen der aktualisierten Warnfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie eine Warnung zum Testen.	1. Melden Sie sich im Firewall-Subnetz an einer Testarbeitsstation an.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie einen Befehl ein, der eine Warnung generieren soll. Sie können beispielsweise die Datei `curl` verwenden. `curl -A "badstuff" http://www.amazon.com -o /dev/null`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob die Warnung geändert wurde.	1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/ 2. Navigieren Sie zur richtigen Protokollgruppe und zum richtigen Stream. 3. Vergewissern Sie sich, dass das protokollierte Ereignis dem folgenden Beispiel ähnelt. Das Beispiel zeigt nur den relevanten Teil der Warnung. `"alert": { "action": "allowed", "signature_id": 3, "rev": 2, "signature": "Watch out - Bad Stuff!!", "category": "Misc activity", "severity": 2, "metadata": { "custom-field": [ "More Info" ], "custom-field-2": [ "Danger!" ] }`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	}	

Zugehörige Ressourcen

Referenzen

- Senden von Warnungen von AWS Network Firewall an einen Slack-Kanal (AWS Prescriptive Guidance)
- Skalieren der Bedrohungsprävention in AWS mit Suricata (AWS-Blogbeitrag)
- Bereitstellungsmodelle für AWS Network Firewall (AWS-Blogbeitrag)
- Suricata-Meta-Keyworks (Suricata-Dokumentation)

Tutorials und Videos

- AWS Network Firewall-Workshop

Zusätzliche Informationen

Im Folgenden finden Sie die Klassifizierungskonfigurationsdatei aus Suricata 5.0.2. Diese Klassifizierungen werden beim Erstellen der Firewall-Regeln verwendet.

```
# config classification:shortname,short description,priority

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1
```

```
# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
config classification: suspicious-login,An attempted login using a suspicious username
 was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
config classification: unusual-client-port-connection,A client was using an unusual
 port,2
config classification: network-scan,Detection of a Network Scan,3
config classification: denial-of-service,Detection of a Denial of Service Attack,2
config classification: non-standard-protocol,Detection of a non-standard protocol or
 event,2
config classification: protocol-command-decode,Generic Protocol Command Decode,3
config classification: web-application-activity,access to a potentially vulnerable web
 application,2
config classification: web-application-attack,Web Application Attack,1
config classification: misc-activity,Misc activity,3
config classification: misc-attack,Misc Attack,2
config classification: icmp-event,Generic ICMP event,3
config classification: inappropriate-content,Inappropriate Content was Detected,1
config classification: policy-violation,Potential Corporate Privacy Violation,1
config classification: default-login-attempt,Attempt to login by a default username and
 password,2

# Update
config classification: targeted-activity,Targeted Malicious Activity was Detected,1
config classification: exploit-kit,Exploit Kit Activity Detected,1
config classification: external-ip-check,Device Retrieving External IP Address
 Detected,2
config classification: domain-c2,Domain Observed Used for C2 Detected,1
config classification: pup-activity,Possibly Unwanted Program Detected,2
config classification: credential-theft,Successful Credential Theft Detected,1
config classification: social-engineering,Possible Social Engineering Attempted,2
config classification: coin-mining,Crypto Currency Mining Activity Detected,2
config classification: command-and-control,Malware Command and Control Activity
 Detected,1
```

Migrieren Sie DNS-Datensätze in großen Mengen in eine privat gehostete Zone von Amazon Route 53

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Netzwerk; Cloudnativ; DevOpsInfrastruktur	AWS-Services: AWS Cloud9; Amazon Route 53; Amazon S3

Übersicht

Netzwerkingenieure und Cloud-Administratoren benötigen eine effiziente und einfache Möglichkeit, DNS-Datensätze (Domain Name System) zu privat gehosteten Zonen in Amazon Route 53 hinzuzufügen. Die Verwendung eines manuellen Ansatzes zum Kopieren von Einträgen aus einem Microsoft-Excel-Speicherort an die entsprechenden Speicherorte in der Route 53-Konsole ist mühsam und fehleranfällig. Dieses Muster beschreibt einen automatisierten Ansatz, der den Zeit- und Arbeitsaufwand für das Hinzufügen mehrerer Datensätze reduziert. Es bietet auch einen wiederholbaren Satz von Schritten für die Erstellung mehrerer gehosteter Zonen.

Dieses Muster verwendet die integrierte Entwicklungsumgebung (IDE) von AWS Cloud9 für Entwicklung und Tests und Amazon Simple Storage Service (Amazon S3) zum Speichern von Datensätzen. Um effizient mit Daten zu arbeiten, verwendet das Muster aufgrund seiner Einfachheit und seiner Fähigkeit, ein Python-Wörterbuch (`dict`-Datentyp) zu unterstützen, das JSON-Format.

Hinweis: Wenn Sie eine Zonendatei aus Ihrem System generieren können, sollten Sie stattdessen die Route 53-Importfunktion verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Excel-Arbeitsmaterial, das private Datensätze für gehostete Zonen enthält
- Vertrautheit mit verschiedenen Arten von DNS-Datensätzen wie A-Datensatz, Name Authority Pointer (NAPTR)-Datensatz und SRV-Datensatz (siehe Unterstützte DNS-Datensatztypen)
- Vertrautheit mit der Python-Sprache und ihren Bibliotheken

Einschränkungen

- Das Muster bietet nicht für alle Anwendungsfallszenarien eine umfassende Abdeckung. Der Aufruf change_resource_record_sets verwendet beispielsweise nicht alle verfügbaren Eigenschaften der API.
- Im Excel-Ensemble wird davon ausgegangen, dass der Wert in jeder Zeile eindeutig ist. Es wird erwartet, dass mehrere Werte für jeden vollqualifizierten Domainnamen (FQDN) in derselben Zeile erscheinen. Wenn dies nicht zutrifft, sollten Sie den in diesem Muster angegebenen Code ändern, um die erforderliche Verkettung durchzuführen.
- Das Muster verwendet das AWS SDK for Python (Boto3), um den Route 53-Service direkt aufzurufen. Sie können den Code erweitern, um einen AWS- CloudFormation Wrapper für die `update_stack` Befehle `create_stack` und zu verwenden, und die JSON-Werte verwenden, um Vorlagenressourcen zu füllen.

Architektur

Technologie-Stack

- Privat gehostete Route 53-Zonen zum Weiterleiten von Datenverkehr
- AWS Cloud9 IDE für Entwicklung und Tests
- Amazon S3 zum Speichern der JSON-Ausgabedatei

Der Workflow besteht aus diesen Schritten, wie im vorherigen Diagramm dargestellt und im Abschnitt „Epics“ erörtert:

1. Laden Sie ein Excel-Kabel mit den Datensatzinformationen in einen S3-Bucket hoch.
2. Erstellen und führen Sie ein Python-Skript aus, das die Excel-Daten in das JSON-Format konvertiert.
3. Lesen Sie die Datensätze aus dem S3-Bucket und bereinigen Sie die Daten.
4. Erstellen Sie Datensätze in Ihrer privat gehosteten Zone.

Tools

- Route 53 – Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Webservice, der Domänenregistrierung, DNS-Routing und Zustandsprüfungen übernimmt.
- AWS Cloud9 – AWS Cloud9 ist eine IDE, die eine umfassende Codebearbeitungserfahrung mit Unterstützung für mehrere Programmiersprachen und Laufzeit-Debugger sowie ein integriertes Terminal bietet. Es enthält eine Sammlung von Tools, die Sie verwenden, um Software zu codieren, zu erstellen, auszuführen, zu testen und zu debuggen, und Ihnen hilft, Software in der Cloud zu veröffentlichen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.

Polen

Daten für die Automatisierung vorbereiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Excel-Datei für Ihre Datensätze.	Verwenden Sie die Datensätze, die Sie aus Ihrem aktuellen System exportiert haben, um einen Excel-Ausschnitt zu erstellen, der die erforderlichen Spalten für einen Datensatz enthält, z. B. vollqualifizierter Domainname (FQDN), Datensatztyp, Time to Live (TTL) und Wert. Für NAPTR- und SRV-Datensätze ist der Wert eine Kombination aus mehreren Eigenschaften. Verwenden Sie daher die Excel-`concat`Methode, um diese Eigenschaften zu kombinieren.	Dateningenieur, Excel-Fähigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	FqdnN Recor Wert TTL e somet A 1.1.1.1 900 .exam org	

Überprüfen Sie die Arbeitsumgebung.	Erstellen Sie in der AWS Cloud9 IDE eine Python-Datei, um das Excel-Eingabefragment in das JSON-Format zu konvertieren. (Statt AWS Cloud9 können Sie auch ein Amazon- SageMaker Notebook verwenden, um mit Python-Code zu arbeiten.)
	
	Stellen Sie sicher, dass die Python-Version, die Sie verwenden, Version 3.7 oder höher ist.
	
	`python3 --version`
	
	Installieren Sie das Pandas-Paket.
	
	`pip3 install pandas --user`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konvertieren Sie die Excel-Kabeldaten in JSON.	Erstellen Sie eine Python-Datei, die den folgenden Code enthält, um von Excel in JSON zu konvertieren.
	`import pandas as pd`
	`data=pd.read_excel('./Book1.xls')`
	`data.to_json(path_or_buf='my.json', orient='records')`
	Dabei `Book1` ist der Name des Excel-Koordinatens und `my.json` der Name der Ausgabe-JSON-Datei.
		Dateningenieur, Python-Fähigkeiten

Laden Sie die JSON-Datei in einen S3-Bucket hoch.	Laden Sie die Datei `my.json` zu einem S3-Bucket hoch. Weitere Informationen finden Sie unter Erstellen eines Buckets in der Amazon S3-Dokumentation.	App-Developer

Datensätze einfügen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine privat gehostete Zone.	Verwenden Sie die create_hosted_zone-API und den folgenden Python-Beispielcode, um eine privat gehostete Zone zu erstellen. Ersetzen Sie die Parameter `hostedZoneName` , `vpcRegion` und	Cloud-Architekt, Netzwerkadministrator, Python-Fähigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`vpcId` durch Ihre eigenen Werte.
	
	`import boto3`
	`import random`
	`hostedZoneName ="xxx"`
	`vpcRegion = "us-east-1"`
	`vpcId="vpc-xxxx"`
	`route53_client = boto3.client('route53')`
	`response = route53_client.create_hosted_zone(`
	`Name= hostedZoneName,`
	`VPC={`
	`'VPCRegion: vpcRegion,`
	`'VPCId': vpcId`
	`},`
	`CallerReference=str(random.random()*100000),`
	`HostedZoneConfig={`
	`'Comment': "private hosted zone created by automation",`
	`'PrivateZone': True`
	`}`
	`)`
	`print(response)`
	
	Sie können auch ein Infrastructure as Code (IaC)-Tool wie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS verwenden, CloudFormation um diese Schritte durch eine Vorlage zu ersetzen, die einen Stack mit den entsprechenden Ressourcen und Eigenschaften erstellt.	
Rufen Sie Details als Wörterbuch von Amazon S3 ab.	Verwenden Sie den folgenden Code, um aus dem S3-Bucket zu lesen und die JSON-Werte als Python-Wörterbuch abzurufen. `fileobj = s3_client.get_object( Bucket=bucket_name, Key='my.json' ) filedata = fileobj['Body'].read() contents = filedata.decode('utf-8') json_content=json.loads(contents) print(json_content)` wobei das Python-Wörterbuch `json_content` enthält.	App-Entwickler, Python-Fähigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen Sie Datenwerte für Leerzeichen und Unicode-Zeichen.	Verwenden Sie als Sicherheitsmaßnahme zur Sicherstellung der Richtigkeit der Daten den folgenden Code, um eine Entfernungsoperation für die Werte in durchzuführen `json_content` . Dieser Code entfernt die Leerzeichen am Anfang und am Ende jeder Zeichenfolge. Es verwendet auch die -`replace`Methode, um harte (nicht störende) Leerzeichen (die `\xa0` Zeichen) zu entfernen.
	
	`for item in json_content:`
	`  fqn_name = unicodedata.normalize("NFKD",item["FqdnName"].replace("u'", "'").replace('\xa0', '').strip())`
	`  rec_type = item["RecordType"].replace('\xa0', '').strip()`
	`  res_rec = {`
	
	`  'Value': item["Value"].replace('\xa0', '').strip()`
	`  }`
		App-Entwickler, Python-Fähigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Datensätze ein.	Verwenden Sie den folgenden Code als Teil der vorherigen `for` Schleife. `change_response = route53_client.change_resource_record_sets( HostedZoneId="xxxxxxxx", ChangeBatch={ 'Comment': 'Created by automation', 'Changes': [ { 'Action': 'UPSERT', 'ResourceRecordSet': { 'Name': fqn_name, 'Type': rec_type, 'TTL': item["TTL"], 'ResourceRecords': res_rec } } ] } )`	App-Entwickler, Python-Fähigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wobei die ID der gehosteten Zone aus dem ersten Schritt dieses Epics xxxxxxx ist.	

Zugehörige Ressourcen

Referenzen

- Erstellen von Datensätzen durch Importieren einer Zonendatei (Amazon Route 53-Dokumentation)
- create_hosted_zone-Methode (Boto3-Dokumentation)
- change_resource_record_sets-Methode (Boto3-Dokumentation)

Tutorials und Videos

- Das Python-Tutorial (Python-Dokumentation)

- DNS-Design mit Amazon Route 53 (YouTube Video, AWS Online Tech Talks)

Ändern von HTTP-Headern bei der Migration von F5 zu einem Application Load Balancer in AWS

Erstellt von Sachin Trivedi (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: On-Premise	Ziel: AWS Cloud
R-Typ: Plattformwechsel	Workload: Alle anderen Workloads	Technologien: Netzwerk, Hybrid Cloud, Migration
AWS-Services: Amazon CloudFront; Elastic Load Balancing (ELB); AWS Lambda		

Übersicht

Wenn Sie eine Anwendung, die einen F5 Load Balancer verwendet, zu Amazon Web Services (AWS) migrieren und einen Application Load Balancer in AWS verwenden möchten, ist die Migration von F5-Regeln für Header-Änderungen ein häufiges Problem. Ein Application Load Balancer unterstützt keine Header-Änderungen, aber Sie können Amazon CloudFront als Content Delivery Network (CDN) und Lambda@Edge verwenden, um Header zu ändern.

Dieses Muster beschreibt die erforderlichen Integrationen und bietet Beispielcode für die Header-Änderung mithilfe von AWS CloudFront und Lambda@Edge.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine On-Premises-Anwendung, die einen F5-Load Balancer mit einer Konfiguration verwendet, die den HTTP-Header-Wert mithilfe von ersetzt`if, else`. Weitere Informationen zu dieser Konfiguration finden Sie unter HTTP::header in der F5-Produktdokumentation.

Einschränkungen

- Dieses Muster gilt für die F5-Load-Balancer-Header-Anpassung. Informationen zur Unterstützung finden Sie in der Load Balancer-Dokumentation anderer Load Balancer von Drittanbietern.
- Die Lambda-Funktionen, die Sie für Lambda@Edge verwenden, müssen sich in der Region USA Ost (Nord-Virginia) befinden.

Architektur

Das folgende Diagramm zeigt die Architektur in AWS, einschließlich des Integrationsablaufs zwischen dem CDN und anderen AWS-Komponenten.

Tools

AWS-Services

- Application Load Balancer – Ein Application Load Balancer ist ein vollständig verwalteter AWS-Load-Balancing-Service, der auf der siebten Ebene des Open Systems Interconnection (OSI)-Modells funktioniert. Es gleicht den Datenverkehr über mehrere Ziele aus und unterstützt erweiterte Routing-Anforderungen basierend auf HTTP-Headern und -Methoden, Abfragezeichenfolgen und hostbasiertem oder pfadbasiertem Routing.
- Amazon CloudFront – Amazon CloudFront ist ein Webservice, der die Verteilung Ihrer statischen und dynamischen Webinhalte wie HTML-, CSS-, .js- und Image-Dateien für Ihre Benutzer beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden, um eine geringere Latenz und verbesserte Leistung zu erzielen.
- Lambda@Edge Bol Lambda@Edge ist eine Erweiterung von AWS Lambda, mit der Sie Funktionen ausführen können, um den Inhalt anzupassen, der CloudFront bereitstellt. Sie können Funktionen in der Region USA Ost (Nord-Virginia) erstellen und die Funktion dann einer CloudFront Verteilung zuordnen, um Ihren Code automatisch auf der ganzen Welt zu replizieren, ohne Server bereitstellen oder verwalten zu müssen. Dies reduziert die Latenz und verbessert die Benutzererfahrung.

Code

Der folgende Beispielcode bietet eine Vorlage zum Ändern von CloudFront Antwort-Headern. Folgen Sie den Anweisungen im Abschnitt „Epics“, um den Code bereitzustellen.

```
exports.handler = async (event, context) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;


    const headerNameSrc = 'content-security-policy';
    const headerNameValue = '*.xyz.com';


    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
        }];
        console.log(`Response header "${headerNameSrc}" was set to ` +
                    `"${headers[headerNameSrc.toLowerCase()][0].value}"`);
    }
    else {
            headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
            }];
    }
    return response;
};
```

Polen

Erstellen einer CDN-Verteilung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFront Web-Verteilung.	In diesem Schritt erstellen Sie eine - CloudFront Verteilung, um mitzuteilen, von CloudFron t wo aus Inhalte bereitges tellt werden sollen, sowie die Details zur Nachverfolgung und Verwaltung der Bereitste llung von Inhalten.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um eine Verteilung mithilfe der Konsole zu erstellen, melden Sie sich bei der AWS-Manag ementkonsole an, öffnen Sie die CloudFront Konsole und folgen Sie dann den Schritten in der CloudFront Dokumenta tion .	

Erstellen und Bereitstellen der Lambda@Edge-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und Bereitstellen einer Lambda@Edge-Funkti on.	Sie können eine Lambda@Ed ge-Funktion erstellen, indem Sie einen Blueprint zum Ändern von CloudFront Antwort-Headern verwenden . (Andere bluePrints sind für verschiedene Anwendung sfälle verfügbar. Weitere Informationen finden Sie unter Lambda@Edge-Beispielfunktionen in der - CloudFront Dokumentation.) So erstellen Sie eine Lambda@Edge-Funktion: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Lambda-Konsole unter https://console.aws.amazon .com/lambda/.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Stellen Sie sicher, dass Sie sich in der Region USA Ost (Nord-Virginia) befinden. CloudFront Blueprints sind nur in dieser Region verfügbar. 3. Wählen Sie Funktion erstellen. 4. Wählen Sie Blueprint verwenden und geben Sie dann cloudfront in das Suchfeld Blueprints ein. 5. Wählen Sie den cloudfron t-modify-response-header Blueprint und dann Konfigurieren aus. 6. Geben Sie auf der Seite Grundlegende Informati onen die folgenden Informationen ein: a. Geben Sie einen Funktionsnamen ein. b. Wählen Sie unter Execution Role (Ausführungsrolle) die Option Create a new role from AWS policy templates (Neue Rolle aus AWS-Richtlinienvor lagen erstellen). c. Ordnen Sie den erforderl ichen AWS Identity and	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Access Management (IAM)-Rollennamen zu. 7. Wählen Sie Funktion erstellen. 8. Wählen Sie im Abschnitt Designer der Seite Ihren Funktionsnamen aus. 9. Ersetzen Sie im Abschnitt Funktionscode den Vorlagencode durch den Beispielcode, der zuvor in diesem Muster bereitgestellt wurde, im Abschnitt Code. 10. Ersetzen Sie im Beispielcode durch `xyz.com` Ihren Domänennamen. 11. Wählen Sie Speichern.	
Stellen Sie die Lambda@Edge-Funktion bereit.	Folgen Sie den Anweisungen in Schritt 4 des Tutorials: Erstellen einer einfachen Lambda@Edge-Funktion in der Amazon- CloudFront Dokumentation, um den CloudFront Auslöser zu konfigurieren und die Funktion bereitzustellen.	AWS-Administrator

Zugehörige Ressourcen

CloudFront -Dokumentation

- Verhalten von Anfragen und Antworten für benutzerdefinierte Ursprünge
- Arbeiten mit Verteilungen

- Lambda@Edge-Beispielfunktionen
- Anpassen am Edge mit Lambda@Edge
- Tutorial: Erstellen einer einfachen Lambda@Edge-Funktion

Privater Zugriff auf einen zentralen AWS-Service-Endpunkt aus mehreren VPCs

Erstellt von microSD Guenthner (AWS) und SamSpeed Gordon (AWS)

Code-Repository: VPC-Endpunktfreigabe	Umgebung: Produktion	Technologien: Netzwerk; Infrastruktur
AWS-Services: AWS RAM; Amazon Route 53; Amazon SNS ;AWS Transit Gateway; Amazon VPC		

Übersicht

Sicherheits- und Compliance-Anforderungen für Ihre Umgebung können darauf hinweisen, dass der Datenverkehr zu Amazon Web Services (AWS)-Services oder -Endpunkten nicht über das öffentliche Internet übertragen werden darf. Dieses Muster ist eine Lösung, die für eine hub-and-spoke Topologie entwickelt wurde, bei der eine zentrale Hub-VPC mit mehreren verteilten Spoke-VPCs verbunden ist. In dieser Lösung verwenden Sie AWS, PrivateLink um einen Schnittstellen-VPC-Endpunkt für den AWS-Service im Hub-Konto zu erstellen. Anschließend verwenden Sie Transit Gateways und eine verteilte DNS-Regel (Domain Name System), um Anforderungen an die private IP-Adresse des Endpunkts über die verbundenen VPCs aufzulösen.

Dieses Muster beschreibt, wie Sie AWS Transit Gateway , einen eingehenden Amazon Route 53 Resolver-Endpunkt und eine gemeinsame Route 53-Weiterleitungsregel verwenden, um die DNS-Abfragen von den Ressourcen in verbundenen VPCs aufzulösen. Sie erstellen den Endpunkt, das Transit Gateway, den Resolver und die Weiterleitungsregel im Hub-Konto. Anschließend verwenden Sie AWS Resource Access Manager (AWS RAM), um das Transit-Gateway und die Weiterleitungsregel für die Spoke-VPCs freizugeben. Die bereitgestellten AWS- CloudFormation Vorlagen helfen Ihnen bei der Bereitstellung und Konfiguration der Ressourcen in der Hub-VPC und Spoke-VPCs.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Hub-Konto und ein oder mehrere Spoke-Konten, die in derselben Organisation in AWS Organizations verwaltet werden. Weitere Informationen finden Sie unter Erstellen und Verwalten einer Organisation.
- AWS Resource Access Manager (AWS RAM) ist als vertrauenswürdiger Service in AWS Organizations konfiguriert. Weitere Informationen finden Sie unter Verwenden von AWS Organizations mit anderen AWS-Services.
- Die DNS-Auflösung muss im Hub und den Spoke-VPCs aktiviert sein. Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC (Dokumentation von Amazon Virtual Private Cloud).

Einschränkungen

- Dieses Muster verbindet Hub- und Spoke-Konten in derselben AWS-Region. Bei Bereitstellungen mit mehreren Regionen müssen Sie dieses Muster für jede Region wiederholen.
- Der AWS-Service muss PrivateLink als Schnittstellen-VPC-Endpunkt in integriert werden. Eine vollständige Liste finden Sie unter AWS-Services, die in AWS integriert sind PrivateLink (PrivateLink Dokumentation).
- Die Affinität zur Availability Zone ist nicht garantiert. Beispielsweise können Abfragen aus Availability Zone A mit einer IP-Adresse aus Availability Zone B antworten.
- Die dem VPC-Endpunkt zugeordnete Elastic Network-Schnittstelle hat ein Limit von 10.000 Abfragen pro Sekunde.

Architektur

Zieltechnologie-Stack

- Eine Hub-VPC im Hub-AWS-Konto
- Eine oder mehrere Spoke-VPCs in einem Spoke-AWS-Konto
- Ein oder mehrere Schnittstellen-VPC-Endpunkte im Hub-Konto
- Ein- und ausgehende Route 53 Resolver im Hub-Konto
- Eine Route 53-Resolver-Weiterleitungsregel, die im Hub-Konto bereitgestellt und mit dem Spoke-Konto geteilt wird
- Ein Transit-Gateway, das im Hub-Konto bereitgestellt und mit dem Spoke-Konto geteilt wird
- AWS Transit Gateway verbindet den Hub und Spoke-VPCs

Zielarchitektur

Die folgende Abbildung zeigt eine Beispielarchitektur für diese Lösung. In dieser Architektur hat die Route-53-Resolver-Weiterleitungsregel im Hub-Konto die folgende Beziehung zu den anderen Architekturkomponenten:

1. Die Weiterleitungsregel wird mithilfe von AWS RAM mit der Spoke-VPC geteilt.
2. Die Weiterleitungsregel ist dem ausgehenden Resolver in der Hub-VPC zugeordnet.
3. Die Weiterleitungsregel zielt auf den eingehenden Resolver in der Hub-VPC ab.

Die folgende Abbildung zeigt den Datenverkehrsfluss durch die Beispielarchitektur:

1. Eine Ressource, z. B. eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance, in der Spoke-VPC stellt eine DNS-Anfrage an `<service>.<region>.amazonaws.com`. Die Anforderung wird vom gesprochenen Amazon DNS Resolver empfangen.
2. Die Route 53-Weiterleitungsregel, die vom Hub-Konto gemeinsam genutzt und der Spoke-VPC zugeordnet wird, fängt die Anforderung ab.
3. In der Hub-VPC verwendet der ausgehende Resolver die Weiterleitungsregel, um die Anforderung an den eingehenden Resolver weiterzuleiten.
4. Der eingehende Resolver verwendet den Hub-VPC-Amazon-DNS-Resolver, um die IP-Adresse für in die private IP-Adresse eines VPC-Endpunkts `<service>.<region>.amazonaws.com` aufzulösen. Wenn kein VPC-Endpunkt vorhanden ist, wird er in die öffentliche IP-Adresse aufgelöst.

Tools

AWS-Tools und -Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und sie schnell hoch- oder herunterskalieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- Mit AWS Resource Access Manager (AWS RAM) können Sie Ihre Ressourcen sicher über AWS-Konten hinweg freigeben, um den betrieblichen Aufwand zu reduzieren und Transparenz und Überprüfbarkeit zu gewährleisten.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS)-Web-Service.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang.
- AWS Transit Gateway ist ein zentraler Hub, der VPCs und On-Premises-Netzwerke miteinander verbindet.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Andere Tools und Services

- nslookup ist ein Befehlszeilen-Tool, das zum Abfragen von DNS-Datensätzen verwendet wird. In diesem Muster verwenden Sie dieses Tool, um die Lösung zu testen.

Code-Repository

Der Code für dieses Muster ist auf GitHubim vpc-endpoint-sharingRepository verfügbar. Dieses Muster bietet zwei AWS- CloudFormation Vorlagen:

- Eine Vorlage für die Bereitstellung der folgenden Ressourcen im Hub-Konto:
  - `rSecurityGroupEndpoints` – Die Sicherheitsgruppe, die den Zugriff auf den VPC-Endpunkt steuert.

  - `rSecurityGroupResolvers` – Die Sicherheitsgruppe, die den Zugriff auf den Route 53 Resolver steuert.
  - `rKMSEndpoint`, `rSSMEndpoint`, und `rEC2MessagesEndpoint` – Beispiel für Schnittstellen`rSSMMessagesEndpoint`-VPC-Endpunkte im Hub-Konto. Passen Sie diese Endpunkte an Ihren Anwendungsfall an.
  - `rInboundResolver` – Ein Route 53 Resolver, der DNS-Abfragen für den Amazon DNS Resolver des Hubs auflöst.
  - `rOutboundResolver` – Ein ausgehender Route 53 Resolver, der Abfragen an den eingehenden Resolver weiterleitet.
  - `rAWSApiResolverRule` – Die Route 53-Resolver-Weiterleitungsregel, die für alle Spoke-VPCs freigegeben wird.
  - `rRamShareAWSResolverRule` – Die AWS RAM-Freigabe, die es den Spoke-VPCs ermöglicht, die `rAWSApiResolverRule` Weiterleitungsregel zu verwenden.
  - *`rVPC` – Die Hub-VPC, die zur Modellierung der freigegebenen Services verwendet wird.
  - *`rSubnet1` – Ein privates Subnetz, das zum Speichern der Hub-Ressourcen verwendet wird.
  - *`rRouteTable1` – Die Routing-Tabelle für die Hub-VPC.
  - *`rRouteTableAssociation1` – Für die `rRouteTable1` Routing-Tabelle in der Hub-VPC die Zuordnung für das private Subnetz.
  - *`rRouteSpoke` – Die Route von der Hub-VPC zur Spoke-VPC.
  - *`rTgw` – Das Transit-Gateway, das für alle Spoke-VPCs freigegeben ist.
  - *`rTgwAttach` – Die Anfügung, die es der Hub-VPC ermöglicht, Datenverkehr an das `rTgw` Transit-Gateway weiterzuleiten.
  - *`rTgwShare` – Die AWS RAM-Freigabe, die es den Spoke-Konten ermöglicht, das `rTgw` Transit-Gateway zu verwenden.
- Eine Vorlage für die Bereitstellung der folgenden Ressourcen in den Spoke-Konten:
  - `rAWSApiResolverRuleAssociation` – Eine Zuordnung, die es der Spoke-VPC ermöglicht, die gemeinsame Weiterleitungsregel im Hub-Konto zu verwenden.
  - *`rVPC` – Die Spoke-VPC.
  - *`rSubnet1, rSubnet2, rSubnet3` – Ein Subnetz für jede Availability Zone, das zum Speichern der privaten Spoke-Ressourcen verwendet wird.
  - *`rTgwAttach` – Der Anhang, der es der Spoke-VPC ermöglicht, Datenverkehr an das `rTgw` Transit-Gateway weiterzuleiten.

- *`rRouteTable1` – Die Routing-Tabelle für die Spoke-VPC.
- *`rRouteEndpoints` – Die Route von den Ressourcen in der Spoke-VPC zum Transit-Gateway.
- *`rRouteTableAssociation1/2/3` – Für die `rRouteTable1` Routing-Tabelle in der Spoke-VPC die Zuordnungen für die privaten Subnetze.
- *`rInstanceRole` – Die IAM-Rolle, die zum Testen der Lösung verwendet wird.
- *`rInstancePolicy` – Die IAM-Richtlinie, die zum Testen der Lösung verwendet wird.
- *`rInstanceSg` – Die Sicherheitsgruppe, die zum Testen der Lösung verwendet wird.
- *`rInstanceProfile` – Das IAM-Instance-Profil, das zum Testen der Lösung verwendet wird.
- *`rInstance` – Eine EC2-Instance, die für den Zugriff über AWS Systems Manager vorkonfiguriert ist. Verwenden Sie diese Instance, um die Lösung zu testen.

* Diese Ressourcen unterstützen die Beispielarchitektur und sind möglicherweise nicht erforderlich, wenn dieses Muster in einer vorhandenen Landing Zone implementiert wird.

Sekunden

Vorbereiten der CloudFormation Vorlagen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repository.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis an den Speicherort, an dem Sie die Beispieldateien speichern möchten. 2. Geben Sie den folgenden Befehl ein: `git clone https://github.com/aws-samples/vpc-endpoint-sharing.git`	Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Vorlagen.	1. Öffnen Sie im geklonten Repository die Dateien hub.yml und Spoke.yml. 2. Überprüfen Sie die von diesen Vorlagen erstellte n Ressourcen und passen Sie die Vorlagen nach Bedarf für Ihre Umgebung an. Eine vollständige Liste finden Sie im Abschnitt Code-Repository unter Tools . Wenn Ihre Konten bereits über einige dieser Ressourcen verfügen, entfernen Sie sie aus der CloudFormation Vorlage. Weitere Informationen finden Sie unter Arbeiten mit Vorlagen (CloudFor mation Dokumentation). 3. Speichern und schließen Sie die Dateien hub.yml und Spoke.yml.	Netzwerkadministrator, Cloud-Architekt

Bereitstellen der Ressourcen in den Zielkonten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Hub-Resso urcen bereit.	Erstellen Sie mithilfe der Vorlage hub.yml einen CloudFormation Stack. Wenn Sie dazu aufgefordert werden, geben Sie Werte für die Parameter in der Vorlage	Cloud-Architekt, Netzwerka dministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an. Weitere Informationen finden Sie unter Erstellen eines Stacks (CloudFormation Dokumentation).	
Stellen Sie die Spoke-Ressourcen bereit.	Erstellen Sie mithilfe der spoke.yml-Vorlage einen CloudFormation Stack. Wenn Sie dazu aufgefordert werden, geben Sie Werte für die Parameter in der Vorlage an. Weitere Informationen finden Sie unter Erstellen eines Stacks (CloudFormation Dokumentation).	Cloud-Architekt, Netzwerkadministrator

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie private DNS-Abfragen an den AWS-Service.	1. Stellen Sie mithilfe von Session Manager, einer Funktion von AWS Systems Manager, eine Verbindung mit der `rInstance` EC2-Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance mithilfe von Session Manager (Amazon EC2Dokumentation). 2. Verwenden Sie für einen AWS-Service mit einem	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	VPC-Endpunkt im Hub-Konto , `nslookup` um zu bestätigen, dass die privaten IP-Adressen für den eingehenden Route 53 Resolver zurückgegeben werden. Im Folgenden finden Sie ein Beispiel für die Verwendung von `nslookup`, um einen Amazon Systems Manager-Endpunkt zu erreichen. `nslookup ssm.<region>.amazonaws.com` 3. Geben Sie in der AWS Command Line Interface (AWS CLI) einen Befehl ein, der Ihnen helfen kann zu bestätigen, dass sich die Änderungen nicht auf die Service-Funktionalität ausgewirkt haben. Eine Liste der Befehle finden Sie unter AWS CLI Command Reference. Der folgende Befehl sollte beispielsweise eine Liste von Amazon Systems Manager-Dokumenten zurückgeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws ssm list-documents`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie öffentliche DNS-Abfragen an einen AWS-Service.	1. Verwenden Sie für einen AWS-Service, der keinen VPC-Endpunkt im Hub-Konto hat, , `nslookup` um zu bestätigen, dass die öffentlichen IP-Adressen zurückgegeben werden. Im Folgenden finden Sie ein Beispiel für die Verwendung von `nslookup`, um einen Amazon Simple Notification Service (Amazon SNS)-Endpunkt zu erreichen. `nslookup sns.<region>.amazonaws.com` 2. Geben Sie in der AWS CLI einen Befehl ein, mit dem Sie bestätigen können, dass sich die Änderungen nicht auf die Service-Funktionalität ausgewirkt haben. Eine Liste der Befehle finden Sie unter AWS CLI Command Reference. Wenn beispielsweise Amazon SNS-Themen im Hub-Konto vorhanden sind, sollte der folgende Befehl eine Liste von Themen zurückgeben.	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws sns list-topics`	

Zugehörige Ressourcen

- Aufbau einer skalierbaren und sicheren Multi-VPC-AWS-Netzwerkinfrastruktur (AWS-Whitepaper)
- Arbeiten mit freigegebenen Ressourcen (AWS-RAM-Dokumentation)
- Arbeiten mit Transit Gateways (AWS Transit Gateway-Dokumentation)

Erstellen Sie einen Bericht über die Ergebnisse von Network Access Analyzer für eingehenden Internetzugriff in mehreren AWS-Konten

Erstellt von Bol Virgilio (AWS)

Code-Repository: Network Access Analyzer – Analyse mehrerer Konten	Umgebung: Produktion	Technologien: Netzwerk, Sicherheit, Identität, Compliance
AWS-Services: AWS CloudFormation; Amazon S3; Amazon VPC; AWS Security Hub		

Übersicht

Unbeabsichtigter eingehender Internetzugang auf AWS-Ressourcen kann Risiken für den Datenumfang einer Organisation darstellen. Network Access Analyzer ist eine Amazon Virtual Private Cloud (Amazon VPC)-Funktion, mit der Sie unbeabsichtigten Netzwerkzugriff auf Ihre Ressourcen in Amazon Web Services (AWS) identifizieren können. Sie können Network Access Analyzer verwenden, um Ihre Netzwerkzugriffsanforderungen anzugeben und potenzielle Netzwerkpfade zu identifizieren, die nicht den von Ihnen angegebenen Anforderungen entsprechen. Sie können Network Access Analyzer verwenden, um Folgendes zu tun:

1. Identifizieren Sie AWS-Ressourcen, die über Internet-Gateways für das Internet zugänglich sind.
2. Stellen Sie sicher, dass Ihre Virtual Private Clouds (VPCs) angemessen segmentiert sind, z. B. die Isolierung von Produktions- und Entwicklungsumgebungen und die Trennung von Transaktions-Workloads.

Network Access Analyzer analysiert die Erreichbarkeitsbedingungen des end-to-end Netzwerks und nicht nur eine einzige Komponente. Um festzustellen, ob eine Ressource über das Internet zugänglich ist, wertet Network Access Analyzer das Internet-Gateway, VPC-Routing-Tabellen, Netzwerkzugriffskontrolllisten (ACLs), öffentliche IP-Adressen auf Elastic Network-Schnittstellen und

Sicherheitsgruppen aus. Wenn eine dieser Komponenten den Internetzugang verhindert, generiert Network Access Analyzer keine Erkenntnis. Wenn beispielsweise eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance über eine offene Sicherheitsgruppe verfügt, die Datenverkehr von zulässt, sich die Instance `0/0` jedoch in einem privaten Subnetz befindet, das von keinem Internet-Gateway weitergeleitet werden kann, würde Network Access Analyzer kein Ergebnis generieren. Dies liefert Ergebnisse mit hoher Genauigkeit, sodass Sie Ressourcen identifizieren können, auf die über das Internet wirklich zugegriffen werden kann.

Wenn Sie Network Access Analyzer ausführen, verwenden Sie Network Access Scopes, um Ihre Netzwerkzugriffsanforderungen anzugeben. Diese Lösung identifiziert Netzwerkpfade zwischen einem Internet-Gateway und einer Elastic-Network-Schnittstelle. In diesem Muster stellen Sie die Lösung in einem zentralen AWS-Konto in Ihrer Organisation bereit, das von AWS Organizations verwaltet wird, und es analysiert alle Konten in jeder AWS-Region in der Organisation.

Diese Lösung wurde unter Berücksichtigung der folgenden Aspekte entwickelt:

- Die AWS- CloudFormation Vorlagen reduzieren den Aufwand für die Bereitstellung der AWS-Ressourcen in diesem Muster.
- Sie können die Parameter in den CloudFormation Vorlagen und dem naa-script.sh-Skript zum Zeitpunkt der Bereitstellung anpassen, um sie an Ihre Umgebung anzupassen.
- Bash-Scripting stellt die Netzwerkzugriffsbereiche für mehrere Konten automatisch parallel bereit und analysiert sie.
- Ein Python-Skript verarbeitet die Ergebnisse, extrahiert die Daten und konsolidiert dann die Ergebnisse. Sie können den konsolidierten Bericht der Ergebnisse von Network Access Analyzer im CSV-Format oder in AWS Security Hub überprüfen. Ein Beispiel für den CSV-Bericht finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.
- Sie können Erkenntnisse korrigieren oder sie aus zukünftigen Analysen ausschließen, indem Sie sie der Datei naa-exclusions.csv hinzufügen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto für das Hosten von Sicherheitsservices und -tools, das als Mitgliedskonto einer Organisation in AWS Organizations verwaltet wird. In diesem Muster wird dieses Konto als Sicherheitskonto bezeichnet.

- Im Sicherheitskonto müssen Sie über ein privates Subnetz mit ausgehendem Internetzugang verfügen. Anweisungen finden Sie unter Erstellen eines Subnetzes in der Amazon-VPC-Dokumentation. Sie können den Internetzugang mithilfe eines NAT-Gateways oder eines Schnittstellen-VPC-Endpunkts einrichten.
- Zugriff auf das AWS Organizations-Verwaltungskonto oder ein Konto mit delegierten Administratorberechtigungen für CloudFormation. Anweisungen finden Sie unter Registrieren eines delegierten Administrators in der - CloudFormation Dokumentation.
- Aktivieren Sie den vertrauenswürdigen Zugriff zwischen AWS Organizations und CloudFormation. Anweisungen finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs mit AWS Organizations in der - CloudFormation Dokumentation.
- Wenn Sie die Ergebnisse in Security Hub hochladen, muss Security Hub in dem Konto und der AWS-Region aktiviert sein, in der die EC2-Instance bereitgestellt wird. Weitere Informationen finden Sie unter Einrichten von AWS Security Hub.

Einschränkungen

- Kontoübergreifende Netzwerkpfade werden derzeit aufgrund von Einschränkungen der Network Access Analyzer-Funktion nicht analysiert.
- Die AWS-Zielkonten müssen als Organisation in AWS Organizations verwaltet werden. Wenn Sie AWS Organizations nicht verwenden, können Sie die Vorlage naa-execrole.yaml CloudFormation und das Skript naa-script.sh für Ihre Umgebung aktualisieren. Stattdessen geben Sie eine Liste der AWS-Konto-IDs und Regionen an, in denen Sie das Skript ausführen möchten.
- Die CloudFormation Vorlage ist für die Bereitstellung der EC2-Instance in einem privaten Subnetz mit ausgehendem Internetzugang konzipiert. Der AWS Systems Manager Agent (SSM Agent) benötigt ausgehenden Zugriff, um den Systems Manager-Service-Endpunkt zu erreichen, und Sie benötigen ausgehenden Zugriff, um das Code-Repository zu klonen und Abhängigkeiten zu installieren. Wenn Sie ein öffentliches Subnetz verwenden möchten, müssen Sie die Vorlage naa-resources.yaml ändern, um der EC2-Instance eine Elastic IP-Adresse zuzuordnen.

Architektur

Zieltechnologie-Stack

- Network Access Analyzer
- Amazon EC2-Instance

- AWS Identity and Access Management (IAM)-Rollen
- Amazon Simple Storage Service (Amazon S3)-Bucket
- Amazon Simple Notification Service-Thema (Amazon SNS)
- AWS Security Hub (nur Option 2)

Zielarchitektur

Option 1: Zugreifen auf Ergebnisse in einem Amazon S3-Bucket

Das Diagramm zeigt den folgenden Prozess:

1. Wenn Sie die Lösung manuell ausführen, authentifiziert sich der Benutzer mit Session Manager bei der EC2-Instance und führt dann das Skript naa-script.sh aus. Dieses Shell-Skript führt die Schritte 2 bis 7 aus.

   Wenn Sie die Lösung automatisch ausführen, startet das Skript naa-script.sh automatisch nach dem Zeitplan, den Sie im Cron-Ausdruck definiert haben. Dieses Shell-Skript führt die Schritte 2 bis 7 aus. Weitere Informationen finden Sie unter Automatisierung und Skalierung am Ende dieses Abschnitts.
2. Die EC2-Instance lädt die neueste naa-exception.csv-Datei aus dem S3-Bucket herunter. Diese Datei wird später im Prozess verwendet, wenn das Python-Skript die Ausnahmen verarbeitet.
3. Die EC2-Instance übernimmt die `NAAEC2Role` IAM-Rolle, die Berechtigungen für den Zugriff auf den S3-Bucket und die Übernahme der `NAAExecRole` IAM-Rollen in den anderen Konten in der Organisation gewährt.
4. Die EC2-Instance übernimmt die `NAAExecRole` IAM-Rolle im Verwaltungskonto der Organisation und generiert eine Liste der Konten in der Organisation.
5. Die EC2-Instance übernimmt die `NAAExecRole` IAM-Rolle in den Mitgliedskonten der Organisation (in der Architekturdiagramm als Workload-Konten bezeichnet) und führt in jedem Konto eine Sicherheitsbewertung durch. Die Ergebnisse werden als JSON-Dateien auf der EC2-Instance gespeichert.
6. Die EC2-Instance verwendet ein Python-Skript, um die JSON-Dateien zu verarbeiten, die Datenfelder zu extrahieren und einen CSV-Bericht zu erstellen.
7. Die EC2-Instance lädt die CSV-Datei in den S3-Bucket hoch.

8. Eine Amazon- EventBridge Regel erkennt den Datei-Upload und verwendet ein Amazon SNS-Thema, um eine E-Mail zu senden, die den Benutzer benachrichtigt, dass der Bericht abgeschlossen ist.
9. Der Benutzer lädt die CSV-Datei aus dem S3-Bucket herunter. Der Benutzer importiert die Ergebnisse in die Excel-Vorlage und überprüft die Ergebnisse.

Option 2: Zugreifen auf Ergebnisse in AWS Security Hub

Das Diagramm zeigt den folgenden Prozess:

1. Wenn Sie die Lösung manuell ausführen, authentifiziert sich der Benutzer mit Session Manager bei der EC2-Instance und führt dann das Skript naa-script.sh aus. Dieses Shell-Skript führt die Schritte 2 bis 7 aus.

   Wenn Sie die Lösung automatisch ausführen, startet das Skript naa-script.sh automatisch nach dem Zeitplan, den Sie im Cron-Ausdruck definiert haben. Dieses Shell-Skript führt die Schritte 2 bis 7 aus. Weitere Informationen finden Sie unter Automatisierung und Skalierung am Ende dieses Abschnitts.
2. Die EC2-Instance lädt die neueste naa-exception.csv-Datei aus dem S3-Bucket herunter. Diese Datei wird später im Prozess verwendet, wenn das Python-Skript die Ausnahmen verarbeitet.
3. Die EC2-Instance übernimmt die `NAAEC2Role` IAM-Rolle, die Berechtigungen für den Zugriff auf den S3-Bucket und die Übernahme der `NAAExecRole` IAM-Rollen in den anderen Konten in der Organisation gewährt.
4. Die EC2-Instance übernimmt die `NAAExecRole` IAM-Rolle im Verwaltungskonto der Organisation und generiert eine Liste der Konten in der Organisation.
5. Die EC2-Instance übernimmt die `NAAExecRole` IAM-Rolle in den Mitgliedskonten der Organisation (in der Architekturdiagramm als Workload-Konten bezeichnet) und führt in jedem Konto eine Sicherheitsbewertung durch. Die Ergebnisse werden als JSON-Dateien auf der EC2-Instance gespeichert.
6. Die EC2-Instance verwendet ein Python-Skript, um die JSON-Dateien zu verarbeiten und die Datenfelder für den Import in Security Hub zu extrahieren.
7. Die EC2-Instance importiert die Network Access Analyzer-Ergebnisse in Security Hub.
8. Eine Amazon- EventBridge Regel erkennt den Import und verwendet ein Amazon SNS-Thema, um eine E-Mail zu senden, die den Benutzer benachrichtigt, dass der Vorgang abgeschlossen ist.

9. Der Benutzer zeigt die Ergebnisse in Security Hub an.

Automatisierung und Skalierung

Sie können diese Lösung so planen, dass das Skript naa-script.sh automatisch nach einem benutzerdefinierten Zeitplan ausgeführt wird. Um einen benutzerdefinierten Zeitplan festzulegen, ändern Sie in der Vorlage naa-resources.yaml CloudFormation den `CronScheduleExpression` Parameter . Beispielsweise `0 0 * * 0` führt der Standardwert von die Lösung jeden Sonntag um Mitternacht aus. Ein Wert von `0 0 * 1-12 0` würde die Lösung jeden ersten Sonntag im Monat um Mitternacht ausführen. Weitere Informationen zur Verwendung von Cron-Ausdrücken finden Sie unter Cron- und Rate-Ausdrücke in der Systems Manager-Dokumentation.

Wenn Sie den Zeitplan nach der Bereitstellung des `NAA-Resources`Stacks anpassen möchten, können Sie den Cron-Zeitplan in manuell bearbeiten`/etc/cron.d/naa-schedule`.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mit API-Zielen oder Event Buses in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS-Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang. Dieses Muster verwendet Session Manger, eine Funktion von Systems Manager.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Network Access Analyzer Multi-Account Analysis verfügbar. Das Code-Repository enthält die folgenden Dateien:

- naa-script.sh – Dieses Bash-Skript wird verwendet, um eine Network Access Analyzer-Analyse mehrerer AWS-Konten parallel zu starten. Wie in der Vorlage naa-resources.yaml CloudFormation definiert, wird dieses Skript automatisch im `/usr/local/naa` Ordner auf der EC2-Instance bereitgestellt.
- naa-resources.yaml – Sie verwenden diese CloudFormation Vorlage, um einen Stack im Sicherheitskonto in der Organisation zu erstellen. Diese Vorlage stellt alle erforderlichen Ressourcen für dieses Konto bereit, um die Lösung zu unterstützen. Dieser Stack muss vor der Vorlage naa-execrole.yaml bereitgestellt werden.

  Hinweis: Wenn dieser Stack gelöscht und erneut bereitgestellt wird, müssen Sie das `NAAExecRole` Stack-Set neu erstellen, um die kontoübergreifenden Abhängigkeiten zwischen den IAM-Rollen neu zu erstellen.

- naa-execrole.yaml – Sie verwenden diese CloudFormation Vorlage, um ein Stack-Set zu erstellen, das die `NAAExecRole` IAM-Rolle in allen Konten in der Organisation bereitstellt, einschließlich des Verwaltungskontos.
- naa-processfindings.py – Das naa-script.sh-Skript ruft dieses Python-Skript automatisch auf, um die JSON-Ausgaben des Network Access Analyzer zu verarbeiten, alle bekannten guten Ressourcen in der Datei naa-exclusions.csv auszuschließen und dann entweder eine CSV-Datei der konsolidierten Ergebnisse zu generieren oder die Ergebnisse in Security Hub zu importieren.

Sekunden

Vorbereiten der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repository.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis an den Speicherort, an dem Sie die Beispieldateien speichern möchten. 2. Geben Sie den folgenden Befehl ein. `git clone https://github.com/aws-samples/network-access-analyzer-multi-account-analysis.git`	AWS DevOps
Überprüfen Sie die Vorlagen.	1. Öffnen Sie im geklonten Repository die Dateien naa-resources.yaml und naa-execrole.yaml. 2. Überprüfen Sie die von diesen Vorlagen erstellten Ressourcen und passen Sie die Vorlagen nach Bedarf für Ihre Umgebung an. Weitere Informationen finden Sie unter Arbeiten mit Vorlagen in der -CloudFormation Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Speichern und schließen Sie die Dateien naa-resources.yaml und naa-execrole.yaml.	

Erstellen der CloudFormation Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Sicherheitskonto bereit.	Mit der Vorlage naa-resources.yaml erstellen Sie einen CloudFormation Stack, der alle erforderlichen Ressourcen im Sicherheitskonto bereitstellt. Anweisungen finden Sie unter Erstellen eines Stacks in der - CloudFormation Dokumentation. Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite Vorlage angeben die Option Vorlage ist bereit und laden Sie dann die Datei naa-resources.yaml hoch. 2. Geben Sie auf der Seite Stack-Details angeben im Feld Stack-Name ein`NAA-Resources` . 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `VPCId` – Wählen Sie eine VPC im Konto aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `SubnetId` – Wählen Sie ein privates Subnetz mit Internetzugang aus. Hinweis: Wenn Sie ein öffentliches Subnetz auswählen, wird der EC2-Instance möglicher weise keine öffentliche IP-Adresse zugewiesen, da die CloudFormation Vorlage standardmäßig keine Elastic IP-Adresse bereitstellt und anfügt. • `InstanceType` – Behalten Sie den Standard-Instance-Typ bei. • `InstanceImageId` – Behalten Sie die Standardeinstellung bei. • `KeyPairName` – Wenn Sie SSH für den Zugriff verwenden, geben Sie den Namen eines vorhandenen Schlüssel paars an. • `PermittedSSHInboun d` – Wenn Sie SSH für den Zugriff verwenden , geben Sie einen zulässigen CIDR-Block an. Wenn Sie SSH nicht verwenden, behalten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Standardwert bei`127.0.0.1` . • `BucketName` – Der Standardwert ist `naa-<accountID>-<region>` . Sie können dies nach Bedarf ändern. Wenn Sie einen benutzerdefinierten Wert angeben, werden die Konto-ID und die Region automatisch an den angegebenen Wert angehängt. • `EmailAddress` – Geben Sie eine E-Mail-Adresse für eine Amazon SNS-Benachrichtigung an, wenn die Analyse abgeschlossen ist. Hinweis: Die Amazon SNS-Abonnementkonfiguration muss vor Abschluss der Analyse bestätigt werden, sonst wird keine Benachrichtigung gesendet. • `NAAEC2Role` – Behalten Sie die Standardeinstellung bei, es sei denn, Ihre Namenskonventionen erfordern einen anderen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen für diese IAM-Rolle. • `NAAExecRole` – Behalten Sie die Standardeinstellung bei, es sei denn, bei der Bereitstellung von naa-execrole.yaml wird ein anderer Name verwendet • `Parallelism` – Geben Sie die Anzahl der durchzuführenden parallelen Bewertungen an. • `Regions` – Geben Sie die AWS-Regionen an, die Sie analysieren möchten. • `ScopeNameValue` – Geben Sie das Tag an, das dem Bereich zugewiesen werden soll. Dieses Tag wird verwendet, um den Netzwerkzugriffsbereich zu bestimmen. • `ExclusionFile` – Geben Sie den Namen der Ausschlussdatei an. Einträge in dieser Datei werden von den Ergebnissen ausgeschl ossen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `FindingsToCSV` – Geben Sie an, ob Ergebnisse in CSV ausgegeben werden sollen. Zulässige Werte sind `true` und `false`. • `FindingsToSecurityHub` – Geben Sie an, ob Ergebnisse in Security Hub importiert werden sollen. Zulässige Werte sind `true` und `false`. • `EmailNotificationsForSecurityHub` – Geben Sie an, ob beim Importieren von Ergebnissen in Security Hub E-Mail-Benachrichtigungen generiert werden sollen. Zulässige Werte sind `true` und `false`. • `ScheduledAnalysis` – Wenn die Lösung automatisch nach einem Zeitplan ausgeführt werden soll, geben Sie ein `true`und passen Sie dann den Zeitplan im `CronScheduleExpression` Parameter an. Wenn Sie die Lösung nicht automatisch ausführen möchten, geben Sie ein`false`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `CronScheduleExpression` – Wenn Sie die Lösung automatisch ausführen, geben Sie einen Cron-Ausdruck ein, um den Zeitplan zu definieren. Weitere Informationen finden Sie unter Automatisierung und Skalierung im Abschnitt Architektur dieses Musters. 1. Wählen Sie auf der Seite Überprüfen die folgenden Ressource(n) mit den erforderlichen Funktionen aus: [AWS::IAM::Role] und wählen Sie dann Stack erstellen aus. 2. Nachdem der Stack erfolgreich erstellt wurde, kopieren Sie in der CloudFormation Konsole auf der Registerkarte Outputs den `NAAEC2Role` Amazon-Ressourcennamen (ARN). Sie verwenden diesen ARN später bei der Bereitstellung der Datei naa-execrole.yaml.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle in den Mitgliedskonten bereit.	Verwenden Sie im AWS Organizations-Verwaltungskonto oder einem Konto mit delegierten Administratorberechtigungen für die Vorlage naa-execrole.yaml CloudFormation, um ein CloudFormation Stack-Set zu erstellen. Das Stack-Set stellt die `NAAExecRole` IAM-Rolle in allen Mitgliedskonten in der Organisation bereit. Anweisungen finden Sie unter Erstellen eines Stack-Sets mit serviceverwalteten Berechtigungen in der - CloudFormation Dokumentation. Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie unter Vorlage vorbereiten die Option Vorlage ist bereit aus und laden Sie dann die Datei naa-execrole.yaml hoch. 2. Geben Sie auf der Seite StackSet Details angeben den Namen des Stack-Sets an`NAA-ExecRole`. 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `AuthorizedARN` – Geben Sie den `NAAEC2Role` ARN	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein, den Sie beim Erstellen des `NAA-Resources` Stacks kopiert haben. • `NAARoleName` – Behalten Sie den Standardwert von bei, `NAAExecRole` es sei denn, bei der Bereitstellung der Datei naa-resources.yaml wurde ein anderer Name verwendet. 4. Wählen Sie unter Permissions (Berechtigungen) die Option Service-managed permissions (Servicev erwaltete Berechtigungen) aus. 5. Wählen Sie auf der Seite Bereitstellungsoptionen festlegen unter Bereitstellungsziele die Option In Organisation bereitstellen aus und akzeptieren Sie alle Standardwerte. Hinweis: Wenn die Stacks gleichzeitig für alle Mitgliedskonten bereitgestellt werden sollen, legen Sie Maximale Anzahl gleichzeitiger Konten und Fehlertoleranz	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf einen hohen Wert fest, z. B. 100. 6. Wählen Sie unter Bereitstellungsregionen die Region aus, in der die EC2-Instance für Network Access Analyzer bereitgestellt wird. Da IAM-Ressourcen global und nicht regional sind, wird die IAM-Rolle in allen aktiven Regionen bereitgestellt. 7. Wählen Sie auf der Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt, und wählen Sie dann Erstellen aus StackSet. 8. Überwachen Sie die Registerkarte Stack-Instances (für den Status eines einzelnen Kontos) und die Registerkarte Vorgänge (für den Gesamtstatus), um festzustellen, wann die Bereitstellung abgeschlossen ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle im Verwaltungskonto bereit.	Mit der Vorlage naa-execrole.yaml erstellen Sie einen CloudFormation Stack, der die `NAAExecRole` IAM-Rolle im Verwaltungskonto der Organisation bereitstellt. Das zuvor erstellte StackSet stellt die IAM-Rolle nicht im Verwaltungskonto bereit. Anweisungen finden Sie unter Erstellen eines Stacks in der CloudFormation Dokumentation. Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite Vorlage angeben die Option Vorlage ist bereit und laden Sie dann die Datei naa-execrole.yaml hoch. 2. Geben Sie auf der Seite Stack-Details angeben im Feld Stack-Name ein `NAA-ExecRole` . 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `AuthorizedARN` – Geben Sie den `NAAEC2Role` ARN ein, den Sie beim Erstellen des `NAA-Resources` Stacks kopiert haben.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `NAARoleName` – Behalten Sie den Standardwert von bei, `NAAExecRole` es sei denn, bei der Bereitstellung der Datei naa-resources.yaml wurde ein anderer Name verwendet. 4. Wählen Sie auf der Seite Überprüfen die folgenden Ressource(n) aus, die Funktionen erfordern: [AWS::IAM::Role] und wählen Sie dann Stack erstellen aus.	

Durchführen der Analyse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Shell-Skript an.	1. Melden Sie sich beim Sicherheitskonto in der Organisation an. 2. Stellen Sie mithilfe von Session Manager eine Verbindung mit der EC2-Instance für Network Access Analyzer her, die Sie zuvor bereitgestellt haben. Anweisungen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance mithilfe	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	von Session Manager. Wenn Sie keine Verbindung herstellen können, finden Sie weitere Informationen im Abschnitt Fehlerbehebung dieses Musters.
	3. Geben Sie die folgenden Befehle ein, um die Datei naa-script.sh zur Bearbeitung zu öffnen.
	`sudo -i`
	`cd /usr/local/naa`
	`vi naa-script.sh`
	4. Überprüfen und ändern Sie die anpassbaren Parameter und Variablen in diesem Skript nach Bedarf für Ihre Umgebung. Weitere Informationen zu Anpassungsoptionen finden Sie in den Kommentaren am Anfang des Skripts.
	Anstatt beispielsweise eine Liste aller Mitglieds konten in der Organisation vom Verwaltungskonto abzurufen, können Sie das Skript ändern, um die AWS-Konto-IDs oder AWS-Regionen anzugeben, die Sie scannen möchten, oder Sie können auf eine externe	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei verweisen, die diese Parameter enthält. 5. Speichern und schließen Sie die Datei naa-script.sh.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Analysieren Sie die Zielkonten.	1. Geben Sie die folgenden Befehle ein. Dadurch wird das Skript naa-script.sh ausgeführt.
	`sudo -i`
	`cd /usr/local/naa`
	`screen`
	`./naa-script.sh`
	Beachten Sie Folgendes:
	• Der `screen` Befehl erlaubt dem Skript, weiter ausgeführt zu werden, falls die Verbindung abläuft oder Sie den Konsolenzugriff verlieren.
	• Nachdem der Scan gestartet wurde, können Sie das Trennen eines Bildschirms erzwingen, indem Sie Strg+A D drücken. Der Bildschirm wird getrennt und Sie können die Instance-Verbindung schließen, während die Analyse fortgesetzt wird.
	• Um eine getrennte Sitzung fortzusetzen, stellen Sie eine Verbindung mit der Instance her und geben
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie `sudo -i` dann ein`screen -r`. 2. Überwachen Sie die Ausgabe auf Fehler, um sicherzustellen, dass das Skript ordnungsg emäß funktioniert. Eine Beispielausgabe finden Sie im Abschnitt Zusätzlic he Informationen dieses Musters. 3. Warten Sie, bis die Analyse abgeschlossen ist. Wenn Sie E-Mail-Benachricht igungen konfiguriert haben, erhalten Sie eine E-Mail, wenn die Ergebnisse in den S3-Bucket hochgelad en oder in Security Hub importiert wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 – Ruft die Ergebnisse aus dem S3-Bucket ab.	1. Laden Sie die CSV-Datei aus dem `naa-<accountID>-<region>` Bucket herunter. Anweisungen finden Sie unter Herunterladen eines Objekts in der Amazon S3-Dokumentation. 2. Löschen Sie die CSV-Datei aus dem S3-Bucket. Dies ist eine bewährte Methode für die Kostenoptimierung. Anweisungen finden Sie unter Löschen von Objekten in der Amazon S3-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2 – Überprüfen Sie die Ergebnisse in Security Hub.	1. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/. 2. Wählen Sie im Navigationsbereich die Option Erkenntnisse aus. 3. Überprüfen Sie die Ergebnisse von Network Access Analyzer. Anweisungen finden Sie unter Anzeigen von Erkenntnislisten und Details in der Security Hub-Dokumentation. Hinweis: Sie können Ergebnisse durchsuchen, indem Sie einen Titel hinzufügen, der mit dem Filter beginnt und eingibt`Network Access Analyzer`.	AWS DevOps

Ergebnisse korrigieren und ausschließen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie Ergebnisse.	Korrigieren Sie alle Erkenntnisse, die Sie beheben möchten. Weitere Informationen und bewährte Methoden zum Erstellen eines Perimeters um Ihre AWS-Identitäten,	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ressourcen und Netzwerke finden Sie unter Erstellen eines Datenperimeters in AWS (AWS-Whitepaper).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie Ressourcen mit bekannten guten Netzwerkp faden aus.	Wenn Network Access Analyzer Ergebnisse für Ressourcen generiert, auf die über das Internet zugegriff en werden kann, können Sie diese Ressourcen zu einer Ausschlussliste hinzufüge n. Wenn Network Access Analyzer das nächste Mal ausgeführt wird, wird kein Ergebnis für diese Ressource generiert. 1. Navigieren Sie zu `/usr/local/naa` und öffnen Sie dann das Skript naa-script.sh. Notieren Sie sich den Wert der `S3_EXCLUSION_FILE` Variable. 2. Wenn der Wert der `S3_EXCLUSION_FILE` Variable lautet`true`, laden Sie die Datei naa-exclusions.csv aus dem `naa-<accountID>-<region>` Bucket herunter. Anweisungen finden Sie unter Herunterladen eines Objekts in der Amazon S3-Dokumentation. Wenn der Wert der `S3_EXCLUSION_FILE` Variable lautet`false`, navigieren Sie zur Datei	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	naa-exclusions.csv `/usr/local/naa` und öffnen Sie sie.
	
	Hinweis: Wenn der Wert der `S3_EXCLUSION_FILE` Variable lautet`false`, verwendet das Skript eine lokale Version der Ausschlussdatei. Wenn Sie den Wert später in ändern`true`, überschreibt das Skript die lokale Version mit der Datei im S3-Bucket.
	3. Geben Sie in der Datei naa-exclusions.csv die Ressourcen ein, die Sie ausschließen möchten. Geben Sie in jede Zeile eine Ressource ein und verwenden Sie das folgende Format.
	
	`<resource_id>,<secgroup_id>,<sgrule_cidr>,<sgrule_portrange>,<sgrule_protocol>`
	
	Im Folgenden finden Sie eine Beispielressource.
	
	`eni-1111aaaaa2222bbbb,sg-3333ccccc44`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`44dddd,0.0.0.0/0,80 to 80,tcp` 4. Speichern und schließen Sie die Datei naa-exclusions.csv. 5. Wenn Sie die Datei naa-exclusions.csv aus dem S3-Bucket heruntergeladen haben, laden Sie die neue Version hoch. Anweisungen finden Sie unter Hochladen von Objekten in der Amazon S3-Dokumentation.	

(Optional) Aktualisieren des naa-script.sh-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie das naa-script.sh-Skript.	Wenn Sie das naa-script.sh-Skript auf die neueste Version im Repo aktualisieren möchten, gehen Sie wie folgt vor: 1. Stellen Sie mithilfe von Session Manager eine Verbindung mit der EC2-Instance her. Anweisungen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance mithilfe von Session Manager.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Geben Sie den folgenden Befehl ein.
	`sudo -i`
	3. Navigieren Sie zum Skriptverzeichnis naa-script.sh.
	`cd /usr/local/naa`
	4. Geben Sie den folgenden Befehl ein, um das lokale Skript zu verbergen , damit Sie benutzerdefinierte Änderungen mit der neuesten Version zusammenführen können.
	`git stash`
	5. Geben Sie den folgenden Befehl ein, um die neueste Version des Skripts abzurufen.
	`git pull`
	6. Geben Sie den folgenden Befehl ein, um das benutzerdefinierte Skript mit der neuesten Version des Skripts zusammenzuführen.
	`git stash pop`	

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle bereitgestellten Ressourcen.	Sie können die in den Konten bereitgestellten Ressourcen belassen. Wenn Sie die Bereitstellung aller Ressourcen aufheben möchten, gehen Sie wie folgt vor: 1. Löschen Sie den im Verwaltungskonto bereitgestellten `NAA-ExecRole` Stack. Anweisungen finden Sie unter Löschen eines Stacks in der CloudFormation Dokumentation. 2. Löschen Sie das `NAA-ExecRole` Stack-Set, das im Verwaltungskonto der Organisation oder im delegierten Administratorkonto bereitgestellt wurde. Anweisungen finden Sie unter Löschen eines Stack-Sets in der CloudFormation Dokumentation. 3. Löschen Sie alle Objekte im `naa-<accountID>-<region>` S3-Bucket. Anweisungen finden Sie unter Löschen von Objekten	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der Amazon S3-Dokumentation. 4. Löschen Sie den im Sicherheitskonto bereitgestellten `NAA-Resources` Stack. Anweisungen finden Sie unter Löschen eines Stacks in der CloudFormation Dokumentation.	

Fehlerbehebung

Problem	Lösung
Es konnte keine Verbindung mit der EC2-Instance mithilfe von Session Manager hergestellt werden.	Der SSM-Agent muss mit dem Systems Manager-Endpunkt kommunizieren können. Gehen Sie wie folgt vor: 1. Überprüfen Sie, ob das Subnetz, in dem die EC2-Instance bereitgestellt wird, Internetzugang hat. 2. Starten Sie die EC2-Instance neu.
Bei der Bereitstellung des Stack-Sets werden Sie von der CloudFormation Konsole zu aufgefordert`Enable trusted access with AWS Organizations to use service-managed permissions` .	Dies weist darauf hin, dass der vertrauenswürdige Zugriff zwischen AWS Organizations und nicht aktiviert wurde CloudFormation. Vertrauenswürdiger Zugriff ist erforderlich, um das serviceverwaltete Stack-Set bereitzustellen. Wählen Sie die Schaltfläche, um den vertrauenswürdigen Zugriff zu aktivieren. Weitere Informationen finden Sie unter Vertrauenswürdigen Zugriff aktivieren in der CloudFormation Dokumentation.

Zugehörige Ressourcen

- Neu – Amazon VPC Network Access Analyzer (AWS-Blogbeitrag)
- AWS re:Inforce 2022 – Validierung effektiver Netzwerkzugriffskontrollen in AWS (NIS202) (Video)
- Demo – Organisationsweite Internet-Ingress-Datenpfadanalyse mit Network Access Analyzer (Video)

Zusätzliche Informationen

Beispiel für eine Konsolenausgabe

Das folgende Beispiel zeigt die Ausgabe der Generierung der Liste der Zielkonten und der Analyse der Zielkonten.

```
[root@ip-10-10-43-82 naa]# ./naa-script.sh
download: s3://naa-<account ID>-us-east-1/naa-exclusions.csv to ./naa-exclusions.csv

AWS Management Account: <Management account ID>

AWS Accounts being processed...
<Account ID 1> <Account ID 2> <Account ID 3>

Assessing AWS Account: <Account ID 1>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 2>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 3>, using Role: NAAExecRole
Processing account: <Account ID 1> / Region: us-east-1
Account: <Account ID 1> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 2> / Region: us-east-1
Account: <Account ID 2> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 3> / Region: us-east-1
Account: <Account ID 3> / Region: us-east-1 - Detecting Network Analyzer scope...
Account: <Account ID 1> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 1> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 2> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 2> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 3> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 3> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
```

Beispiele für CSV-Berichte

Die folgenden Bilder sind Beispiele für die CSV-Ausgabe.

Automatisches Markieren von Transit Gateway-Anhängen mit AWS Organizations

Erstellt von Richard Milner-Watts (AWS),is Bin Ayub (AWS) und John Capps (AWS)

Code-Repository: Transit Gateway Attachment Tagger	Umgebung: Produktion	Technologien: Netzwerk; Infrastruktur; Management und Governance; Betrieb
AWS-Services: AWS Step Functions ;AWS Transit Gateway; Amazon VPC; AWS Lambda		

Übersicht

Auf Amazon Web Services (AWS) können Sie AWS Resource Access Manager verwenden, um AWS Transit Gateway über AWS-Kontogrenzen hinweg gemeinsam zu nutzen. Wenn Sie jedoch Transit-Gateway-Anhänge über Kontogrenzen hinweg erstellen, werden die Anhänge ohne Namens-Tag erstellt. Dadurch kann die Identifizierung von Anhängen zeitaufwändig sein.

Diese Lösung bietet einen automatisierten Mechanismus zum Sammeln von Informationen über jeden Transit Gateway-Anhang für Konten innerhalb einer Organisation, die von AWS Organizations verwaltet wird. Der Prozess umfasst das Suchen des CIDR-Bereichs (Classless Inter-Domain Routing) aus der Transit-Gateway-Routing-Tabelle. Die Lösung wendet dann ein Namens-Tag in Form von `<CIDR-range>-<AccountName>` auf den Anhang innerhalb des Kontos an, das das Transit Gateway enthält.

Diese Lösung kann zusammen mit einer Lösung wie dem Serverless Transit Network Orchestrator aus der AWS Solutions Library verwendet werden. Serverless Transit Network Orchestrator ermöglicht die automatisierte Erstellung von Transit-Gateway-Anhängen in großem Umfang.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Eine AWS Organizations-Organisation, die alle zugehörigen Konten enthält
- Zugriff auf das Organisationsverwaltungskonto unter dem Stammverzeichnis der Organisation, um die erforderliche AWS Identity and Access Management (IAM)-Rolle zu erstellen
- Ein Shared Networking-Mitgliedskonto mit einem oder mehreren Transit Gateways, die für die Organisation freigegeben sind und Anlagen haben

Architektur

Der folgende Screenshot der AWS-Managementkonsole zeigt Beispiele für Transit Gateway-Anfügungen ohne zugeordnetes Name-Tag und zwei Transit Gateway-Anfügungen mit Name-Tags, die von dieser Lösung generiert wurden. Die Struktur des generierten Namens-Tags ist `<CIDR-range>-<AccountName>`.

Diese Lösung verwendet AWS CloudFormation, um einen AWS Step Functions-Workflow bereitzustellen, der die Erstellung von Transit Gateway-Namens-Tags in allen konfigurierten Regionen verwaltet. Der Workflow ruft AWS Lambda-Funktionen auf, die die zugrunde liegenden Aufgaben ausführen.

Nachdem die Lösung die Kontonamen von AWS Organizations erhalten hat, ruft der Step Functions-Zustandsautomat alle Transit Gateway-Anhangs-IDs ab. Diese werden parallel von der AWS-Region verarbeitet. Diese Verarbeitung beinhaltet das Nachschlagen des CIDR-Bereichs für jede Anfügung. Der CIDR-Bereich wird durch Durchsuchen der Transit-Gateway-Routing-Tabellen innerhalb der Region nach einer übereinstimmenden Transit-Gateway-Anhangs-ID abgerufen. Wenn alle erforderlichen Informationen verfügbar sind, wendet die Lösung ein Namens-Tag auf den Anhang an. Die Lösung überschreibt keine vorhandenen Name-Tags.

Die Lösung wird nach einem von einem Amazon EventBridge-Ereignis gesteuerten Zeitplan ausgeführt. Das Ereignis initiiert die Lösung jeden Tag um 6:00 Uhr UTC.

Zieltechnologie-Stack

- Amazon EventBridge
- AWS Lambda
- AWS Organizations
- AWS Transit Gateway
- Amazon Virtual Private Cloud (Amazon VPC)

- AWS X-Ray

Zielarchitektur

Die Lösungsarchitektur und der Workflow sind im folgenden Diagramm dargestellt.

1. Das geplante Ereignis initiiert die Regel.
2. Die EventBridge Regel startet den Step Functions-Zustandsautomaten.
3. Der Zustandsautomat ruft die `tgw-tagger-organizations-account-query` Lambda-Funktion auf.
4. Die `tgw-tagger-organizations-account-query` Lambda-Funktion übernimmt die Rolle im Verwaltungskonto der Organisation.
5. Die `tgw-tagger-organizations-account-query` Lambda-Funktion ruft die Organizations-API auf, um AWS-Kontometadaten zurückzugeben.
6. Der Zustandsautomat ruft die `tgw-tagger-attachment-query` Lambda-Funktion auf.
7. Parallel ruft der Zustandsautomat für jede Region die `tgw-tagger-rtb-query` Lambda-Funktion auf, um den CIDR-Bereich für jede Anfügung zu lesen.
8. Parallel ruft der Zustandsautomat für jede Region die `tgw-tagger-attachment-tagger`Lambda-Funktion auf.
9. Namens-Tags werden für Transit-Gateway-Anfügungen im Shared Networking-Konto erstellt.

Automatisierung und Skalierung

Die Lösung verarbeitet jede Region parallel, um die Gesamtdauer des Laufs zu reduzieren.

Tools

AWS-Services

- AWS CloudFormation – AWS CloudFormation bietet eine Möglichkeit, eine Sammlung verwandter AWS- und Drittanbieterressourcen zu modellieren, sie schnell und konsistent bereitzustellen und während ihres gesamten Lebenszyklus zu verwalten, indem Infrastruktur als Code behandelt wird.
- Amazon EventBridge – Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge

empfängt ein Ereignis, einen Indikator für eine Änderung der Umgebung, und wendet eine Regel an, um das Ereignis an ein Ziel weiterzuleiten. Regeln ordnen Ereignisse Zielen zu, die entweder auf der Struktur des Ereignisses, einem so genannten Ereignismuster, oder nach einem Zeitplan basieren.

- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch, von einigen Anfragen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die tatsächlich konsumierte Zeit. Es werden keine Gebühren berechnet, solange Ihr Code nicht ausgeführt wird.
- AWS Organizations – AWS Organizations hilft Ihnen dabei, Ihre Umgebung zentral zu verwalten und zu verwalten, wenn Sie Ihre AWS-Ressourcen vergrößern und skalieren. Mit AWS Organizations können Sie programmgesteuert neue AWS-Konten erstellen und Ressourcen zuweisen, Konten gruppieren, um Ihre Workflows zu organisieren, Richtlinien für die Verwaltung auf Konten oder Gruppen anwenden und die Abrechnung vereinfachen, indem Sie eine einzige Zahlungsweise für alle Ihre Konten verwenden.
- AWS Step Functions – AWS Step Functions ist ein visueller Workflow-Service mit geringem Code, der verwendet wird, um AWS-Services zu orchestrieren, Geschäftsprozesse zu automatisieren und Serverless-Anwendungen zu erstellen. Workflows verwalten Fehler, Wiederholungsversuche, Parallelisierung, Serviceintegrationen und Beobachtbarkeit, sodass sich Entwickler auf eine höherwertige Geschäftslogik konzentrieren können.
- AWS Transit Gateway – AWS Transit Gateway verbindet VPCs und On-Premises-Netzwerke über einen zentralen Hub. Dies vereinfacht Ihr Netzwerk und beendet komplexe Peering-Beziehungen. Sie fungiert als Cloud-Router, sodass jede neue Verbindung nur einmal hergestellt wird.
- Amazon VPC – Amazon Virtual Private Cloud (Amazon VPC) ist ein Service zum Starten von AWS-Ressourcen in einem von Ihnen definierten logisch isolierten virtuellen Netzwerk.
- AWS X-Ray – AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren.

Code

Der Quellcode für diese Lösung ist im Transit Gateway Attachment Tagger GitHub -Repository verfügbar. Das Repository enthält die folgenden Dateien:

- `tgw-attachment-tagger-main-stack.yaml` erstellt alle Ressourcen zur Unterstützung dieser Lösung innerhalb des Shared Networking-Kontos.

- `tgw-attachment-tagger-organizations-stack.yaml`erstellt eine Rolle im Verwaltungskonto der Organisation.

Polen

Bereitstellen des Hauptlösungs-Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie die erforderlichen erforderlichen erforderlichen Informationen.	Um den kontoübergreifende n Zugriff von der Lambda-Fu nktion auf die AWS Organizat ions-API zu konfigurieren, benötigen Sie die Konto-ID für das Verwaltungskonto der Organisation. Hinweis: Die Reihenfolge, in der die beiden CloudForm ation Stacks erstellt werden, ist wichtig. Sie müssen Ressourcen zuerst im Konto Shared Networking bereitste llen. Die Rolle im Shared Networking-Konto muss bereits vorhanden sein, bevor Ressourcen im Verwaltun gskonto der Organisation bereitgestellt werden. Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps Techniker
Starten Sie die CloudForm ation Vorlage für den Hauptlösungs-Stack.	Die Vorlage für den Hauptlösu ngs-Stack stellt die IAM-Rollen, den Step Functions -Workflow, die Lambda-Fu	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nktionen und das CloudWatch Ereignis bereit. Öffnen Sie die AWS-Managementkonsole für das Konto Shared Networking und öffnen Sie dann die CloudFormation Konsole. Erstellen Sie den Stack mithilfe der `tgw-attachment-tagger-main-stack.yaml` Vorlage und der folgenden Werte: • Stack-Name – tgw-attachment-tagger-main-Stack • awsOrganizationsRootAccountId – Konto-ID für das Verwaltungskonto der Organisation • TGWRegions-Parameter – AWS-Regionen für die Lösung, eingegeben als durch Komma getrennte Zeichenfolge • TGWList-Parameter – Transit-Gateway-IDs, die von der Lösung ausgeschlossen werden sollen, eingegeben in einer durch Komma getrennten Zeichenfolge Weitere Informationen zum Starten eines CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stacks finden Sie in der AWS-Dokumentation.	
Überprüfen Sie, ob die Lösung erfolgreich gestartet wurde.	Warten Sie, bis der CloudFormation Stack den Status CREATE_COMPLETE erreicht hat. Dies sollte weniger als eine Minute dauern. Öffnen Sie die Step-Functions-Konsole und überprüfen Sie, ob ein neuer Zustandsautomat mit dem Namen tgw-attac hment-tagger-state-machine erstellt wurde.	DevOps Techniker

Bereitstellen des AWS Organizations-Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie die erforderlichen erforderlichen erforderlichen Informationen.	Um den kontoübergreifende n Zugriff von der Lambda-Fu nktion auf die AWS Organizat ions-API zu konfigurieren, benötigen Sie die -Konto-ID für das Shared Networking-Konto.	DevOps Techniker
Starten der CloudFormation Vorlage für den Organizations-Stack	Die Vorlage für den AWS Organizations-Stack stellt die IAM-Rolle im Verwaltun gskonto der Organisation bereit.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Greifen Sie auf die AWS-Konsole für das Verwaltungskonto der Organisation zu und öffnen Sie dann die - CloudFormation Konsole. Erstellen Sie den Stack mithilfe der `tgw-attachment-tagger-organizations-stack.yaml` Vorlage und der folgenden Werte: • Stack-Name – tgw-attachment-tagger-organizations-Stack • NetworkingAccountId Parameter – Konto-ID für das Konto für freigegebenes Netzwerk Verwenden Sie für die anderen Stack-Erstellungsoptionen die Standardwerte.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lösung erfolgreich gestartet wurde.	Warten Sie, bis der CloudFormation Stack den Status CREATE_COMPLETE erreicht. Dies sollte weniger als eine Minute dauern. Öffnen Sie die Identity and Access Management (IAM)-Konsole und überprüfen Sie, ob eine neue Rolle mit dem Namen tgw-attachment-tag ger-organization-query-role erstellt wurde.	DevOps Techniker

Überprüfen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Zustandsa utomaten aus.	Öffnen Sie die Step Functions-Konsole für das Konto Shared Networking und wählen Sie im Navigationsbereich Zustandsa utomaten aus. Wählen Sie die Zustandsm aschine tgw-attachment-tag ger-state-Maschine und dann Ausführung starten aus. Da die Eingabe für diesen Zustandsautomaten nicht von der Lösung verwendet wird, können Sie den Standardwert verwenden.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	    "Comment": "Insert your JSON here"
	}</pre>
	Wählen Sie Start Execution aus.	

Beobachten Sie den Zustandsautomaten bis zum Abschluss.	Auf der sich öffnenden neuen Seite können Sie die Ausführung des Zustandsautomaten beobachten. Die Dauer hängt von der Anzahl der zu verarbeitenden Transit-Gateway-Anhänge ab. Auf dieser Seite können Sie jeden Schritt des Zustandsautomaten untersuchen. Sie können die verschiedenen Aufgaben innerhalb des Zustandsautomaten anzeigen und Links zu den CloudWatch Protokollen für die Lambda-Funktionen folgen. Für die Aufgaben, die parallel innerhalb der Karte ausgeführt werden, können Sie die Dropdownliste Index verwenden, um die spezifischen Implementierungen für jede Region anzuzeigen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Transit-Gateway-Anfügungs-Tags.	Öffnen Sie die VPC-Konsole für das Konto für freigegebenes Netzwerk und wählen Sie Transit-Gateway-Anhänge aus. In der Konsole wird ein Namens-Tag für Anlagen bereitgestellt, die die Kriterien erfüllt haben (der Anhang wird an eine Transit-Gateway-Routing-Tabelle weitergegeben und der Ressourcenbesitzer ist Mitglied der Organisation).	DevOps Techniker
Überprüfen Sie die CloudWatch Ereignisauslösung.	Warten Sie, bis das CloudWatch Ereignis ausgelöst wurde. Dies ist für 06:00 Uhr UTC geplant. Öffnen Sie dann die Step-Functions-Konsole für das Konto Shared Networking und wählen Sie im Navigationsbereich Zustandsautomaten aus. Wählen Sie die Zustandsmaschine tgw-attachment-tagger-state-Maschine aus. Stellen Sie sicher, dass die Lösung um 06:00 Uhr UTC ausgeführt wurde.	DevOps Techniker

Zugehörige Ressourcen

- AWS Organizations

- AWS Resource Access Manager
- Serverless Transit Network Orchestrator
- Erstellen von IAM-Rollen
- Erstellen eines Stacks in der AWS- CloudFormation Konsole

Stellen Sie sicher, dass ELB-Load Balancer eine TLS-Beendigung erfordern

Erstellt von Priyanka Chaudhary (AWS)

Umgebung: Produktion	Technologien: Netzwerk, Sicherheit, Identität, Compliance	AWS-Services: Amazon CloudWatch Events; Elastic Load Balancing (ELB); AWS Lambda

Übersicht

In der Amazon Web Services (AWS) Cloud verteilt Elastic Load Balancing (ELB) eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container, IP-Adressen und AWS Lambda-Funktionen. Die Load Balancer verwenden Listener, um die Ports und Protokolle zu definieren, die der Load Balancer verwendet, um Datenverkehr von Benutzern zu akzeptieren. Application Load Balancer treffen Routing-Entscheidungen auf Anwendungsebene und verwenden die HTTP/HTTPS-Protokolle. Classic Load Balancer treffen Routing-Entscheidungen entweder auf der Transportebene, mithilfe von TCP- oder Secure Sockets Layer (SSL)-Protokollen oder auf Anwendungsebene, indem sie HTTP/HTTPS verwenden.

Dieses Muster bietet eine Sicherheitskontrolle, die mehrere Ereignistypen für Application Load Balancer und Classic Load Balancer untersucht. Wenn die Funktion aufgerufen wird, überprüft AWS Lambda das Ereignis und stellt sicher, dass der Load Balancer konform ist.

Die Funktion initiiert ein Amazon CloudWatch Events-Ereignis für die folgenden API-Aufrufe: CreateLoadBalancer, CreateLoadBalancerListeners, DeleteLoadBalancerListeners, CreateLoadBalancerPolicy, SetLoadBalancerPoliciesOfListener, CreateListenerDeleteListener, und ModifyListener. Wenn das Ereignis eine dieser APIs erkennt, ruft es AWS Lambda auf, das ein Python-Skript ausführt. Das Python-Skript prüft, ob der Listener ein SSL-Zertifikat enthält und ob die angewendete Richtlinie Transport Layer Security (TLS) verwendet. Wenn festgestellt wird, dass es sich bei der SSL-Richtlinie um etwas anderes als TLS handelt, sendet die Funktion eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung mit den entsprechenden Informationen an den Benutzer.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

Einschränkungen

- Diese Sicherheitskontrolle sucht nicht nach vorhandenen Load Balancern, es sei denn, es wird eine Aktualisierung der Load-Balancer-Listener vorgenommen.
- Diese Sicherheitskontrolle ist regional. Sie müssen sie in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten.
- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.

- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `ELBRequirestlstermination.zip` – Der Lambda-Code für die Sicherheitskontrolle.
- `ELBRequirestlstermination.yml` – Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Polen

Einrichten des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket zum Hosten der ZIP-Datei des Lambda-Codes. Dieser S3-Bucket muss sich in derselben AWS-Region befinden wie der Load Balancer, den Sie auswerten möchten. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konten gemeinsam	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	genutzt. Der S3-Bucket-Name darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie den Lambda-Code (`ELBRequirestlstermination.zip` -Datei), der im Abschnitt Anhänge bereitgestellt wird, in den S3-Bucket hoch.	Cloud-Architekt

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die AWS-CloudFormation Vorlage.	Öffnen Sie die AWS-CloudFormation Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die angehängte Vorlage bereit`ELBRequirestlstermination.yml` . Weitere Informationen zum Bereitstellen von AWS-CloudFormation Vorlagen finden Sie unter Erstellen eines Stacks in der AWS-CloudFormation Konsole in der - CloudFormation Dokumentation.	Cloud-Architekt
Schließen Sie die Parameter in der Vorlage ab.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert:	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• S3-Bucket: Geben Sie den Bucket an, den Sie im ersten Epos erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (`ELBRequirestlstermination.zip` -Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. `ELBRequirestlstermination.zip` oder `controls/ELBRequirestlstermination.zip`). Schließen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, an die Sie Amazon SNS-Benachrichtigungen erhalten möchten. • Lambda-Protokollierungsebene: Geben Sie die Protokollierungsebene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen zum Fortschritt, Fehler bei	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Fehlerereignissen, die die Bereitstellung weiterhin zulassen würden, und Warnung bei potenziell schädlichen Situationen zu protokollieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines Stacks in der AWS- CloudFormation Konsole (AWS- CloudFormation Dokumentation)
- Was ist AWS Lambda? (AWS Lambda-Dokumentation)
- Was ist ein Classic Load Balancer? (ELB-Dokumentation)
- Was ist ein Application Load Balancer? (ELB-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen

Erstellt von Ivo Pinto

Umgebung: PoC oder Pilot	Technologien: Netzwerke; Cloud-nativ; Bereitstellung von Inhalten; Betrieb; Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Services: Amazon CloudWatch; Amazon CloudWatch Logs; AWS-Netzwerk-Firewall		

Übersicht

Viele Unternehmen verwenden Splunk Enterprise als zentralisiertes Aggregations- und Visualisierungstool für Logs und Metriken aus verschiedenen Quellen. Dieses Muster hilft Ihnen, Splunk so zu konfigurieren, dass mithilfe des Splunk-Add-Ons für AWS Protokolle und Metriken der AWS Network Firewall von Amazon CloudWatch Logs abgerufen werden.

Um dies zu erreichen, erstellen Sie eine schreibgeschützte AWS Identity and Access Management (IAM) -Rolle. Splunk Add-On für AWS verwendet diese Rolle für den Zugriff. CloudWatch Sie konfigurieren das Splunk Add-On für AWS zum Abrufen von Metriken und Protokollen von. CloudWatch Schließlich erstellen Sie Visualisierungen in Splunk aus den abgerufenen Protokolldaten und Metriken.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Splunk-Konto
- Eine Splunk Enterprise-Instanz, Version 8.2.2 oder höher
- Ein aktives AWS-Konto
- Network Firewall, eingerichtet und konfiguriert, um Protokolle an Logs zu CloudWatch senden

Einschränkungen

- Splunk Enterprise muss als Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der AWS-Cloud bereitgestellt werden.
- Das Sammeln von Daten mithilfe einer automatisch erkannten IAM-Rolle für Amazon EC2 wird in den AWS-Regionen China nicht unterstützt.

Architektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Die Network Firewall veröffentlicht CloudWatch Protokolle in Logs.
2. Splunk Enterprise ruft Metriken und Protokolle von ab. CloudWatch

Um Beispielmetriken und Logs in dieser Architektur aufzufüllen, generiert ein Workload Traffic, der über den Netzwerk-Firewall-Endpunkt ins Internet geleitet wird. Dies wird durch die Verwendung von Routentabellen erreicht. Obwohl dieses Muster eine einzelne Amazon EC2 EC2-Instance als Workload verwendet, kann dieses Muster für jede Architektur gelten, sofern die Network Firewall so konfiguriert ist, dass sie CloudWatch Protokolle an Logs sendet.

Diese Architektur verwendet auch eine Splunk Enterprise-Instanz in einer anderen Virtual Private Cloud (VPC). Die Splunk-Instance kann sich jedoch an einem anderen Standort befinden, z. B. in derselben VPC wie der Workload, sofern sie die APIs erreichen kann. CloudWatch

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Die AWS Network Firewall ist ein zustandsbehafteter, verwalteter Netzwerk-Firewall sowie Service zur Erkennung und Verhinderung von Eindringlingen für VPCs in der AWS-Cloud.

Andere Tools

- Splunk unterstützt Sie bei der Überwachung, Visualisierung und Analyse von Protokolldaten.

Epen

Erstellen einer IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie.	Folgen Sie den Anweisungen unter Richtlinien mit dem JSON-Editor erstellen, um die IAM-Richtlinie zu erstellen, die schreibgeschützten Zugriff auf die CloudWatch Logs-Daten und -Metriken gewährt. CloudWatch Fügen Sie die folgende -Richtlinie in den JSON-Editor ein. `{ "Statement": [ { "Action": [ "cloudwatch:List*", "cloudwatch:Get*", "network-firewall:List*", "logs:Describe*", "logs:Get*", "logs:List*", "logs:StartQuery",`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"logs:StopQuery",
	
	"logs:TestMetricFi
	lter",
	
	"logs:FilterLogEve
	nts",
	
	"network-firewall:
	Describe*"
	],
	"Effect":
	"Allow",
	"Resource":
	"*"
	}
	],
	"Version":
	"2012-10-17"
	}</pre>	

Erstellen Sie eine neue IAM-Rolle.	Folgen Sie den Anweisungen unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service, um die IAM-Rolle zu erstellen, auf die das Splunk Add-On für AWS zugreift. CloudWatch Wählen Sie für Berechtigungsrichtlinien die Richtlinie aus, die Sie zuvor erstellt haben.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie den EC2-Instances im Splunk-Cluster die IAM-Rolle zu.	1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. 2. Wählen Sie im Navigationsbereich Instances aus. 3. Wählen Sie die EC2-Instances im Splunk-Cluster aus. 4. Wählen Sie Aktionen, Sicherheit und dann IAM-Rolle ändern aus. 5. Wählen Sie die IAM-Rolle aus, die Sie zuvor erstellt haben, und klicken Sie dann auf Speichern.	AWS-Administrator

Installieren Sie das Splunk-Add-On für AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das Add-on.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Apps. 2. Suchen Sie nach dem Splunk-Add-on für Amazon Web Services. 3. Wählen Sie Installieren aus. 4. Geben Sie Ihre Splunk-Anmeldeinformationen ein.	Splunk-Administrator
Konfigurieren Sie die AWS-Anmeldeinformationen.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Add-on for AWS. 2. Wählen Sie Konfiguration.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie in der Spalte Autodiscovered IAM Role die IAM-Rolle aus, die Sie zuvor erstellt haben. Weitere Informationen finden Sie in der Splunk-Dokumentation unter Suchen Sie eine IAM-Rolle in Ihrer Splunk-Plattform-Instance.	

Konfigurieren Sie den Splunk-Zugriff auf CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Abruf von Netzwerk-Firewall-Protokollen aus CloudWatch Protokollen.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Add-on for AWS. 2. Wählen Sie Eingabe. 3. Wählen Sie Neue Eingabe erstellen. 4. Wählen Sie in der Liste Benutzerdefinierter Datentyp und dann CloudWatch Protokolle aus. 5. Geben Sie den Namen, das AWS-Konto, die AWS-Region und die Protokoll gruppe für Ihre Netzwerk-Firewall-Protokolle an. 6. Wählen Sie Speichern.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardmäßig ruft Splunk die Protokolldaten alle 10 Minuten ab. Dies ist ein konfigurierbarer Parameter unter Erweiterte Einstellungen. Weitere Informationen finden Sie in der Splunk-Dokumentation unter Konfiguration einer CloudWatch Log-Eingabe mit Splunk Web.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Abruf von Netzwerk-Firewall-Metriken von CloudWatch.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Add-on for AWS. 2. Wählen Sie Eingabe. 3. Wählen Sie Neue Eingabe erstellen. 4. Wählen Sie in der Liste CloudWatch. 5. Geben Sie den Namen, das AWS-Konto und die AWS-Region für Ihre Netzwerk-Firewall-Metriken an. 6. Wählen Sie neben Metric Configuration die Option Im erweiterten Modus bearbeiten aus. 7. (Optional) Löschen Sie alle vorkonfigurierten Namespaces. 8. Wählen Sie Add Namespace und nennen Sie ihn dann NetworkFirewallAWS/. 9. Fügen Sie unter Dimensionswert Folgendes hinzu. `[{"AvailabilityZone":[".*"],"Engine":[".*"],"FirewallName":[".*"]}]` 10. Wählen Sie für Metriken die Option Alle aus.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie für Metrische Statistiken die Option Summe aus. 12. Wählen Sie OK aus. 13. Wählen Sie Speichern. Standardmäßig ruft Splunk die Metrikdaten alle 5 Minuten ab. Dies ist ein konfigurierbarer Parameter unter Erweitert e Einstellungen. Weitere Informationen finden Sie in der Splunk-Dokumentati on unter Eine CloudWatch Eingabe mithilfe von Splunk Web konfigurieren.	

Erstellen Sie Splunk-Visualisierungen mithilfe von Abfragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die wichtigsten Quell-IP-Adressen an.	1. Navigieren Sie im Splunk-Dashboard zu Search & Reporting. 2. Geben Sie im Feld „Suche hier eingeben“ Folgendes ein. `sourcetype="aws:cl oudwatchlogs" | top event.src_ip` Diese Abfrage zeigt eine Tabelle mit den Quell-IP-	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Adressen mit dem meisten Verkehr in absteigender Reihenfolge an. 3. Für eine grafische Darstellung wählen Sie Visualization.	
Paketstatistiken anzeigen.	1. Navigieren Sie im Splunk-Dashboard zu Search & Reporting. 2. Geben Sie im Feld „Suche hier eingeben“ Folgendes ein. `sourcetype="aws:cloudwatch"| timechart sum(Sum) by metric_name` Diese Abfrage zeigt eine Tabelle mit den Metriken `DroppedPackets` `PassedPackets` , und `ReceivedPackets` pro Minute an. 3. Wählen Sie für eine grafische Darstellung Visualization aus.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die am häufigsten verwendeten Quellports an.	1. Navigieren Sie im Splunk-Dashboard zu Search & Reporting. 2. Geben Sie im Feld „Suche hier eingeben“ Folgendes ein. `sourcetype="aws:cloudwatchlogs" | top event.dest_port` Diese Abfrage zeigt eine Tabelle der Quellports mit dem meisten Verkehr in absteigender Reihenfolge an. 3. Für eine grafische Darstellung wählen Sie Visualisierung.	Splunk-Administrator

Zugehörige Ressourcen

AWS-Dokumentation

- Eine Rolle erstellen, um Berechtigungen an einen AWS-Service zu delegieren (IAM-Dokumentation)
- IAM-Richtlinien erstellen (IAM-Dokumentation)
- Protokollierung und Überwachung in der AWS-Netzwerk-Firewall (Netzwerk-Firewall-Dokumentation)
- Routentabellenkonfigurationen für die AWS-Netzwerk-Firewall (Netzwerk-Firewall-Dokumentation)

AWS-Blogbeiträge

- Bereitstellungsmodelle für AWS-Netzwerk-Firewalls

AWS Marketplace

- Splunk Enterprise Amazon Machine Image (AMI)

Mehr Muster

- Zugreifen auf einen Bastion-Host mithilfe von Session Manager und Amazon EC2 Instance Connect
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- ???
- Suchen Sie nach Netzwerkeinträgen mit einem Host in den Eingangsregeln für Sicherheitsgruppen für IPv4 und IPv6
- Bereitstellen einer Firewall mit AWS Network Firewall und AWS Transit Gateway
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Stellen Sie mithilfe von AWS Config detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit
- ???
- Aktivieren verschlüsselter Verbindungen für PostgreSQL-DB-Instances in Amazon RDS
- Erweitern Sie VRFs auf AWS mithilfe von AWS Transit Gateway Connect
- Migrieren eines F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS Cloud
- Aufbewahren von routbarem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze, die keine Workload sind
- Verhindern Sie den Internetzugang auf Kontoebene mithilfe einer Dienststeuerungsrichtlinie
- Senden von Warnungen von AWS Network Firewall an einen Slack-Kanal
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Einrichten der Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery
- Einrichten der DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit mehreren Konten
- Verwenden Sie Bol Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren
- Verwenden Sie die Network Firewall, um die DNS-Domänennamen von der Server Name Indication (SNI) für ausgehenden Datenverkehr zu erfassen

Betriebssysteme

Themen

Migrieren Sie RHEL-BYOL-Systeme mithilfe von AWS MGN zu Instances mit AWS-Lizenz

Erstellt von Mike Kuznetsov (AWS)

Umgebung: Produktion	Quelle: RHEL BYOL-Instanz (vor Ort oder in einer anderen Cloud-Umgebung)	Ziel: RHEL-Instance inklusive AWS-Lizenz
R-Typ: Rehost	Arbeitslast: Alle anderen Workloads	Technologien: Betriebssysteme; Infrastruktur; Migration
AWS-Services: AWS-Anwendungsmigrationsservice		

Übersicht

Wenn Sie Ihre Workloads mithilfe von AWS Application Migration Service (AWS MGN) zu AWS migrieren, müssen Sie möglicherweise Ihre Red Hat Enterprise Linux (RHEL) -Instances hochziehen (rehosten) und die Lizenz während der Migration vom Standardmodell Bring Your Own License (BYOL) auf ein AWS-Lizenzmodell (LI) ändern. AWS MGN unterstützt einen skalierbaren Ansatz, der Amazon Machine Image (AMI) -IDs verwendet. Dieses Muster beschreibt, wie die Lizenzänderung auf RHEL-Servern während der Rehost-Migration in großem Umfang durchgeführt werden kann. Außerdem wird erklärt, wie Sie die Lizenz für ein RHEL-System ändern können, das bereits auf Amazon Elastic Compute Cloud (Amazon EC2) läuft.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zugriff auf das AWS-Zielkonto
- AWS MGN wurde im AWS-Zielkonto und in der Region für die Migration initialisiert (nicht erforderlich, wenn Sie bereits von Ihrem lokalen System zu AWS migriert haben)
- Ein RHEL-Quellserver mit einer gültigen RHEL-Lizenz

Architektur

Dieses Muster deckt zwei Szenarien ab:

- Migrieren Sie ein System mithilfe von AWS MGN direkt von einem lokalen System in eine AWS LI-Instance. Folgen Sie für dieses Szenario den Anweisungen im ersten Epic (Migration zur LI-Instance — Option 1) und im dritten Epic.
- Änderung des Lizenzmodells von BYOL auf LI für ein zuvor migriertes RHEL-System, das bereits auf Amazon EC2 läuft. Folgen Sie für dieses Szenario den Anweisungen im zweiten Epic (Migration zur LI-Instance — Option 2) und im dritten Epic.

Hinweis: Das dritte Epic beinhaltet die Neukonfiguration der neuen RHEL-Instance, um die von AWS bereitgestellten Red Hat Update Infrastructure (RHUI) -Server zu verwenden. Dieser Prozess ist für beide Szenarien derselbe.

Tools

AWS-Services

- Mit dem AWS Application Migration Service (AWS MGN) können Sie Anwendungen ohne Änderungen und mit minimalen Ausfallzeiten in die AWS-Cloud rehosten (Lift and Shift).

Epen

Zur LI-Instanz migrieren — Option 1 (für ein lokales RHEL-System)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie die AMI-ID der RHEL AWS LI-Instance in der Zielregion.	Besuchen Sie AWS Marketplace oder verwenden Sie die Amazon EC2 EC2-Konsole, um die RHEL-AMI-ID zu finden, die der Version des RHEL-Quellsystems entspricht (z. B. RHEL-7.7), und notieren Sie sich die AMI-ID. In der Amazon EC2	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2-Konsole können Sie die AMIs mit einem der folgenden Suchbegriffe filtern: • Beschreibung = Bereitgestellt von Red Hat, Inc. • AMI-Name = RHEL-7.7	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS MGN-Starteinstellungen.	1. Fügen Sie auf der AWS MGN-Konsole das RHEL-Quellsystem hinzu: Installieren Sie den AWS Replication Agent und fügen Sie den Quellserver hinzu, indem Sie den Anweisungen in der AWS MGN-Dokumentation folgen. 2. Wählen Sie auf der Seite Quellserver das RHEL-Quellsystem und dann die Registerkarte Starteinstellungen aus. 3. Wählen Sie im Abschnitt Allgemeine Starteinstellungen die Option Bearbeiten aus. Um die automatische Auswahl zu deaktivieren und den Zielinstanztyp manuell anzugeben, ändern Sie die Größe des Instanztyps auf Keine und wählen Sie dann Einstellungen speichern. Auf diese Weise können Sie den Instance-Typ verwenden, den Sie in Ihrer Amazon EC2 EC2-Startvorlage konfigurieren. Weitere Informationen finden Sie in der AWS MGN-Dokumentation.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Abschnitt EC2 Launch Template die Option Modify aus. Wählen Sie im Dialogfeld „Informationen zum Ändern von EC2-Startvorlagen“ erneut die Option Ändern aus. Dadurch wird die Amazon EC2 EC2-Konsole geöffnet, sodass Sie die Vorlage für diese Instance ändern können. 5. Lesen Sie die wichtigsten Überlegungen in der AWS MGN-Dokumentation. Hinweis: Sie können die Warnung vor der Auswahl Ihres eigenen AMI ignorieren. 6. Ändern Sie auf der Amazon EC2 EC2-Konsole in der neuen Startvorlage Folgendes: • Geben Sie für AMI die AMI-ID an, die Sie zuvor identifiziert haben, oder suchen Sie nach RHEL- x und geben Sie die Version an, die Sie benötigen (z. B. RHEL-7.7). • Stellen Sie unter Instance-Typ den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gewünschten Ziel-Instance-Typ ein. • Lassen Sie die folgenden Abschnitte unverändert: Schlüsselpaar (Anmeldung), Netzwerkeinstellungen (sofern Sie kein Zielsubnetz und Sicherheitsgruppen angeben möchten), Speicher, Ressourcen-Tags (sofern Sie keine Tags hinzufügen oder ändern möchten). • (Optional) Geben Sie im Abschnitt Erweiterte Details die Rolle des IAM-Instance-Profils an, falls dies für die future Verwaltung durch AWS Systems Manager erforderlich ist. 7. Wählen Sie Vorlagenversion erstellen und wählen Sie dann den Link in der Erfolgsmeldung, um die Startvorlage anzuzeigen. 8. Wählen Sie „Aktionen“, „Standardversion festlegen“. Wählen Sie unter Vorlagenversion die neueste Version aus (Version 2 für ein neues System) und wählen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann Als Standardversion festlegen aus. AWS MGN wird nun diese Version der Startvorlage verwenden, um Test- oder Cutover-Instances zu starten. Weitere Informationen finden Sie in der AWS MGN-Dokumentation.	
Einstellungen validieren.	1. Wählen Sie in der AWS MGN-Konsole auf der Seite Quellserver Ihren Quellserver und dann die Registerkarte Starteinstellungen aus. 2. Vergewissern Sie sich im Abschnitt EC2 Launch Template, dass die Parameter Instance-Typ, Subnetz und Sicherheitsgruppen korrekt eingestellt sind. Hinweis: In diesem Abschnitt wird die von Ihnen ausgewählte AMI-ID nicht angezeigt. Um die ID zu sehen, können Sie die Amazon EC2 EC2-Konsole in der Ansicht Vorlagen starten öffnen und nach der Vorlagen-ID suchen, die in diesem Abschnitt angezeigt wird.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die neue LI-Instanz.	1. Wenn die erste Synchronisierung abgeschlossen ist, ändert sich die Spalte Migrationslebenszyklus für den Server auf der Seite Quellserver der AWS-MGN-Konsole in Bereit zum Testen. Um die neue Test-Instance zu starten, wählen Sie Ihren Quellserver aus, öffnen Sie das Menü Test und Übernahme und wählen Sie dann Test-Instances starten. Wählen Sie Jobdetails anzeigen, um den Status des Startjobs zu überwachen. Weitere Informationen finden Sie in der AWS MGN-Dokumentation. 2. Warten Sie, bis der Startjob abgeschlossen ist, und öffnen Sie dann die Detailseite der gestarteten EC2-Instance. Wählen Sie die Registerkarte Details und vergewissern Sie sich, dass der Abschnitt mit den Instanzdetails Folgendes enthält: • Plattformdetails: „Red Hat Enterprise Linux“ • AMI-Name: Der Name des AMI, das Sie in	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der EC2-Startvorlage angegeben haben 3. Wechseln Sie zur neuen LI-Instance, indem Sie den Anweisungen in der AWS MGN-Dokumentation folgen. 4. Konfigurieren Sie die neue Instanz neu, sodass sie die von AWS bereitgestellten RHUI-Server verwendet, indem Sie die Schritte im letzten Epic befolgen.	

Zur LI-Instanz migrieren — Option 2 (für eine RHEL BYOL EC2-Instanz)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Ihre RHEL BYOL EC2-Instance zu einer AWS LI-Instance.	Sie können RHEL-Systeme, die Sie zuvor als BYOL zu AWS migriert haben, zu AWS LI-Instances wechseln, indem Sie ihre Festplatten (Amazon Elastic Block Store-Volumes) verschieben und sie an eine neue LI-Instance anhängen. Gehen Sie wie folgt vor, um diesen Wechsel vorzunehmen: 1. Starten Sie eine neue RHEL-Zielinstanz von einem RHEL LI AMI aus. Vergewissern Sie sich, dass	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das von Ihnen gewählte AMI: • Verwendet dieselbe RHEL-Version wie Ihre aktuelle RHEL-Instance. • Hat denselben Startvorg ang (BIOS oder UEFI) wie Ihre aktuelle RHEL-Instanz. Wenn der Quellserver beispiels weise BIOS-basiert ist, verwenden Sie das AWS Marketplace RHEL AMI, das ebenfalls BIOS-basi ert ist. Wählen Sie für UEFI-basierte Systeme das UEFI-basierte AMI. 2. Stoppen Sie beide Instances: die neue LI-Instance und die ursprüngl iche Quell-Instance. 3. Trennen Sie alle EBS-Volumes (einschließlich der Root-Festplatte) von der neuen LI-Instanz und löschen Sie sie. 4. Trennen Sie alle EBS-Volumes (einschließlich der Root-Festplatte) von der alten Quell-Instance und fügen Sie sie der neuen LI-Instance hinzu. Behalten Sie die gleiche Zuordnung von Volumes zu Geräten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bei. (Beispielsweise muss das EBS-Volume, das zuvor an das `/dev/sda` Laufwerk angeschlossen war, genauso wie das EBS-Volume `/dev/sda` an die neue Instanz angehängt werden.) 5. Löschen Sie die Quellinst anz (jetzt ohne Festplatte). 6. Starten Sie die neue LI-Instanz. Melden Sie sich bei der Instance an und konfigurieren Sie sie neu, um die von AWS bereitges tellten RHUI-Server zu verwenden, indem Sie die Schritte im nächsten Epic befolgen.	

Neukonfiguration von RHEL OS zur Verwendung von AWS-bereitgestelltem RHUI — beide Optionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie das Betriebss ystem vom Red Hat Abonnement und der Lizenz ab.	Nach der Migration und der erfolgreichen Umstellung muss das RHEL-System aus dem Red Hat-Abonnement entfernt werden, um den Verbrauch der Red Hat-Lizen z zu beenden und Doppelabr echnungen zu vermeiden.	Linux oder Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um RHEL OS aus dem Red Hat-Abonnement zu entfernen, folgen Sie dem in der Dokumentation zu Red Hat Subscription Management (RHSM) beschriebenen Prozess. Verwendung des -CLI-Befehls: `subscription-manager unregister` Sie können das Subscription Manager-Plugin auch deaktivieren, um den Status des Abonnements nicht mehr bei jedem Yum-Anruf zu überprüfen. Bearbeiten Sie dazu die Konfigurationsdatei `/etc/yum/pluginconf.d/subscription-manager.conf` und ändern Sie den Parameter `enabled=1` auf `enabled=0`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ersetzen Sie die alte Update-Konfiguration (RHUI, Red Hat Satellite Network, Yum-Repositorys) durch das von AWS bereitgestellte RHUI.	Sie müssen das migrierte RHEL-System neu konfigurieren, um die von AWS bereitgestellten RHUI-Server zu verwenden. Dadurch erhalten Sie Zugriff auf die RHUI-Server innerhalb der AWS-Regionen, ohne dass eine externe Update-Infrastruktur erforderlich ist. Die Änderung umfasst den folgenden Prozess: 1. Erstellen Sie eine Sicherungskopie der vorhandenen Yum-Konfiguration. 2. Entfernen Sie die alte RHUI-Konfiguration (Yum-Repositories) und die alten Pakete. 3. Fügen Sie die neuen von AWS bereitgestellten RHUI-Konfiguration und die Zertifikatspakete hinzu. Sie müssen diese von einer anderen RHEL-Instance auf AWS abrufen, da diese Konfigurationspakete nur auf von AWS bereitgestellten RHUI-Servern verfügbar sind.	Linux oder Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Hier sind die detaillierten Schritte und Befehle:
	
	1. Sichern Sie die bestehende Yum-Konfiguration und die Zertifikate, indem Sie alle `/etc/pki/*` Ordner `/etc/yum*` und an einen Backup-Speicherort kopieren. Beispielsweise:
	
	`mkdir yum-backup`
	`cp -ra /etc/yum* /etc/pki ./yum-backup`
	`tar czf yum-backup.tgz ./yum-backup`
	
	2. Entfernen Sie die alte RHUI-Konfiguration und die Pakete:
	
	a. Finden Sie alle installierten RHUI-Pakete:
	
	`sudo rpm -qa | grep rhui`
	
	b. Löschen Sie diese Pakete:
	
	`sudo yum remove $(rpm -qa | grep rhui)`
	
	c. Entfernen Sie die `/etc/yum/vars/releasever` Datei, falls sie existiert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Fügen Sie die neuen von AWS bereitgestellten RHUI- und Zertifikatspakete hinzu. Sie müssen diese von einer anderen RHEL-Instance auf AWS abrufen. Dazu stehen verschiedene Möglichke iten zur Verfügung. Sie können beispielsweise den Anweisungen im Red Hat Knowledgebase-Artikel folgen: a. Starten Sie eine weitere RHEL-Instance (RHEL-EC2) über den AWS Marketplace. b. Laden Sie zwei Pakete von dieser Instance herunter: das neueste RHUI-Client-Konfig urationspaket und die Zertifikate der Zertifizi erungsstelle (CA). Führen Sie beispiels weise diesen Befehl von Ihrem Desktop aus aus: `ssh RHEL-EC2 "sudo yumdownloader ca-certificates rh-amazon-rhui-cli ent"` c. Kopieren Sie die Pakete von der RHEL-EC2-Instanz auf das neue	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	migrierte System. Beispielsweise:
	`scp RHEL-EC2:rh-amazon-rhui-client\* RHEL-EC2:ca-certificates\* . ssh <migrated-instance> "mkdir /tmp/amazon" scp rh-amazon-rhui-client* ca-certificates* <migrated-instance>:/tmp/amazon`
	d. Installieren Sie die neuen RHUI- und CA-Konfigurationspakete auf der migrierten Instanz:
	`ssh <migrated-instance> "sudo rpm -Uhv /tmp/amazon/*"`	

Überprüfen Sie die Konfiguration.	Stellen Sie auf der migrierten Zielinstanz sicher, dass die neue Konfiguration korrekt ist: `sudo yum clean all sudo yum repolist`	Linux oder Systemadministrator

Zugehörige Ressourcen

- AWS Application Migration Service (AWS MGN) — Benutzerhandbuch

- Holen Sie sich ein AWS RHUI-Clientpaket, das IMDSv2 unterstützt (Artikel in der Red Hat Knowledgebase)
- Amazon EC2 EC2-Startvorlagen (Amazon EC2 EC2-Dokumentation)

Beheben von Verbindungsfehlern nach der Migration von Microsoft SQL Server zur AWS Cloud

Erstellt von Premkumar Chelladurai (AWS)

Umgebung: Produktion	Technologien: Betriebssysteme; Migration	Workload: Microsoft
AWS-Services: Amazon EC2		

Übersicht

Nachdem Sie Microsoft SQL Server auf Windows Server 2008 R2, 2012 oder 2012 R2 zu Amazon Elastic Compute Cloud (Amazon EC2)-Instances in der Amazon Web Services (AWS) Cloud migriert haben, schlägt die Verbindung zu SQL Server fehl und die folgenden Fehler werden angezeigt:

- `[Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error`
- `ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure. System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`
- `TCP Provider: The semaphore timeout period has expired`

Dieses Muster beschreibt, wie Sie diese Fehler beheben können, indem Sie die Windows Scalable Networking Pack (SNP)-Funktionen auf Betriebssystem- (OS) und Netzwerkschnittstellenebene für SQL Server deaktivieren, der auf Windows Server 2008 R2, 2012 oder 2012 R2 ausgeführt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Administratorrechte für Windows Server.
- Wenn Sie AWS Application Migration Service als Migrationstool verwendet haben, benötigen Sie eine der folgenden Windows Server-Versionen:
  - Windows Server 2008 R2 Service Pack 1, 2012 oder 2012 R2

- Wenn Sie CloudEndure Migration als Migrationstool verwendet haben, benötigen Sie eine der folgenden Windows Server-Versionen:
  - Windows Server 2003 R2 Service Pack 3, 2008, 2008 R2 Service Pack 1, 2012 oder 2012 R2

Tools

- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können Amazon EC2 verwenden, um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können auf- oder abskalieren.
- Windows Server – Windows Server ist eine Plattform zum Aufbau einer Infrastruktur mit verbundenen Anwendungen, Netzwerken und Webservices.

Polen

Deaktivieren von SNP-Funktionen auf Betriebssystem- und Elastic-Network-Schnittstellenebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie die SNP-Funktionen auf Betriebssystemebene.	1. Melden Sie sich bei Windows Server an und öffnen Sie eine Eingabeaufforderung als Administrator. 2. Führen Sie den Befehl `netsh int tcp show global` aus. 3. Überprüfen Sie in der Ausgabe, ob sich entweder `Receive-Side Scaling` oder `Chimney Offload` im `enabled` Modus befindet. Wenn einer von ihnen ist`enabled`, führen Sie die folgenden Befehle aus:	AWS-Administrator, AWS-Systemadministrator, Migrationsingenieur, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `netsh int tcp set global chimney=disabled` • `netsh int tcp set global rss=disabled`	
Deaktivieren Sie die SNP-Funktionen auf der Ebene der Elastic Network-Schnittstelle.	1. Wählen Sie Start, geben Sie ein `ncpa.cpl` und drücken Sie dann die Eingabetaste. 2. Klicken Sie mit der rechten Maustaste auf Elastic Network Adapter . 3. Wählen Sie im Popup-Menü Eigenschaften aus. 4. Wählen Sie im Fenster Ethernet Adapter Properties die Option Configure aus. 5. Wählen Sie im Popup-Fenster Eigenschaften des Amazon Elastic Network Adapters die Registerkarte Erweitert aus. 6. Deaktivieren Sie im Abschnitt Eigenschaft alle Auslagerungen und RSS.	AWS-Administrator, Cloud-Administrator, AWS-Systemadministrator

Zugehörige Ressourcen

- Fehlerbehebung bei erweiterten Netzwerkleistungsfunktionen wie RSS und NetDMA

Mehr Muster

- Sichern von SunSpeedRC-Servern im Stromasys Charon-SSP-Emulator in der AWS Cloud
- ???
- Migrieren einer lokalen Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server mithilfe nativer Sicherungs- und Wiederherstellungsmethoden
- Migrieren Sie Db2 für LUW zu Amazon EC2 mit Notfallwiederherstellung für hohe Verfügbarkeit
- Überwachen von SAP RHEL-Pacemaker-Clustern mithilfe von AWS-Services
- ???
- Starten Sie den AWS Replication Agent automatisch neu, ohne SELinux nach dem Neustart eines RHEL-Quellservers zu deaktivieren

Operationen

Themen

Automatisches Erstellen eines RFC in AMS mit Python

Erstellt von Gnanasekaranlasam (AWS)

Umgebung: Produktion	Technologien: Betrieb; Cloudnativ	AWS-Services: AWS Managed Services

Übersicht

AWS Managed Services (AMS) hilft Ihnen, Ihre cloudbasierte Infrastruktur effizienter und sicherer zu betreiben, indem es die kontinuierliche Verwaltung Ihrer Amazon Web Services (AWS)-Infrastruktur ermöglicht. Um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen, müssen Sie eine neue Änderungsanforderung (RFC) erstellen und einreichen, die eine Änderungstyp-ID (CT) für eine bestimmte Operation oder Aktion enthält.

Die manuelle Erstellung eines RFC kann jedoch etwa fünf Minuten dauern und Teams in Ihrer Organisation müssen möglicherweise jeden Tag mehrere RFCs einreichen. Dieses Muster hilft Ihnen, den RFC-Erstellungsprozess zu automatisieren, die Erstellungszeit für jeden RFC zu reduzieren und manuelle Fehler zu vermeiden.

Dieses Muster beschreibt, wie Sie Python-Code verwenden, um automatisch das `Stop EC2 instance` RFC zu erstellen, das Amazon Elastic Compute Cloud (Amazon EC2)-Instances in Ihrem AMS-Konto stoppt. Anschließend können Sie den Ansatz dieses Musters und die Python-Automatisierung auf andere RFC-Typen anwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AMS-Advanced-Konto. Weitere Informationen dazu finden Sie unter AMS-Betriebspläne in der AWS Managed Services-Dokumentation.
- Mindestens eine vorhandene EC2-Instance in Ihrem AMS-Konto.
- Ein Verständnis dafür, wie RFCs in AMS erstellt und übermittelt werden.
- Vertrautheit mit Python.

Einschränkungen

- Sie können RFCs nur für Änderungen in Ihrem AMS-Konto verwenden. Ihr AWS-Konto verwendet verschiedene Prozesse für ähnliche Änderungen.

Architektur

Technologie-Stack

- AMS
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- AWS SDK für Python (Boto3)
- Python und seine erforderlichen Pakete (JSON und Boto3)

Automatisierung und Skalierung

Dieses Muster bietet Beispielcode zur Automatisierung des `Stop EC2 instance` RFC, aber Sie können den Beispielcode und den Ansatz dieses Musters für andere RFCs verwenden.

Tools

- AWS Managed Services – AMS hilft Ihnen, Ihre AWS-Infrastruktur effizienter und sicher zu betreiben.
- AWS CLI – AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services. In AMS bietet die API für das Änderungsmanagement Operationen zum Erstellen und Verwalten von RFCs.
- AWS SDK for Python (Boto3) – SDK for Python erleichtert die Integration Ihrer Python-Anwendung, -Bibliothek oder -Skripts in AWS-Services.

Code

Die `AMS Stop EC2 Instance.zip` Datei (angefügt) enthält den Python-Code zum Erstellen eines `Stop EC2 instance` RFC. Sie können diesen Code auch so konfigurieren, dass ein einziges RFC für mehrere EC2-Instances gesendet wird.

Polen

Option 1 – Umgebung für macOS oder Linux einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und validieren Sie Python.	1. Öffnen Sie ein Terminalf enster und führen Sie den `brew install python3` Befehl aus. 2. Überprüfen Sie, ob Python korrekt installiert ist, indem Sie den `python --version` Befehl ausführen. 3. Überprüfen Sie, ob korrekt installiert `pip` ist, indem Sie den `pip --version` Befehl ausführen.	AWS-Systemadministrator
Installieren Sie AWS CLI.	Führen Sie den `pip install awscli --upgrade –user` Befehl aus, um AWS CLI zu installieren.	AWS-Systemadministrator
Installieren Sie Boto3.	Führen Sie den `pip install boto3` Befehl aus, um Boto3 zu installieren.	AWS-Systemadministrator
Installieren Sie JSON.	Führen Sie den `pip install json` Befehl aus, um JSON zu installieren.	AWS-Systemadministrator
Richten Sie die AMS-CLI ein.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AMS-Konso le und wählen Sie dann	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokumentation aus. Laden Sie die ZIP-Datei herunter, die die AMS-CLI enthält, entpacken Sie sie und installieren Sie sie dann auf Ihrem lokalen Computer. Führen Sie nach der Installation der AMS-CLI den `aws amscm help` Befehl aus. Die Ausgabe enthält Informationen über den AMS-Änderungsmanagementprozess.	

Option 2 – Umgebung für Windows einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und validieren Sie Python.	1. Öffnen Sie die Seite Python-Versionen für Windows, laden Sie die neueste Version herunter und installieren Sie dann Python. 2. Überprüfen Sie, ob Python korrekt installiert ist, indem Sie den `python --version` Befehl ausführen. 3. Überprüfen Sie, ob korrekt installiert `pip` ist, indem Sie den `pip --version` Befehl ausführen.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS CLI.	Führen Sie den `pip install awscli --upgrade –user` Befehl aus, um AWS CLI zu installieren.	AWS-Systemadministrator
Installieren Sie Boto3.	Führen Sie den `pip install boto3` Befehl aus, um Boto3 zu installieren.	AWS-Systemadministrator
Installieren Sie JSON.	Führen Sie den `pip install json` Befehl aus, um JSON zu installieren.	AWS-Systemadministrator
Richten Sie die AMS-CLI ein.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AMS-Konsole und wählen Sie dann Dokumentation aus. Laden Sie die ZIP-Datei herunter, die die AMS-CLI enthält, entpacken Sie sie und installieren Sie sie dann auf Ihrem lokalen Computer. Führen Sie nach der Installation der AMS-CLI den `aws amscm help` Befehl aus. Die Ausgabe enthält Informationen zum AMS-Änderungsmanagementprozess	AWS-Systemadministrator

Extrahieren der CT-ID und der Ausführungsparameter für das RFC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie die CT-ID, die Version und die Ausführun gsparameter für das RFC.	Jedes RFC hat eine andere CT-ID, Version und Ausführun gsparameter. Sie können diese Informationen mit einer der folgenden Optionen extrahieren: 1. Folgen Sie den Anweisung en im Abschnitt Suchen einer Änderungsanforderu ng (RFC) mit der CLI in RFC-Anwendungsbeispiele aus der AWS Managed Services-Dokumentation. 2. Öffnen Sie ein vorhanden es RFC eines ähnlichen Typs oder erstellen Sie ein neues RFC als Test über die AMS-Konsole. Verwenden Sie die CT-ID und die Ausführun gsparameter des RFC. Weitere Informationen dazu finden Sie unter Suchen eines RFC mit der Konsole in der AWS Managed Services-Dokumentation. Hinweis: Um die Python-Automatisierung dieses Musters für andere RFCs anzupassen, ersetzen Sie den	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CT-Typ und die Parameter werte in der `ams_stop_ec2_instance` Python-Codedatei aus der `AMS Stop EC2 Instance.zip` Datei (angefügt) durch diejenigen, die Sie extrahiert haben.	

Ausführen der Python-Automatisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Python-Automatisierung aus.	1. Laden Sie die `AMS Stop EC2 Instance.zip` Datei (angefügt) auf Ihren lokalen Computer herunter und extrahieren Sie die Datei. 2. Aktualisieren Sie `input_instances` mit Ihren EC2-Instance-Informationen. 3. Öffnen Sie ein Terminal und navigieren Sie zum Pfad für Ihren extrahierten Code 4. Führen Sie den Befehl `pythonams_stop_ec2_instance.py` aus.	AWS-Systemadministrator

Zugehörige Ressourcen

- Was sind Änderungstypen?
- CLI-Tutorial: Zweistufiger Hochverfügbarkeits-Stack (Linux/RHEL)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen einer RACI- oder RASCI-Matrix für ein Cloud-Betriebsmodell

Erstellt von Teddy Ger Made (AWS), Jerome Descreux (AWS), Josselin LE MIN (AWS) und Bolian Leroux (AWS)

Umgebung: Produktion	Technologien: Betrieb; Management und Governance

Übersicht

Das Cloud Center of Excellence (CCoE) oder CEE (Cloud Enablement Engine) ist ein engagiertes und rechenschaftspflichtiges Team, das sich auf die Betriebsbereitschaft für die Cloud konzentriert. Ihr Schwerpunkt liegt darauf, die IT-Informationsorganisation von einem On-Premises-Betriebsmodell in ein Cloud-Betriebsmodell umzuwandeln. Das CCoE sollte ein funktionsübergreifendes Team sein, das die Darstellung von Infrastruktur, Anwendungen, Betrieb und Sicherheit umfasst.

Eine der wichtigsten Komponenten eines Cloud-Betriebsmodells ist eine RACI-Matrix oder RASCI-Matrix. Dies wird verwendet, um die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien zu definieren. Der Matrixname wird aus den in der Matrix definierten Verantwortungstypen abgeleitet: verantwortlich (R), rechenschaftspflichtig (A), Support (S), konsultiert (C) und informiert (I). Der Support-Typ ist optional. Wenn Sie sie einschließen, wird sie als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Wenn Sie mit der angehängten Vorlage beginnen, kann Ihr CCoE-Team eine RACI- oder RASCI-Matrix für Ihre Organisation erstellen. Die Vorlage enthält Teams, Rollen und Aufgaben, die in Cloud-Betriebsmodellen üblich sind. Die Grundlage dieser Matrix sind die Aufgaben im Zusammenhang mit der Betriebsintegration und den CCoE-Funktionen. Sie können diese Vorlage jedoch an die Anforderungen der Struktur und des Anwendungsfalls Ihrer Organisation anpassen.

Die Implementierung einer RACI-Matrix ist unbegrenzt. Dieser Ansatz funktioniert für große Organisationen, Startups und alles dazwischen. Für kleine Organisationen kann dieselbe Ressource mehrere Rollen ausfüllen.

Polen

Erstellen der Matrix

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die wichtigsten Stakeholder.	Identifizieren Sie wichtige Service- und Teammanager, die mit den strategischen Zielen Ihres Cloud-Betriebsmodells verknüpft sind.	Projektmanager
Passen Sie die Matrixvorlage an.	Laden Sie die Vorlage im Abschnitt Anhänge herunter und aktualisieren Sie dann die RACI- oder RASCI-Matrix wie folgt: • Aktualisieren Sie auf dem Cloud Teams-Arbeitsprogramm die CCoE-Streamnamen, Teamnamen und Teambeschreibungen nach Bedarf für Ihre Organisation. • Aktualisieren Sie auf der Seite Cloud Roles microSD die Rollen, Teamnamen und Rollenbeschreibungen nach Bedarf für Ihre Organisation. • Aktualisieren Sie auf dem RASCI-Kabel nach Bedarf Folgendes für Ihre Organisation: • Aktualisieren Sie in Zeile 1 und Spalte A die CCoE-Streams.	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Aktualisieren Sie in Zeile 2 die Teamnamen. • Aktualisieren Sie in Zeile 3 die Rollennamen. • Aktualisieren Sie in den Spalten D und E die allgemeinen Felder und Aktivitäten, die Sie in Ihr RASCI-Diagramm aufnehmen möchten.	
Planen Sie Meetings.	1. Teilen Sie allen Stakeholdern die RASCI-Ziele mit. 2. Planen Sie ein oder mehrere Treffen, damit ein erzwungener Mitarbeiter aus jedem Team teilnehmen kann.	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Füllen Sie die Matrix aus.	Gehen Sie im Treffen mit allen Stakeholdern wie folgt vor: 1. Vergewissern Sie sich, dass ein -Mitarbeiter aus jedem Team angestellt ist. Die Teilnahme des Teams ist obligatorisch, damit Sie die Verantwortungstype n für jede Aufgabe genau zuweisen können. 2. Überprüfen Sie mit den Teilnehmern, was eine RASCI-Matrix ist und welche Ziele es gibt. 3. Überprüfen Sie das Modell der geteilten Verantwor tung mit den Teilnehme rn, damit sie den Umfang der Verantwortung ihrer Organisation für die Sicherheit in der Cloud verstehen. 4. Füllen Sie auf dem RASCI-Koordinate für jede Aufgabe oder Aktivität die Spalten F bis AN aus, um die folgenden Verantwor tungstypen zuzuweisen: • Verantwortlich (R) – Diese Rolle ist für die Ausführung der Arbeit zur Ausführung der Aufgabe verantwortlich.	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Rechenschaftsfähig (A) – Diese Rolle ist dafür verantwortlich, sicherzustellen, dass die Aufgabe abgeschlossen wird. Diese Rolle ist auch dafür verantwortlich, sicherzustellen, dass die Voraussetzungen erfüllt sind, und die Aufgabe an die verantwortlichen Personen zu delegieren. • Support (S) – Diese Rolle hilft denjenigen, die für die Ausführung der Aufgabe verantwortlich sind. Dieser Verantwortungstyp ist optional, und Sie können ihn ausschließen, um eine traditionellere RACI-Matrix zu erstellen. • Konsultiert (C) – Diese Rolle sollte konsultiert werden, um Meinungen oder Fachwissen zur Aufgabe zu erhalten. Abhängig von der Aufgabe ist dieser Verantwortungstyp möglicherweise nicht erforderlich. • (I) – Diese Rolle sollte über den Fortschritt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Aufgabe auf dem Laufenden gehalten und nach Abschluss der Aufgabe benachrichtigt werden. • Leer – Diese Rolle ist nicht an der Aktivität oder Aufgabe beteiligt.	
Teilen Sie die RASCI-Matrix.	Wenn die RACI- oder RASCI-Matrix abgeschlossen ist, lassen Sie sie von der Geschäftsleitung genehmigen. Speichern Sie es in einem gemeinsam genutzten Repository oder einem zentralen Ort, an dem alle Stakeholder darauf zugreifen können. Wir empfehlen Ihnen, Standard-Dokumentenkontrollprozesse zu verwenden, um Revisionen der Matrix aufzuzeichnen und zu genehmigen.	Projektmanager

Zugehörige Ressourcen

- AWS-Modell der geteilten Verantwortung

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen einer AWS Cloud9-IDE, die Amazon EBS-Volumes mit Standardverschlüsselung verwendet

Erstellt von Janardhan Malyala (AWS) und Dhr Boljioti Mukherjee (AWS)

Umgebung: Produktion	Technologien: Betrieb	Workload: Alle anderen Workloads
AWS-Services: AWS Cloud9; AWS KMS		

Übersicht

Sie können die standardmäßige Verschlüsselung verwenden, um die Verschlüsselung Ihrer Amazon Elastic Block Store (Amazon EBS)-Volumes und Snapshot-Kopien in der Amazon Web Services (AWS) Cloud zu erzwingen.

Sie können eine integrierte AWS Cloud9-Entwicklungsumgebung (IDE) erstellen, die standardmäßig verschlüsselte EBS-Volumes verwendet. Die serviceverknüpfte Rolle AWS Identity and Access Management (IAM) für AWS Cloud9 benötigt jedoch Zugriff auf den AWS Key Management Service (AWS KMS)-Schlüssel für diese EBS-Volumes. Wenn kein Zugriff bereitgestellt wird, kann die AWS Cloud9-IDE möglicherweise nicht gestartet werden und das Debuggen kann schwierig sein.

Dieses Muster enthält die Schritte zum Hinzufügen der serviceverknüpften Rolle für AWS Cloud9 zum AWS KMS-Schlüssel, der von Ihren EBS-Volumes verwendet wird. Die in diesem Muster beschriebene Einrichtung hilft Ihnen, erfolgreich eine IDE zu erstellen und zu starten, die standardmäßig EBS-Volumes mit Verschlüsselung verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Die Standardverschlüsselung ist für EBS-Volumes aktiviert. Weitere Informationen zur standardmäßigen Verschlüsselung finden Sie unter Amazon-EBS-Verschlüsselung in der Amazon Elastic Compute Cloud (Amazon EC2)-Dokumentation.

- Ein vorhandener kundenverwalteter KMS-Schlüssel zum Verschlüsseln Ihrer EBS-Volumes.

Hinweis: Sie müssen die serviceverknüpfte Rolle für AWS Cloud9 nicht erstellen. Wenn Sie eine AWS Cloud9-Entwicklungsumgebung erstellen, erstellt AWS Cloud9 die serviceverknüpfte Rolle für Sie.

Architektur

Technologie-Stack

- AWS Cloud9
- IAM
- AWS KMS

Tools

- AWS Cloud9 ist eine integrierte Entwicklungsumgebung (IDE), mit der Sie Software programmieren, erstellen, ausführen, testen und debuggen können. Es hilft Ihnen auch, Software in der AWS Cloud zu veröffentlichen.
- Amazon Elastic Block Store (Amazon EBS) stellt Volumes für die Speicherung auf Blockebene für die Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2)-Instances bereit.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel, um Ihre Daten zu schützen.

Polen

Ermitteln des Standardverschlüsselungsschlüsselwerts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie den Standard-Verschlüsselungsschlüsselwert für die EBS-Volumes.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon EC2-Konsole. Wählen Sie EC2-Dashboard und dann Datenschutz und Sicherheit in Kontoattribute aus. Kopieren Sie im Abschnitt EBS-Verschlüsselung den Wert im Standardverschlüsselungsschlüssel und notieren Sie ihn.	Cloud-Architekt, DevOps Techniker

Gewähren des Zugriffs auf den AWS KMS-Schlüssel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie AWS Cloud9 Zugriff auf den KMS-Schlüssel für EBS-Volumes bereit.	1. Öffnen Sie die AWS KMS-Konsole und wählen Sie dann Kundenverwaltete Schlüssel aus. Wählen Sie den AWS KMS-Schlüssel aus, der für die Amazon EBS-Verschlüsselung verwendet wird, und wählen Sie dann Schlüssel anzeigen aus. 2. Vergewissern Sie sich auf der Registerkarte Schlüsselrichtlinie, dass Sie das Textformular der Schlüssel	Cloud-Architekt, DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	richtlinie sehen können. Wenn das Textformu lar nicht angezeigt wird, wählen Sie Zur Richtlini enansicht wechseln aus. 3. Wählen Sie Bearbeiten aus. Fügen Sie der Richtlini e den Code im Abschnitt Zusätzliche Informati onen hinzu und wählen Sie dann Änderungen speichern aus. Die Richtlini enänderungen ermöglich en der serviceverknüpften Rolle für AWS Cloud9, `AWSServiceRoleForA WSCloud9` , den Zugriff auf den Schlüssel. Weitere Informationen zum Aktualisieren einer Schlüsselrichtlinie finden Sie unter So ändern Sie eine Schlüsselrichtlinie (AWS-KMS-Dokumentation). Wichtig: Die serviceverknüpfte Rolle für AWS Cloud9 wird automatisch erstellt, wenn Sie Ihre erste IDE starten. Weitere Informationen finden Sie unter Erstellen einer serviceve rknüpften Rolle in der AWS Cloud9-Dokumentation.	

Erstellen und Starten der IDE

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und starten Sie die AWS Cloud9-IDE.	Öffnen Sie die AWS Cloud9-Konsole und wählen Sie Umgebung erstellen aus.Konfigurieren Sie die IDE entsprechend Ihren Anforderungen, indem Sie die Schritte unter Erstellen einer EC2-Umgebung in der AWS Cloud9-Dokumentation befolgen.	Cloud-Architekt, DevOps Techniker

Zugehörige Ressourcen

- Verschlüsseln von EBS-Volumes, die von AWS Cloud9 verwendet werden
- Erstellen einer serviceverknüpften Rolle für AWS Cloud9
- Erstellen einer EC2-Umgebung in AWS Cloud9

Zusätzliche Informationen

AWS KMS-Schlüsselrichtlinienaktualisierungen

Ersetzen Sie <aws_accountid> durch Ihre AWS-Konto-ID.

```
{
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
```

```
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
```

Verwenden eines kontoübergreifenden Schlüssels

Wenn Sie einen kontoübergreifenden KMS-Schlüssel verwenden möchten, müssen Sie eine Erteilung in Kombination mit der KMS-Schlüsselrichtlinie verwenden. Dies ermöglicht den kontoübergreifenden Zugriff auf den Schlüssel. Führen Sie in demselben Konto, mit dem Sie die Cloud9-Umgebung erstellt haben, den folgenden Befehl im Terminal aus.

```
aws kms create-grant \
 --region <Region where Cloud9 environment is created> \
 --key-id <The cross-account KMS key ARN> \
 --grantee-principal arn:aws:iam::<The account where Cloud9 environment is
 created>:role/aws-service-role/cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9 \
 --operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

Nachdem Sie diesen Befehl ausgeführt haben, können Sie Cloud9-Umgebungen erstellen, indem Sie die EBS-Verschlüsselung mit einem Schlüssel in einem anderen Konto verwenden.

Automatisches Erstellen von Tag-basierten CloudWatch Amazon-Dashboards

Erstellt von Janak Vadaria (AWS), RAJNEESH TYAGI (AWS) und Vinodkumar Mandalapu (AWS)

Code-Repository: Goldensignals	Umgebung: Produktion	Technologien: Betrieb; Cloud-nativ; Verwaltung und Unternehmensführung
AWS-Dienste: AWS CDK; Amazon CloudWatch; AWS CodeBuild; AWS CodePipeline		

Übersicht

Das manuelle Erstellen verschiedener CloudWatch Amazon-Dashboards kann zeitaufwändig sein, insbesondere wenn Sie mehrere Ressourcen erstellen und aktualisieren müssen, um Ihre Umgebung automatisch zu skalieren. Eine Lösung, die Ihre CloudWatch Dashboards automatisch erstellt und aktualisiert, kann Ihnen Zeit sparen. Dieses Muster hilft Ihnen bei der Implementierung einer vollautomatischen AWS Cloud Development Kit (AWS CDK) Pipeline, die CloudWatch Dashboards für Ihre AWS Ressourcen auf der Grundlage von Tag-Änderungsereignissen erstellt und aktualisiert, um Golden Signals-Metriken anzuzeigen.

Im Bereich Site Reliability Engineering (SRE) bezieht sich Golden Signals auf einen umfassenden Satz von Kennzahlen, die einen umfassenden Überblick über einen Service aus Nutzer- oder Verbrauchersicht bieten. Diese Metriken bestehen aus Latenz, Traffic, Fehlern und Sättigung. Weitere Informationen finden Sie unter Was ist Site Reliability Engineering (SRE)? auf der AWS Website.

Die durch dieses Muster bereitgestellte Lösung ist ereignisgesteuert. Nach der Bereitstellung überwacht es kontinuierlich die Tag-Änderungsereignisse und aktualisiert die CloudWatch Dashboards und Alarme automatisch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Voraussetzungen für die AWS CDK Version 2
- Eine Bootstrap-Umgebung auf AWS
- Python versie 3
- AWS SDK for Python (Boto3), installiert
- Node.js Version 18 oder höher
- Node Package Manager (npm), installiert und konfiguriert für AWS CDK
- Mittlere Vertrautheit (Stufe 200) mit dem und AWS CDK AWS CodePipeline

Einschränkungen

Diese Lösung erstellt derzeit automatisierte Dashboards nur für die folgenden AWS-Services:

- Amazon Relational Database Service (Amazon RDS)
- AWS Auto Scaling
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon-DynamoDB
- AWS Lambda

Architektur

Zieltechnologie-Stack

- CloudWatch Dashboards
- CloudWatch Alarme

Zielarchitektur

1. Ein AWS Tag-Änderungsereignis für die konfigurierten Anwendungs-Tags oder Codeänderungen initiiert eine Pipeline AWS CodePipeline zur Erstellung und Bereitstellung aktualisierter Dashboards. CloudWatch

2. AWS CodeBuild führt ein Python-Skript aus, um die Ressourcen zu finden, für die Tags konfiguriert sind, und speichert die Ressourcen-IDs in einer lokalen Datei in einer CodeBuild Umgebung.
3. CodeBuild führt cdk synth aus, um AWS CloudFormation Vorlagen zu generieren, die CloudWatch Dashboards und Alarme bereitstellen.
4. CodePipeline stellt die AWS CloudFormation Vorlagen in der angegebenen Region bereit. AWS-Konto
5. Wenn der AWS CloudFormation Stack erfolgreich bereitgestellt wurde, können Sie sich die CloudWatch Dashboards und Alarme ansehen.

Automatisierung und Skalierung

Diese Lösung wurde mithilfe von automatisiert AWS CDK. Sie finden den Code im CloudWatch Repository GitHub Golden Signals Dashboards auf Amazon. Für zusätzliche Skalierung und zur Erstellung benutzerdefinierter Dashboards können Sie mehrere Tag-Schlüssel und -Werte konfigurieren.

Tools

Amazon-Dienste

- Amazon EventBridge ist ein serverloser Event-Bus-Service, der Ihnen hilft, Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen zu verbinden, darunter AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

Als bewährte Sicherheitsmethode können Sie Verschlüsselung und Authentifizierung für die Quell-Repositorys verwenden, die eine Verbindung zu Ihren Pipelines herstellen. Weitere bewährte Methoden finden Sie in der Dokumentation unter CodePipeline Bewährte Methoden und Anwendungsfälle. CodePipeline

Epen

Konfigurieren und implementieren Sie die Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implementieren Sie die Beispielanwendung.	1. Klonen Sie das GitHub Beispielcode-Repository mit dem folgenden Befehl: `git clone https://github.com/aws-samples/golden-signals-dashboards-sample-app` 2. Navigieren Sie zum geklonten Repository auf Ihrem Computer und öffnen Sie die `src/project-settings.ts` Datei mit einem Editor Ihrer Wahl. 3. Ändern Sie den `projectSettings` konstanten Wert entsprechend Ihren AWS Ressourcen-Tags und Anwendungszuordnungen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Legen Sie die `AWS_ACCOUNT` `GS_DASHBOARD_INSTANCE` Umgebungsvariablen `AWS_REGION` , und fest: • Stellen `AWS_ACCOUNT` Sie die Konto-ID Ihres AWS Kontos ein. • Wählen `AWS_REGION` Sie die Region aus, in der Sie die Beispielanwendung bereitstellen möchten. • Stellen Sie `GS_DASHBOARD_INSTANCE` `dev` dies `test` je nach Entwicklungsumgebung auf`prod`, oder ein. (Wir empfehlen `test` das in diesem Muster beschriebene Testverfahren.) 5. Richten Sie das AWS CLI mit Ihren AWS Anmeldeinformationen ein. Weitere Informationen finden Sie in der AWS CLI Dokumentation unter Einrichten und Anzeigen von Konfigurationseinstellungen mithilfe von Befehlen. 6. Führen Sie den folgenden Befehl aus, um die Golden Signals Dashboard-Beispielanwendung bereitzustellen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sh deploy.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Automatisches Erstellen von Dashboards und Alarmen.	Nachdem Sie die Beispielanwendung bereitgestellt haben, können Sie alle Ressourcen, die diese Lösung unterstützt, mit den erwarteten Tag-Werten erstellen. Dadurch werden automatisch die angegebenen Dashboards und Alarme erstellt. Um diese Lösung zu testen, erstellen Sie eine AWS Lambda Funktion: 1. Melden Sie sich in dem AWS Management Console Bereich an, in AWS-Region dem Sie die Beispielanwendung bereitgestellt haben. 2. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda/. 3. Wählen Sie Funktion erstellen und geben Sie dann einen Funktionsnamen ein. 4. Wählen Sie im Bereich Erweiterte Einstellungen die Option Tags aktivieren und dann Neues Tag hinzufügen aus. Geben Sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den folgenden Schlüssel und Wert ein: • Schlüssel: `AutoDashboard` • Wert: `True` 5. Wählen Sie Funktion erstellen. Die Lambda-Funktion startet sofort eine CodePipeline, die die Dashboards und Alarme für diese bestimmte Lambda-Funktion automatisch erstellt. 6. Um die automatisierten Dashboards und Alarme anzuzeigen, öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/. Sie können die benutzerdefinierten Dashboards und Alarme für die Funktion anzeigen, die Sie in der `projectSettings` Konstante angegeben haben (standardmäßig App1-Lambda). 7. Wählen Sie das Dashboard für die Lambda-Funktion aus, um zusätzliche automatisierte Dashboards anzuzeigen, die im Rahmen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieser Lösung erstellt wurden. 8. Wiederholen Sie diese Schritte für andere Dienste wie Amazon RDS, Amazon SNS und DynamoDB AWS Auto Scaling, um die zugehörigen Dashboards zu generieren. Ein Beispiel für Amazon RDS finden Sie im Abschnitt Zusätzliche Informationen.	

Entfernen Sie die Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entferne das `golden-signals-dashboard` Konstrukt.	1. Um alle von der Beispielanwendung erstellten AWS CloudFormation Stacks zu entfernen, müssen Sie die `GS_DASHBOARD_INSTANCE` Umgebungsvariablen `AWS_ACCOUNT` `AWS_REGION` , und neu konfigurieren. Für den `destroy.sh` Befehl sind diese Konfigurationen erforderlich. • `AWS_ACCOUNT` ist die Konto-ID Ihres AWS Kontos. • `AWS_REGION` ist die Region, in der Sie Ihre	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispielanwendung bereitgestellt haben. • `GS_DASHBOARD_INSTANCE` basiert`dev`,`test`, oder`prod`, auf Ihren vorherigen Einstellungen. 2. AWS CLI Mit Ihren AWS Anmeldeinformationen einrichten. 3. Führen Sie den folgenden Befehl aus, um die Beispielanwendung und alle zugehörigen AWS CloudFormation Stacks zu entfernen: `sh destroy.sh`	

Fehlerbehebung

Problem	Lösung
Der Python-Befehl wurde nicht gefunden (bezieht `findresources.sh` sich auf Zeile 8).	Überprüfen Sie die Version Ihrer Python-In stallation. Wenn Sie Python Version 3 installie rt haben, `python` ersetzen `python3` Sie es durch Zeile 8 der `resources.sh` Datei und führen Sie den `sh deploy.sh` Befehl erneut aus, um die Lösung bereitzustellen.

Zugehörige Ressourcen

- Bootstrapping (Dokumentation)AWS CDK

- Benannte Profile verwenden (Dokumentation)AWS CLI
- AWS CDK Werkstatt

Zusätzliche Informationen

Die folgende Abbildung zeigt ein Beispiel-Dashboard für Amazon RDS, das als Teil dieser Lösung erstellt wurde.

Suchen Sie AWS-Ressourcen basierend auf ihrem Erstellungsdatum mithilfe von erweiterten AWS Config-Abfragen

Erstellt von Inna Saman (AWS)

Umgebung: Produktion	Technologien: Betrieb; Sicherheit, Identität, Compliance	AWS-Services: AWS Config; Amazon EBS; Amazon EC2; Amazon S3; AWS Lambda

Übersicht

Dieses Muster zeigt, wie AWS-Ressourcen basierend auf ihrem Erstellungsdatum mithilfe der erweiterten AWS Config-Abfragefunktion gefunden werden.

Erweiterte AWS Config-Abfragen verwenden eine Teilmenge von SQL, um den Konfigurationsstatus von AWS-Ressourcen für Bestandsverwaltung, Operational Intelligence, Sicherheit und Compliance abzufragen. Sie können diese Abfragen verwenden, um AWS-Ressourcen in einem einzigen AWS-Konto und einer AWS-Region oder über mehrere Konten und Regionen hinweg zu finden. Durch Ausführen einer Abfrage, die die -resourceCreationTimeEigenschaft verwendet, können Sie eine Liste Ihrer AWS-Ressourcen basierend auf ihrem spezifischen Erstellungsdatum zurückgeben. Sie können erweiterte AWS config-Abfragen mit einer der folgenden Methoden ausführen:

- Der AWS Config Query Editor in der AWS Config-Konsole
- Die AWS-Befehlszeilenschnittstelle (AWS CLI)

Die Beispielabfrage im Abschnitt Zusätzliche Informationen dieses Musters gibt eine Liste der AWS-Ressourcen zurück, die innerhalb eines bestimmten Zeitraums von 60 Tagen erstellt wurden. Die Ausgabe der Abfrage enthält Informationen über Folgendes für jede identifizierte Ressource:

- Konto-ID
- Region
- Ressourcenname
- Ressourcen-ID
- Ressourcentyp

- Tags
- Zeitpunkt der Erstellung

Die Beispielabfrage zeigt auch, wie die Bestandsliste auf bestimmte Ressourcentypen mit dem „WHERE ... IN“-Anweisung. Sie können eine ähnliche Abfrage verwenden, um andere AWS-Ressourcentypen zu finden, die auch mit Tags funktionieren.

Hinweis: Um Ressourcen über mehrere AWS-Konten und Regionen oder über eine AWS Organizations-Organisation abzufragen, müssen Sie einen AWS Config-Aggregator verwenden. Weitere Informationen finden Sie unter Datenaggregation für mehrere Konten und Regionen im AWS Config-Entwicklerhandbuch. Globale Ressourcen werden nur in ihrer Heimatregion aufgezeichnet. AWS Identity and Access Management (IAM) ist beispielsweise eine globale Ressource und wird in us-east-1 (Nord-Virginia-Region) aufgezeichnet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein oder mehrere aktive AWS-Konten, für die AWS Config aktiviert ist, um alle unterstützten Ressourcentypen aufzuzeichnen (Standardkonfiguration)
- (Für Abfragen mit mehreren Konten und Regionen) Ein aktivierter AWS Config-Aggregator

Einschränkungen

- Die erweiterten Abfrageergebnisse von AWS Config werden paginiert. Wenn Sie Exportieren wählen, werden bis zu 500 Ergebnisse aus der AWS-Managementkonsole exportiert. Sie können APIs auch verwenden, um bis zu 100 paginierte Ergebnisse gleichzeitig abzurufen.
- Erweiterte AWS Config-Abfragen verwenden eine Teilmenge von SQL mit eigenen Syntaxbeschränkungen. Weitere Informationen finden Sie unter Einschränkungen bei der Abfrage des aktuellen Konfigurationsstatus von AWS-Ressourcen im AWS Config-Entwicklerhandbuch.

Tools

Tools

- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und wie sie konfiguriert sind. Auf diese Weise können Sie feststellen, wie Ressourcen miteinander in Beziehung stehen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Polen

Ausführen einer erweiterten AWS Config-Abfrage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Ressourcen, die Sie abfragen, von AWS Config unterstützt werden.	Eine vollständige Liste der AWS-Ressourcen, die AWS Config unterstützt, finden Sie unter Unterstützte Ressourcentypen im AWS Config-Entwicklerhandbuch.	Cloud-Administrator
Stellen Sie sicher, dass der Konfigurations-Recorder erstellt wurde und ausgeführt wird.	Folgen Sie den Anweisungen unter Verwalten des Konfigurations-Recorders im AWS Config-Entwicklerhandbuch. Hinweis: AWS Config erstellt und startet automatisch den Standardkonfigurations-Recorder.	Cloud-Administrator
Führen Sie die Abfrage aus.	Folgen Sie den Anweisungen inQuery mit dem SQL-Abfrage-Editor (Konsole) oderder Abfrage mit dem SQL-Abfrage-Editor (AWS CLI) im AWS Config-Entwicklerhandbuch. Hinweis: Wenn Sie beim Ausführen von AWS CLI-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Befehlen Fehler erhalten, stellen Sie sicher, dass Sie die neueste Version der AWS CLI verwenden. Für einzelne AWS-Konto- und Regionsabfragen Stellen Sie auf der Seite Abfrage-Editor im Abschnitt Abfragebereich sicher, dass Sie Dieses Konto und nur Region auswählen. Für Abfragen mit mehreren Konten und Regionen Stellen Sie auf der Seite Abfrage-Editor im Abschnitt Abfragebereich sicher, dass Sie einen AWS Config-Aggregator erstellen und auswählen. Weitere Informationen finden Sie unter Datenaggregation für mehrere Konten und Regionen im AWS Config-Entwicklerhandbuch. Wenn Abfragen über mehrere Konten oder Regionen nicht funktionieren, folgen Sie den Anweisungen unterFehlerbehebung für die Datenaggregation mehrerer Konten und Regionen im AWS Config-Entwicklerhandbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Um den Umfang der Abfrage basierend auf dem Ressourcentyp zu ändern, verwenden Sie die KonfigurationWHERE resourceType IN (...). Eine Beispielabfrage finden Sie unter Beispiel für eine erweiterte AWS Config-Abfrage im Abschnitt Zusätzliche Informationen.	

Zusätzliche Informationen

Beispiel für eine erweiterte AWS Config-Abfrage

Die folgende Beispielabfrage gibt eine Liste der AWS-Ressourcen zurück, die innerhalb eines bestimmten Zeitraums von 60 Tagen erstellt wurden. Weitere Beispiele für erweiterte AWS Config-Abfragen finden Sie unter Beispielabfragen im AWS Config-Entwicklerhandbuch.

```
SELECT
  accountId,
  awsRegion,
  resourceName,
  resourceId,
  resourceType,
  resourceCreationTime,
  tags
WHERE
  resourceType IN (
    'AWS::CloudFormation::Stack',
    'AWS::EC2::VPC',
    'AWS::EC2::Volume',
    'AWS::EC2::Instance',
    'AWS::RDS::DBInstance',
    'AWS::ElasticLoadBalancingV2::LoadBalancer',
    'AWS::ServiceCatalog::CloudFormationProvisionedProduct',
    'AWS::EC2::NetworkInterface',
    'AWS::EC2::Subnet',
```

```
    'AWS::EC2::SecurityGroup',
    'AWS::AutoScaling::AutoScalingGroup',
    'AWS::Lambda::Function',
    'AWS::DynamoDB::Table',
    'AWS::S3::Bucket'
  )
  AND resourceCreationTime BETWEEN '2022-05-23T00:00:00.000Z' AND
 '2022-07-23T17:59:51.000Z'
ORDER BY
  accountId ASC,
  resourceType ASC
```

Datenschutz und Schutz

AWS Config wird in jeder AWS-Region separat aktiviert. Um die gesetzlichen Anforderungen zu erfüllen, müssen besondere Überlegungen angewendet werden, z. B. die Erstellung separater regionaler Aggregatoren. Weitere Informationen finden Sie unter Datenschutz in AWS Config im AWS Config-Entwicklerhandbuch.

IAM-Berechtigungen

Die von AWS_ConfigRole AWS verwaltete Richtlinie ist als Mindestsatz von Berechtigungen erforderlich, um erweiterte AWS Config-Abfragen auszuführen. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie zum Abrufen von Konfigurationsdetails im Abschnitt Berechtigungen für die AWS Config zugewiesene IAM-Rolle im AWS Config-Entwicklerhandbuch.

EBS-Snapshot-Details für Ihr AWS-Konto oder Ihre Organisation anzeigen

Umgebung: Produktion	Technologien: Betrieb; Speicherung und Sicherung	AWS-Dienste: Amazon EBS

Übersicht

Dieses Muster beschreibt, wie Sie automatisch einen On-Demand-Bericht über alle Amazon Elastic Block Store (Amazon EBS) -Snapshots in Ihrem Amazon Web Services (AWS) -Konto oder Ihrer Organisationseinheit (OU) in AWS Organizations generieren können.

Amazon EBS ist ein skalierbarer easy-to-use, leistungsstarker Blockspeicherservice, der für Amazon Elastic Compute Cloud (Amazon EC2) entwickelt wurde. Ein EBS-Volume bietet dauerhaften und persistenten Speicher, den Sie an Ihre EC2-Instances anhängen können. Sie können EBS-Volumes als Primärspeicher für Ihre Daten verwenden und eine point-in-time Sicherungskopie Ihrer EBS-Volumes erstellen, indem Sie einen Snapshot erstellen. Sie können die AWS-Managementkonsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden, um die Details bestimmter EBS-Snapshots anzuzeigen. Dieses Muster bietet eine programmatische Methode zum Abrufen von Informationen über alle EBS-Snapshots in Ihrem AWS-Konto oder Ihrer Organisationseinheit.

Sie können das in diesem Muster bereitgestellte Skript verwenden, um eine Datei mit kommagetrennten Werten (CSV) zu generieren, die die folgenden Informationen zu jedem Snapshot enthält: Konto-ID, Snapshot-ID, Volume-ID und -Größe, Datum, an dem der Snapshot aufgenommen wurde, Instance-ID und Beschreibung. Wenn Ihre EBS-Snapshots markiert sind, enthält der Bericht auch die Eigentümer- und Teamattribute.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS CLI Version 2 installiert und konfiguriert
- Rolle AWS Identity and Access Management (IAM) mit den entsprechenden Berechtigungen (Zugriffsberechtigungen für ein bestimmtes Konto oder für alle Konten in einer Organisationseinheit, wenn Sie planen, das Skript von AWS Organizations aus auszuführen)

Architektur

Das folgende Diagramm zeigt den Skript-Workflow, der einen On-Demand-Bericht über EBS-Snapshots generiert, die auf mehrere AWS-Konten in einer Organisationseinheit verteilt sind.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Block Store (Amazon EBS) bietet Volumes für die Speicherung auf Blockebene, die mit EC2-Instances verwendet werden.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

Code

Der Code für die in diesem Muster verwendete Beispielanwendung ist im Repository GitHub aws-ebs-snapshots-awsorganizations verfügbar. Folgen Sie den Anweisungen im nächsten Abschnitt, um die Beispieldateien zu verwenden.

Epen

Laden Sie das Skript herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Python-Skript herunter.	Laden Sie das Skript GetSnapshotDetailsAllAccountsOU.py aus dem GitHub Repository herunter.	Allgemeines AWS

EBS-Snapshot-Details für ein AWS-Konto abrufen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie das Python-Skript aus.	Führen Sie den Befehl aus:
	`python3 getsnapshotinfo.py --file <output-file>.csv --region <region-name>`
	wobei `<output-file>` sich auf die CSV-Ausgabedatei bezieht, in der Sie Informationen zu den platzierten EBS-Snapshots abrufen möchten, und `<region-name>` ist die AWS-Region, in der die Snapshots gespeichert werden. Beispielsweise:
	`python3 getsnapshotinfo.py --file snapshots.csv --region us-east-1`
		Allgemeines AWS

Rufen Sie EBS-Snapshot-Details für eine Organisation ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Python-Skript aus.	Führen Sie den Befehl aus: `python3 getsnapshotinfo.py --file <output-file>.csv --role <IAM-role> --region <region-name>`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wobei `<output-file>` sich auf die CSV-Ausgabedatei bezieht, in der Sie Informationen zu den platzierten EBS-Snapshots abrufen möchten, `<IAM-role>` ist eine Rolle, die Berechtigungen für den Zugriff auf AWS Organizations bereitstellt, und `<region-name>` ist die AWS-Region, in der die Snapshots gespeichert werden. Beispielsweise: `python3 getsnapshotinfo.py --file snapshots.csv --role <IAM role> --region us-west-2`	

Zugehörige Ressourcen

- Amazon EBS-Dokumentation
- Amazon EBS-Aktionen
- Amazon EBS API-Referenz
- Verbesserung der Amazon EBS-Leistung
- Amazon EBS-Ressourcen
- EBS-Snapshot-Preise

Zusätzliche Informationen

EBS-Snapshot-Typen

Amazon EBS bietet je nach Besitz und Zugriff drei Arten von Snapshots:

- Gehört Ihnen — Standardmäßig können nur Sie Volumes aus Snapshots erstellen, die Sie besitzen.
- Öffentliche Snapshots — Sie können Snapshots öffentlich mit allen anderen AWS-Konten teilen. Um einen öffentlichen Snapshot zu erstellen, ändern Sie die Berechtigungen für einen Snapshot, um ihn für die von Ihnen angegebenen AWS-Konten freizugeben. Benutzer, die Sie autorisieren, können dann die von Ihnen geteilten Snapshots verwenden, indem sie ihre eigenen EBS-Volumes erstellen. Ihr ursprünglicher Snapshot bleibt davon unberührt. Sie können Ihre unverschlüsselten Snapshots auch allen AWS-Benutzern öffentlich zugänglich machen. Aus Sicherheitsgründen können Sie Ihre verschlüsselten Snapshots jedoch nicht öffentlich zugänglich machen. Öffentliche Schnappschüsse stellen ein erhebliches Sicherheitsrisiko dar, da persönliche und sensible Daten offengelegt werden können. Wir empfehlen dringend, Ihre EBS-Snapshots nicht mit allen AWS-Konten zu teilen. Weitere Informationen zum Teilen von Snapshots finden Sie in der AWS-Dokumentation.
- Private Snapshots — Sie können Snapshots privat mit einzelnen AWS-Konten teilen, die Sie angeben. Um den Snapshot privat mit bestimmten AWS-Konten zu teilen, folgen Sie den Anweisungen in der AWS-Dokumentation und wählen Sie Privat für die Berechtigungseinstellung. Benutzer, die Sie autorisiert haben, können die von Ihnen freigegebenen Snapshots zur Erstellung ihrer eigenen EBS-Volumes verwenden, während Ihr Original-Snapshot davon unberührt bleibt.

Übersichten und Verfahren

Die folgende Tabelle enthält Links zu weiteren Informationen über EBS-Snapshots, einschließlich Informationen dazu, wie Sie die EBS-Volumenkosten senken können, indem Sie unbenutzte Snapshots suchen und löschen und selten aufgerufene Snapshots archivieren, auf die selten zugegriffen wird und die nicht häufig oder schnell abgerufen werden müssen.

Für Informationen über	See
Schnappschüsse, ihre Funktionen und Einschränkungen	Amazon EBS-Snapshots erstellen
Wie erstelle ich einen Snapshot	Konsole: Erstellen Sie einen Snapshot AWS-CLI: Befehl create-snapshot Beispielsweise:

	`aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --description " volume snapshot"`
Löschen von Snapshots (allgemeine Informationen)	Löschen Sie einen Amazon EBS-Snapshot
Wie lösche ich einen Snapshot	Konsole: Löscht einen Snapshot AWS-CLI: Befehl delete-snapshot Beispielsweise: `aws ec2 delete-snapshot --snapshot-id snap-1234567890abcdef0`
Archivieren von Snapshots (allgemeine Informationen)	Amazon EBS-Snapshots archivieren Amazon EBS-Snapshot-Archiv (Blogbeitrag)
Wie archiviere ich einen Snapshot	Konsole: Archivieren Sie einen Snapshot AWS CLI: modify-snapshot-tier Befehl
Wie rufe ich einen archivierten Snapshot ab	Konsole: Stellen Sie einen archivierten Snapshot wieder her AWS CLI: restore-snapshot-tier Befehl
Preise für Snapshots	Amazon EBS-Preise

HÄUFIG GESTELLTE FRAGEN

Was ist der Mindestarchivierungszeitraum?

Der minimale Archivzeitraum beträgt 90 Tage.

Wie lange würde es dauern, einen archivierten Snapshot wiederherzustellen?

Je nach Größe des Snapshots kann es bis zu 72 Stunden dauern, bis ein archivierter Snapshot von der Archivstufe auf die Standardstufe wiederhergestellt wird.

Sind archivierte Snapshots vollständige Snapshots?

Archivierte Snapshots sind immer vollständige Snapshots.

Welche Snapshots kann ein Benutzer archivieren?

Sie können nur Snapshots archivieren, deren Eigentümer Sie in Ihrem Konto sind.

Können Sie einen Snapshot des Root-Geräte-Volumes eines registrierten Amazon Machine Image (AMI) archivieren?

Nein, Sie können keinen Snapshot des Root-Geräte-Volumes eines registrierten AMI archivieren.

Was sind Sicherheitsaspekte bei der gemeinsamen Nutzung eines Snapshots?

Wenn Sie einen Snapshot teilen, gewähren Sie anderen Zugriff auf alle Daten im Snapshot. Teilen Sie Snapshots nur mit Personen, denen Sie Ihre Daten anvertrauen.

Wie teilen Sie einen Snapshot mit einer anderen AWS-Region?

Snapshots sind auf die Region beschränkt, in der sie erstellt wurden. Um einen Snapshot in einer anderen Region freizugeben, kopieren Sie den Snapshot in die Region und geben dann die Kopie frei.

Können Sie verschlüsselte Snapshots teilen?

Sie können keine Snapshots teilen, die mit dem standardmäßigen verwalteten AWS-Schlüssel verschlüsselt sind. Sie können nur Snapshots teilen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Wenn Sie einen verschlüsselten Snapshot teilen, müssen Sie auch den vom Kunden verwalteten Schlüssel teilen, der zum Verschlüsseln des Snapshots verwendet wurde.

Was ist mit unverschlüsselten Snapshots?

Sie können unverschlüsselte Snapshots öffentlich teilen.

Mehr Muster

- EC2-Instances Schreibzugriff auf S3-Buckets in AMS-Konten gewähren
- Automatisieren der AWS-Ressourcenbewertung
- Automatisieren von Sicherheitsscans für kontoübergreifende Workloads mit Amazon Inspector und AWS Security Hub
- ???
- Erstellen Sie einen MLOps-Workflow mithilfe von Amazon SageMaker und Azure DevOps
- Zentralisieren der Überwachung mithilfe von Amazon CloudWatch Observability Access Manager
- Konfigurieren der Protokollierung und Überwachung für Sicherheitsereignisse in Ihrer AWS IoT-Umgebung
- Herstellen einer Verbindung mit einer Amazon EC2-Instance mithilfe von Session Manager
- Erstellen von Alarmen für benutzerdefinierte Metriken mithilfe der Amazon CloudWatch - Anomalieerkennung
- ???
- Verbessern Sie die betriebliche Leistung, indem Sie Amazon DevOps Guru über mehrere AWS-Regionen, Konten und OUs hinweg mit dem AWS-CDK aktivieren
- Aufnehmen und Migrieren von EC2-Windows-Instances in ein AWS Managed Services-Konto
- Installieren Sie den SSM-Agenten und - CloudWatch Agenten auf Amazon-EKS-Worker-Knoten mit preBootstrapCommands
- Integrieren Sie Stonebranch Universal Controller in AWS Mainframe Modernization
- Starten eines CodeBuild Projekts über AWS-Konten hinweg mithilfe von Step Functions und einer Lambda-Proxy-Funktion
- Überwachen und Korrigieren des geplanten Löschens von AWS KMS-Schlüsseln
- Überwachen der Verwendung eines freigegebenen Amazon Machine Image über mehrere AWS-Konten hinweg
- Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus
- Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus
- Richten Sie die CloudFormation AWS-Drift-Erkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein
- Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten

- Automatisches Markieren von Transit Gateway-Anhängen mit AWS Organizations
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen

SaaS

Themen

Mandanten für mehrere SaaS-Produkte auf einer einzigen Steuerebene verwalten

Erstellt von Ramanna Avancha (AWS), Jenifer Pascal (AWS), Kishan Kavala (AWS) und Anusha Mandava (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: SaaS	AWS-Services: Amazon API Gateway ;Amazon Cognito ;AWS Lambda ;AWS Step Functions; Amazon DynamoDB

Übersicht

Dieses Muster zeigt, wie Sie Mandantenlebenszyklen über mehrere Software as a Service (SaaS)-Produkte hinweg auf einer einzigen Steuerebene in der AWS Cloud verwalten. Die bereitgestellte Referenzarchitektur kann Unternehmen dabei unterstützen, die Implementierung redundanter, gemeinsam genutzter Funktionen für ihre einzelnen SaaS-Produkte zu reduzieren und Governance-Effizienzen in großem Umfang bereitzustellen.

Große Unternehmen können mehrere SaaS-Produkte in verschiedenen Geschäftsbereichen haben. Diese Produkte müssen häufig für die Verwendung durch externe Mandanten auf verschiedenen Abonnementebenen bereitgestellt werden. Ohne eine gängige Mandantenlösung müssen IT-Administratoren Zeit mit der Verwaltung undifferenzierter Funktionen über mehrere SaaS-APIs hinweg verbringen, anstatt sich auf die Entwicklung von Kernproduktfunktionen zu konzentrieren.

Die in diesem Muster bereitgestellte gemeinsame Mandantenlösung kann dazu beitragen, die Verwaltung vieler gemeinsam genutzter SaaS-Produktfunktionen einer Organisation zu zentralisieren, darunter die folgenden:

- Sicherheit
- Mandantenbereitstellung
- Tenant-Datenspeicher
- Mandantenkommunikation

- Produktmanagement
- Protokollierung und Überwachung von Metriken

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Kenntnisse von Amazon Cognito oder einem externen Identitätsanbieter (IdP)
- Kenntnisse von Amazon API Gateway
- Kenntnisse von AWS Lambda
- Kenntnisse von Amazon DynamoDB
- Kenntnisse von AWS Identity and Access Management (IAM)
- Kenntnisse von AWS Step Functions
- Kenntnisse von AWS CloudTrail und Amazon CloudWatch
- Kenntnisse der Python-Bibliotheken und des Codes
- Kenntnisse von SaaS-APIs, einschließlich der verschiedenen Arten von Benutzern (Organisationen, Mandanten, Administratoren und Anwendungsbenutzer), Abonnementmodellen und Mandantenisolationsmodellen
- Kenntnisse der SaaS-Anforderungen und Multi-Tenant-Abonnements Ihrer Organisation für mehrere Produkte

Einschränkungen

- Integrationen zwischen der Common-Tenant-Lösung und einzelnen SaaS-Produkten werden in diesem Muster nicht behandelt.
- Dieses Muster stellt den Amazon Cognito-Service nur in einer einzigen AWS-Region bereit.

Architektur

Zieltechnologie-Stack

- Amazon API Gateway
- Amazon Cognito

- AWS CloudTrail
- Amazon CloudWatch
- Amazon DynamoDB
- IAM
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Step-Funktionen

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Verwaltung von Mandantenlebenszyklen über mehrere SaaS-Produkte hinweg auf einer einzigen Steuerebene in der AWS Cloud.

Das Diagramm zeigt den folgenden Workflow:

1. Ein AWS-Benutzer initiiert Mandantenbereitstellung, Produktbereitstellung oder administrative Aktionen, indem er einen Aufruf an einen API Gateway-Endpunkt tätigt.
2. Der Benutzer wird durch ein Zugriffstoken authentifiziert, das aus einem Amazon Cognito-Benutzerpool oder einem anderen IdP abgerufen wird.
3. Einzelne Bereitstellungs- oder Verwaltungsaufgaben werden von Lambda-Funktionen ausgeführt, die in API Gateway-API-Endpunkte integriert sind.
4. Administrations-APIs für die Common-Tenant-Lösung (für Mandanten, Produkte und Benutzer) sammeln alle erforderlichen Eingabeparameter, Header und Token. Anschließend rufen die Administrations-APIs die zugehörigen Lambda-Funktionen auf.
5. IAM-Berechtigungen sowohl für die Administrations-APIs als auch für die Lambda-Funktionen werden vom IAM-Service validiert.
6. Lambda-Funktionen speichern und rufen Daten aus den Katalogen (für Mandanten, Produkte und Benutzer) in DynamoDB und Amazon S3 ab.
7. Nachdem die Berechtigungen validiert wurden, wird ein AWS Step Functions-Workflow aufgerufen, um eine bestimmte Aufgabe auszuführen. Das Beispiel im Diagramm zeigt einen Mandantenbereitstellungs-Workflow.

8. Einzelne AWS Step Functions-Workflow-Aufgaben werden in einem vordefinierten Workflow (Zustandsautomat) ausgeführt.
9. Alle wesentlichen Daten, die zum Ausführen der Lambda-Funktion erforderlich sind, die jeder Workflow-Aufgabe zugeordnet ist, werden entweder von DynamoDB oder Amazon S3 abgerufen. Möglicherweise müssen andere AWS-Ressourcen mithilfe einer AWS- CloudFormation Vorlage bereitgestellt werden.
10. Bei Bedarf sendet der Workflow eine Anforderung zur Bereitstellung zusätzlicher AWS-Ressourcen für ein bestimmtes SaaS-Produkt an das AWS-Konto dieses Produkts.
11. Wenn die Anforderung erfolgreich ist oder fehlschlägt, veröffentlicht der Workflow die Statusaktualisierung als Nachricht an ein Amazon SNS-Thema.
12. Amazon SNS hat das Amazon SNS-Thema des Step-Functions-Workflows abonniert.
13. Amazon SNS sendet dann die Aktualisierung des Workflow-Status zurück an den AWS-Benutzer.
14. Protokolle der Aktionen jedes AWS-Services, einschließlich eines Audit-Trails von API-Aufrufen, werden an gesendet CloudWatch. Spezifische Regeln und Alarme können in CloudWatch für jeden Anwendungsfall konfiguriert werden.
15. Protokolle werden zu Prüfungszwecken in Amazon S3-Buckets archiviert.

Automatisierung und Skalierung

Dieses Muster verwendet eine CloudFormation Vorlage, um die Bereitstellung der Common-Tenant-Lösung zu automatisieren. Die Vorlage kann Ihnen auch dabei helfen, die zugehörigen Ressourcen schnell nach oben oder unten zu verkaufen.

Weitere Informationen finden Sie unter Arbeiten mit AWS- CloudFormation Vorlagen im AWS-CloudFormation Benutzerhandbuch.

Tools

Tools

- Amazon API Gateway unterstützt Sie beim Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST-, HTTP- und - WebSocket APIs in jeder Größenordnung.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Governance, Compliance und des Betriebsrisikos Ihres AWS-Kontos.

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Austausch von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Bewährte Methoden

Die Lösung in diesem Muster verwendet eine einzige Steuerebene, um das Onboarding mehrerer Mandanten zu verwalten und den Zugriff auf mehrere SaaS-Produkte zu ermöglichen. Die Steuerebene hilft Administratorbenutzern bei der Verwaltung von vier anderen, Feature-spezifischen Ebenen:

- Sicherheitsebene
- Workflow-Ebene
- Kommunikationsebene
- Protokollierungs- und Überwachungsebene

Polen

Konfigurieren der Sicherheitsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Anforderungen für Ihre Multi-Tenant-SaaS-Plattform fest.	Legen Sie detaillierte Anforderungen für Folgendes fest: • Mandanten • Benutzer • Rollen • SaaS-Produkte • Subscriptions (Abonnements) • Profilaustausch	Cloud-Architekt, AWS-Systemadministrator
Richten Sie den Amazon Cognito-Service ein.	Folgen Sie den Anweisungen unter Erste Schritte mit Amazon Cognito im Amazon Cognito-Entwicklerhandbuch.	Cloud-Architekt
Konfigurieren Sie die erforderlichen IAM-Richtlinien.	Erstellen Sie die erforderlichen IAM-Richtlinien für Ihren Anwendungsfall. Ordnen Sie dann die Richtlinien IAM-Rollen in Amazon Cognito zu. Weitere Informationen finden Sie unter Verwalten des Zugriffs mithilfe von Richtlinien und Rollenbasierte Zugriffskontrolle im Amazon-Amazon Cognito-Entwicklerhandbuch.	Cloud-Administrator, Cloud-Architekt, AWS IAM-Sicherheit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die erforderlichen API-Berechtigungen.	Richten Sie API Gateway-Zugriffsberechtigungen mithilfe von IAM-Rollen und -Richtlinien und Lambda-Genehmigern ein. Anweisungen finden Sie in den folgenden Abschnitten des Entwicklerhandbuchs für Amazon API Gateway: • Steuern des Zugriffs auf eine API mit IAM-Berechtigungen • API Gateway-Lambda-Genehmiger verwenden	Cloud-Administrator, Cloud-Architekt

Konfigurieren der Datenebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erforderlichen Datenkataloge.	1. Erstellen Sie DynamoDB-Tabellen, um Daten für die Benutzerkataloge zu speichern. Stellen Sie sicher, dass Sie Benutzerattribute und Rollen einschließen. Stellen Sie außerdem sicher, dass Sie eine Datenmodellierung für die Katalogtabellen durchführen, um die erforderlichen und optionalen Attribute für	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	jeden Benutzer und jede Rolle beizubehalten. 2. Erstellen Sie DynamoDB-Tabellen, um Daten für die Produktkataloge zu speichern. Stellen Sie sicher, dass Sie die spezifischen Anwendungsfälle für Ihre SaaS-Produkte modellieren. 3. Erstellen Sie DynamoDB-Tabellen, um Daten für die Tenant-Kataloge zu speichern. Stellen Sie sicher, dass Sie Abonnementmodelle für Mandanten, Produkte und Lizenzen für Multi-SaaS-Abonnements und Tags einrichten. Weitere Informationen finden Sie unter Einrichten von DynamoDB im Amazon-DynamoDB-Entwicklerhandbuch.	

Konfigurieren der Steuerebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Lambda-Funktionen und API Gateway-APIs, um die erforderlichen	Erstellen Sie separate Lambda-Funktionen und API Gateway-APIs, um Folgendes	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aufgaben auf Steuerebene auszuführen.	hinzuzufügen, zu löschen und zu verwalten: • Benutzer • Mandanten • Produkte Weitere Informationen finden Sie unter Verwenden von AWS Lambda mit Amazon API Gateway im AWS Lambda-Entwicklerhandbuch.	

Konfigurieren der Workflow-Ebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Aufgaben, die AWS Step Functions-Workflows ausführen müssen.	Identifizieren und dokumentieren Sie die detaillierten AWS Step Functions-Workflow-Anforderungen für Folgendes: • Benutzer • Mandanten • Produkte Wichtig: Stellen Sie sicher, dass die wichtigsten Stakeholder die Anforderungen genehmigen.	App-Besitzer
Erstellen Sie die erforderlichen AWS Step Functions-Workflows.	1. Erstellen Sie die erforderlichen Workflows für Benutzer, Mandanten	App-Entwickler, Build-Verantwortlicher

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Produkte in AWS Step Functions . Weitere Informationen finden Sie im AWS Step Functions-Entwicklerhandbuch. 2. Identifizieren Sie die Mechanismen zur Wiederholung und Fehlerbehandlung. Weitere Informationen finden Sie unter Umgang mit Fehlern, Wiederholungen und Hinzufügen von Warnungen zu Step Function State Machines im AWS Blog. 3. Implementieren Sie die Workflow-Schritte mithilfe von Lambda-Funktionen. Anweisungen finden Sie unter Erstellen eines Step Functions-Zustandsautomaten, der Lambda verwendet im AWS Step Functions-Entwicklerhandbuch. 4. Integrieren Sie nach Bedarf alle externen Services in AWS Step Functions. 5. Behalten Sie den Status jedes Workflows in einer DynamoDB-Tabelle bei und kommunizieren Sie den Status jedes Workflows mithilfe von Amazon SNS.	

Konfigurieren der Kommunikationsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Amazon SNS-Themen.	Erstellen Sie Amazon SNS-Themen, um Benachric htigungen über Folgendes zu erhalten: • Workflow-Status • Fehler • Wiederholversuche Weitere Informationen finden Sie unter Erstellen eines SNS-Themas im Amazon SNS-Entwicklerhandbuch.	App-Eigentümer, Cloud-Arc hitekt
Abonnieren Sie Endpunkte für jedes Amazon SNS-Thema.	Um Nachrichten zu erhalten, die zu einem Amazon SNS-Thema veröffentlicht wurden, müssen Sie für jedes Thema einen Endpunkt abonnieren. Weitere Informationen finden Sie unter Abonnieren eines Amazon SNS-Themas im Amazon SNS-Entwicklerhand buch.	App-Entwickler, Cloud-Arc hitekt

Konfigurieren der Protokollierungs- und Überwachungsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Protokollierung für jede Komponente der Common-Tenant-Lösung.	Aktivieren Sie die Protokollierung auf Komponentenebene für jede Ressource in der von Ihnen erstellten Common-Tenant-Lösung. Detaillierte Informationen finden Sie hier: • Wie aktiviere ich CloudWatch Protokolle zur Fehlerbehebung bei meiner API Gateway-REST-API oder WebSocket -API? (AWS Knowledge Center) • Protokollierung mit -CloudWatch Protokollen (Entwicklerhandbuch für AWS Step Functions) • AWS Lambda-Funktionsprotokollierung in Python (AWS Lambda-Entwicklerhandbuch) • Protokollierung und Überwachung in Amazon Cognito (Entwickle rhandbuch für Amazon Cognito) • Überwachung mit Amazon CloudWatch (Amazon-DynamoDB-Entwicklerhandbuch)	App-Entwickler, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Sie können Protokolle für jede Ressource mithilfe von IAM-Richtlinien in einem zentralen Protokollierungskonto konsolidieren. Weitere Informationen finden Sie unter Zentralisierte Protokollierung und Sicherheitsleitplanken für mehrere Konten.	

Bereitstellen und Bereitstellen der Common-Tenant-Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie - CloudFormation Vorlagen.	Automatisieren Sie die Bereitstellung und Wartung der vollständigen Common-Tenant-Lösung und ihrer Komponenten mithilfe von - CloudFormation Vorlagen. Weitere Informationen finden Sie im AWS- CloudFormation Benutzerhandbuch.	App-Entwickler, DevOps Techniker, CloudFormation Entwickler

Zugehörige Ressourcen

- Steuern des Zugriffs auf eine REST-API mithilfe von Amazon Cognito-Benutzerpools als Genehmiger (Entwicklerhandbuch für Amazon API Gateway)
- API Gateway-Lambda-Genehmiger verwenden (Entwicklerhandbuch für Amazon API Gateway)
- Amazon Cognito-Benutzerpools (Amazon Cognito-Entwicklerhandbuch)
- Kontoübergreifende regionsübergreifende CloudWatch Konsole (Amazon- CloudWatch Benutzerhandbuch)

Mehr Muster

- Automatisieren Sie die Identifizierung und Planung von Migrationsstrategien mithilfe von AppScore
- Automatisieren der Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation
- Erstellen einer Serverless-Architektur mit mehreren Mandanten in Amazon OpenSearch Service
- Implementieren Sie die SaaSSaaSTenant-Isolation für Amazon S3 mithilfe eines AWS Lambda-Token-Verkäufers
- Integrieren Sie Stonebranch Universal Controller in AWS Mainframe Modernization
- Mandanten-Onboarding in SaaS-Architektur für das Silomodell mit C# und AWS CDK

Sicherheit, Identität, Compliance

Themen

- Löschen ungenutzter Amazon Elastic Block Store (Amazon EBS)-Volumes mithilfe von AWS Config und AWS Systems Manager
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform
- Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme in mehreren Codeergebnissen gleichzeitig erkennt
- Stellen Sie mithilfe von AWS Config detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit
- Stellen Sie präventive attributebasierte Zugriffskontrollen für öffentliche Subnetze bereit
- Stellen Sie die Lösung Security Automations für AWS WAF mithilfe von Terraform bereit
- Generieren Sie dynamisch eine IAM-Richtlinie mit IAM Access Analyzer mithilfe von Step Functions
- Aktivieren Sie Amazon GuardDuty unter bestimmten Bedingungen mithilfe von AWS-Vorlagen CloudFormation
- Aktivieren der transparenten Datenverschlüsselung in Amazon RDS für SQL Server
- Stellen Sie sicher, dass CloudFormation AWS-Stacks von autorisierten S3-Buckets aus gestartet werden
- Sicherstellen, dass AWS Load Balancer sichere Listener-Protokolle (HTTPS, SSL/TLS) verwenden
- Sicherstellen, dass die Verschlüsselung für Amazon-EMR-Daten im Ruhezustand beim Start aktiviert ist
- Sicherstellen, dass ein IAM-Profil einer EC2-Instance zugeordnet ist
- Sicherstellen, dass ein Amazon-Redshift-Cluster bei der Erstellung verschlüsselt wird
- Exportieren Sie einen Bericht über AWS IAM Identity Center-Identitäten und deren Zuweisungen mithilfe von PowerShell
- Überwachen und Korrigieren des geplanten Löschens von AWS KMS-Schlüsseln
- Identifizieren öffentlicher S3-Buckets in AWS Organizations mithilfe von Security Hub
- Verwalten von AWS IAM Identity Center-Berechtigungssätzen als Code mithilfe von AWS CodePipeline
- Verwalten von Anmeldeinformationen mit AWS Secrets Manager
- Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung
- Überwachen Sie ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand
- Überwachen Sie EC2-Instance-Schlüsselpaare mit AWS Config

- Überwachen von ElastiCache Clustern für Sicherheitsgruppen
- IAM-Root-Benutzeraktivitäten überwachen
- Senden einer Benachrichtigung, wenn ein IAM-Benutzer erstellt wird
- Verhindern Sie den Internetzugang auf Kontoebene mithilfe einer Dienststeuerungsrichtlinie
- Scannen Sie Git-Repositorys mithilfe von git-secrets auf sensible Informationen und Sicherheitsprobleme
- Senden von Warnungen von AWS Network Firewall an einen Slack-Kanal
- Vereinfachen der Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM
- Deaktivieren von Sicherheitsstandardkontrollen für alle Security Hub-Mitgliedskonten in einer Umgebung mit mehreren Konten
- Aktualisieren von AWS CLI-Anmeldeinformationen von AWS IAM Identity Center mithilfe von PowerShell
- Verwenden von AWS Config zur Überwachung von Amazon Redshift-Sicherheitskonfigurationen
- Verwenden Sie die Network Firewall, um die DNS-Domänennamen von der Server Name Indication (SNI) für ausgehenden Datenverkehr zu erfassen
- Verwenden von Terraform zum automatischen Aktivieren von Amazon GuardDuty für eine Organisation
- Stellen Sie sicher, dass neue Amazon-Redshift-Cluster über erforderliche SSL-Endpunkte verfügen
- Überprüfen, ob neue Amazon-Redshift-Cluster in einer VPC gestartet werden
- Mehr Muster

Greifen Sie über eine ASP.NET Core-App mithilfe von Amazon Cognito Cognito-Identitätspools auf AWS-Services zu

Erstellt von Bibhuti Sahu (AWS) und Marcelo Barbosa (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Web- und mobile Apps	AWS-Dienste: Amazon Cognito

Übersicht

In diesem Muster wird beschrieben, wie Sie Amazon Cognito Cognito-Benutzerpools und Identitätspools konfigurieren und dann einer ASP.NET Core-App den Zugriff auf AWS-Ressourcen nach erfolgreicher Authentifizierung ermöglichen können.

Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und mobilen Apps. Die beiden Hauptkomponenten von Amazon Cognito sind Benutzerpools und Identitätspools.

Ein Benutzerpool ist ein Benutzerverzeichnis in Amazon Cognito. Mit einem Benutzerpool können sich Ihre Benutzer über Amazon Cognito bei Ihrer Web- oder mobilen Anwendung anmelden. Ihre Benutzer können sich auch über soziale Identitätsanbieter wie Google, Facebook, Amazon oder Apple sowie über SAML-Identitätsanbieter anmelden.

Amazon-Cognito-Identitätspools (Verbundidentitäten) bieten Ihnen die Möglichkeit, eindeutige Identitäten für die Benutzer zu erstellen und diese mit Identitätsanbietern zu verbinden. Mit einem Identitätspool können Sie temporäre AWS-Anmeldeinformationen mit eingeschränkten Rechten abrufen, um auf andere AWS-Services zuzugreifen. Bevor Sie mit der Nutzung Ihres neuen Amazon Cognito Cognito-Identitätspools beginnen können, müssen Sie eine oder mehrere AWS Identity and Access Management (IAM) -Rollen zuweisen, um die Zugriffsebene zu bestimmen, die Ihre Anwendungsbenutzer auf Ihre AWS-Ressourcen haben sollen. Identitäten-Pools definieren zwei Arten von Identitäten: authentifizierte und nicht authentifizierte. Jedem Identitätstyp kann eine eigene Rolle in IAM zugewiesen werden. Authentifizierte Identitäten gehören Benutzern, die von einem öffentlichen Anmeldeanbieter (Amazon Cognito Cognito-Benutzerpools, Facebook, Google, SAML oder einem beliebigen OpenID Connect-Anbieter) oder einem Entwickler-Anbieter (Ihr eigener

Backend-Authentifizierungsprozess) authentifiziert wurden, wohingegen nicht authentifizierte Identitäten in der Regel Gastbenutzern gehören. Wenn Amazon Cognito eine Benutzeranfrage erhält, bestimmt der Service, ob die Anfrage authentifiziert oder nicht authentifiziert ist, bestimmt, welche Rolle diesem Authentifizierungstyp zugeordnet ist, und verwendet dann die dieser Rolle zugeordnete Richtlinie, um auf die Anfrage zu antworten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto mit Amazon Cognito- und IAM-Berechtigungen
- Zugriff auf die AWS-Ressourcen, die Sie verwenden möchten
- ASP.NET Core 2.0.0 oder höher

Architektur

Technologie-Stack

- Amazon Cognito
- ASP.NET-Kern

Zielarchitektur

Tools

Tools, SDKs und AWS-Services

- Visual Studio oder Visual Studio Code
- Amazon. AspNetCore.Identity.Cognito (1.0.4) — Paket NuGet
- AWSSDK.S3 (3.3.110.32) — Paket NuGet
- Amazon Cognito

Code

Die angehängte ZIP-Datei enthält Beispieldateien, die Folgendes veranschaulichen:

- Wie rufe ich ein Zugriffstoken für den angemeldeten Benutzer ab
- So tauschen Sie ein Zugriffstoken gegen AWS-Anmeldeinformationen aus
- So greifen Sie mit AWS-Anmeldeinformationen auf den Amazon Simple Storage Service (Amazon S3) -Service zu

IAM-Rolle für authentifizierte Identitäten

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mobileanalytics:PutEvents",
        "cognito-sync:*",
        "cognito-identity:*",
        "s3:ListAllMyBuckets*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Epen

Erstellen Sie einen Amazon Cognito Cognito-Benutzerpool

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzerpool.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon Cognito Cognito-Konsole unter https://console.aws.amazon.com/cognito/home.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Manage User Pools (Benutzerpools verwalten). 3. Wählen Sie in der rechten oberen Ecke der Seite Create a User Pool (Benutzerpool erstellen) aus. 4. Geben Sie einen Namen für Ihren Benutzerpool ein, wählen Sie Standard überprüfen und dann Pool erstellen aus. 5. Notieren Sie die Pool-ID.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen App-Client hinzu.	Sie können eine App erstellen, um die integrierten Webseiten für die Registrierung und Anmeldung Ihrer Benutzer zu verwenden. 1. Wählen Sie in der Navigationsleiste auf der linken Seite der Benutzerpool-Seite unter Allgemeine Einstellungen die Option App-Clients und dann App-Client hinzufügen aus. 2. Geben Sie Ihrer App einen Namen und wählen Sie dann App-Client erstellen. 3. Notieren Sie sich die App-Client-ID und den geheimen Client-Schlüssel (wählen Sie „Details anzeigen“, um den geheimen Client-Schlüssel zu sehen).	Developer

Amazon-Cognito-Identitätspool erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen -Identitätenpool.	1. Wählen Sie in der Amazon Cognito Cognito-Konsole Manage Identity Pools und dann Create new identity pool aus. 2. Geben Sie einen Namen für den Identitätspool ein.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wenn Sie nicht authentif izierte Identitäten aktivieren möchten, wählen Sie diese Option im Abschnitt Nicht authentifizierte Identitäten aus. 4. Konfigurieren Sie im Abschnitt Authentifizierungs anbieter den Cognito-I dentitätspool, indem Sie die Benutzerpool-ID und die App-Client-ID festlegen , und wählen Sie dann Create Pool aus.	
Weisen Sie IAM-Rollen für den Identitätspool zu.	Sie können die IAM-Rollen für authentifizierte und nicht authentifizierte Benutzer bearbeiten oder die Standarde instellungen beibehalten und dann Zulassen wählen. Für dieses Muster bearbeiten wir die authentifizierte IAM-Rolle und gewähren Zugriff für. `s3:ListAllMyBuckets` Beispielcode finden Sie weiter oben im Abschnitt Tools für die IAM-Rolle.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Identität spool-ID.	Wenn Sie im vorherigen Schritt Zulassen ausgewähl t haben, wird die Seite Erste Schritte mit Amazon Cognito angezeigt. Auf dieser Seite können Sie entweder die Identitätspool-ID aus dem Abschnitt AWS-Anmel deinformationen abrufen kopieren oder oben rechts Identitätspool bearbeiten auswählen und die Identität spool-ID aus dem angezeigten Bildschirm kopieren.	Developer

Konfigurieren Sie Ihre Beispiel-App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie die ASP.NET Core-Beispiel-Web-App.	1. Klonen Sie die Beispiel-.NET-Core-Web-App von https://github.com/aws/aws-aspnet-cognito-identity-provider.git. 2. Navigieren Sie zu dem `samples` Ordner und öffnen Sie die Lösung. In diesem Projekt konfiguri eren Sie die `appsettin gs.json` Datei und fügen eine neue Seite hinzu, auf der nach erfolgreicher	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anmeldung alle S3-Buckets gerendert werden.	
Fügen Sie Abhängigkeiten hinzu.	Fügen Sie Ihrer ASP.NET Core-Anwendung eine NuGet Abhängigkeit für `Amazon.AspNetCore.Identity.Cognito` hinzu.	Developer
Fügen Sie die Konfigurationsschlüssel und Werte zu appsettings.json hinzu.	Fügen Sie den Code aus der angehängten `appsettings.json` Datei in Ihre `appsettings.json` Datei ein und ersetzen Sie dann die Platzhalter durch die Werte aus den vorherigen Schritten.	Developer
Erstellen Sie einen neuen Benutzer und melden Sie sich an.	Erstellen Sie einen neuen Benutzer im Amazon Cognito Cognito-Benutzerpool und stellen Sie sicher, dass der Benutzer unter Benutzer und Gruppen im Benutzerpool vorhanden ist.	Developer
Erstellen Sie eine neue Razor-Seite namens MyS3Buckets.	Fügen Sie Ihrer Beispiel-App eine neue ASP.NET Core Razor-Seite hinzu und ersetzen Sie den Inhalt für und aus dem angehängten Beispiel `MyS3Bucket.cshtml` . `MyS3Bucket.cshtml.cs` Fügen Sie die neue MyS3Bucket-Seite unter Navigation auf der Seite hinzu. `_Layout.cshtml`	Developer

Fehlerbehebung

Problem	Lösung
Nachdem Sie die Beispielanwendung aus dem GitHub Repository geöffnet haben, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, das NuGet Paket zum Samples-Projekt hinzuzufü gen.	Stellen Sie sicher, dass Sie in dem `src` Ordner den Verweis auf das `Amazon.AspNetCore.Identity.Cognito` Projekt aus der `Samples.sln` Datei entfernen. Sie können das NuGet Paket dann problemlos zum Samples-Projekt hinzufügen.

Zugehörige Ressourcen

- Amazon Cognito
- Amazon-Cognito-Benutzerpools
- Amazon Cognito Cognito-Identitätspools
- Beispiele für Zugriffsrichtlinien
- GitHub - AWS ASP.NET Cognito Identitätsanbieter

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Authentifizieren von Microsoft SQL Server auf Amazon EC2 mit AWS Directory Service

Erstellt von Jagadish Kantubugata (AWS) und Bolhun Ajhun (AWS)

Umgebung: PoC oder Pilotprojekt	Quelle: Active Directory	Ziel: AWS Directory Service
R-Typ: N/A	Workload: Microsoft	Technologien: Sicherheit, Identität, Compliance; Datenbanken
AWS-Services: AWS Directory Service		

Übersicht

Dieses Muster beschreibt, wie Sie ein AWS Directory Service-Verzeichnis erstellen und es verwenden, um Microsoft SQL Server auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance zu authentifizieren.

AWS Directory Service bietet mehrere Möglichkeiten, Amazon Cloud Directory und Microsoft Active Directory (AD) mit anderen AWS-Services zu verwenden. Verzeichnisse speichern Informationen über Benutzer, Gruppen und Geräte, und Administratoren verwenden sie, um den Zugriff auf Informationen und Ressourcen zu verwalten. AWS Directory Service bietet mehrere Verzeichnisoptionen für Benutzer, die ihre vorhandenen Microsoft AD- oder Lightweight Directory Access Protocol (LDAP)-fähigen Anwendungen in der Cloud verwenden möchten. Dieselben Optionen bietet es Entwicklern, die ein Verzeichnis zum Verwalten von Benutzern, Gruppen, Geräten und Zugriff benötigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Virtual Private Cloud (VPC) mit mindestens zwei privaten Subnetzen und zwei öffentlichen Subnetzen

- Eine AWS Identity and Access Management (IAM)-Rolle, um den Server mit der Domain zu verbinden

Architektur

Quelltechnologie-Stack

- Die Quelle kann ein On-Premises-Active-Directory sein

Zieltechnologie-Stack

- AWS Directory Service für Microsoft Active Directory (AWS Managed Microsoft AD)

Zielarchitektur

Tools

- SQL Server Management Studio (SSMS) ist ein Tool zur Verwaltung von Microsoft SQL Server, einschließlich Zugriff, Konfiguration und Verwaltung von SQL Server-Komponenten.

Polen

Einrichten eines Verzeichnisses

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie AWS Managed Microsoft AD als Verzeichnistyp aus.	Wählen Sie in der AWS Directory Service-Konsole Verzeichnisse, Verzeichnis einrichten, AWS Managed Microsoft AD ,Weiter aus.	DevOps
Wählen Sie Edition aus.	Wählen Sie in den verfügbaren Editionen für AWS	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Managed Microsoft AD Standard Edition aus.	
Geben Sie den DNS-Namen des Verzeichnisses an.	Verwenden Sie einen vollquali fizierten Domänennamen. Dieser Name wird nur innerhalb Ihrer VPC aufgelöst . Er muss nicht öffentlich auflösbar sein.	DevOps
Legen Sie das Administrator-Passwort fest.	Legen Sie das Passwort für den standardmäßigen Administratorbenutzer mit dem Namen Admin fest.	DevOps
Wählen Sie die VPC und die Subnetze aus.	Wählen Sie die VPC aus, die Ihr Verzeichnis und die Subnetze für die Domain-Co ntroller enthalten soll. Wenn Sie keine VPC mit mindesten s zwei Subnetzen haben, müssen Sie eines erstellen.	DevOps
Überprüfen Sie das Verzeichn is und starten Sie es.	Überprüfen Sie die Editions- und Preisinformationen für das Verzeichnis und wählen Sie dann Verzeichnis erstellen aus.	DevOps

Starten einer EC2-Instance für SQL Server in der Domain

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein AMI für SQL Server aus.	Die Schritte in diesem Epos verbinden eine Windows EC2-	DevOps, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instance nahtlos mit Ihrem AWS Managed Microsoft AD-Verzeichnis. Wählen Sie in der Amazon EC2-Konsole Instance starten und dann das entsprechende Amazon Machine Image (AMI) für SQL Server aus.	
Konfigurieren von Instance-Details.	Konfigurieren Sie die Windows-Instance so, dass sie Ihren Anforderungen für SQL Server entspricht.	DevOps, DBA
Wählen Sie den Namen des Schlüsselpaars aus.	Wählen Sie ein Schlüsselpaar aus und starten Sie dann die Instance.	DevOps, DBA
Fügen Sie ein Netzwerk hinzu.	Sie können die VPC auswählen, in der Ihr Verzeichnis erstellt wurde.	DevOps, DBA
Wählen Sie unter IAM role (IAM-Rolle) eine Rolle aus.	Wählen Sie unter Erweitert e Einstellungen ein IAM-Profil aus, dem die von AWS verwalteten Richtlini en `AmazonSSMDirectory ServiceAccess` angefügt `AmazonSSMManagedIn stanceCore` sind.	DevOps, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie ein Subnetz hinzu.	Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.	DevOps, DBA
Wählen Sie Ihre Domäne aus.	Wählen Sie die von Ihnen erstellte Domain aus der Liste Domain-Join-Verzeichnis aus.	DevOps, DBA
Starten Sie die Instance.	Wählen Sie Launch Instance (Instance starten) aus.	DBA

Authentifizieren von SQL Server mit Directory Service

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich als Windows-Administrator an.	Melden Sie sich mit Windows-Administratoranmeldeinformationen bei der Windows-EC2-Instance an.	DBA
Melden Sie sich bei SQL Server an.	Starten Sie SQL Server Management Studio (SSMS) und melden Sie sich mit der Windows-Authentifizierungsmethode bei SQL Server an.	DBA
Erstellen Sie eine Anmeldung für den Verzeichnisbenutzer.	Wählen Sie in SSMS Sicherheit und dann Neue Anmeldung aus.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach einem Anmeldenamen.	Wählen Sie die Suchschaltfläche neben dem Anmeldetextfeld aus.	DBA
Wählen Sie einen Speicherort aus.	Wählen Sie im Dialogfeld Benutzer oder Gruppe auswählen die Option Standorte aus.	DBA
Geben Sie Netzwerkanmeldeinformationen ein.	Geben Sie die vollständig qualifizierten Netzwerkanmeldeinformationen ein, die Sie beim Erstellen des Verzeichnisservices verwendet haben, z. B.: `test.com\admin` .	DBA
Wählen Sie das Verzeichnis aus.	Wählen Sie den AWS-Verzeichnisnamen und dann OK aus.	DBA
Wählen Sie einen Objektnamen aus.	Wählen Sie den Benutzer aus, für den Sie die Anmeldung erstellen möchten. Wählen Sie den Speicherort aus, wählen Sie das gesamte Verzeichnis aus, suchen Sie nach dem Benutzer und fügen Sie die Anmeldung hinzu.	DBA
Melden Sie sich bei der SQL Server-Instance an.	Melden Sie sich mit Ihren Domänenanmeldeinformationen bei der Windows EC2-Instance für SQL Server an.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich als Domänenbenutzer bei SQL Server an.	Starten Sie SSMS und stellen Sie mithilfe der Windows-Authentifizierungsmethode eine Verbindung mit der Datenbank-Engine her.	DBA

Zugehörige Ressourcen

- AWS Directory Service-Dokumentation (AWS-Website)
- Erstellen Ihres AWS Managed Microsoft AD-Verzeichnisses (Dokumentation zu AWS Directory Service)
- Nahtloser Beitritt zu einer Windows EC2-Instance (Dokumentation zu AWS Directory Service)
- Microsoft SQL Server auf AWS (AWS-Website)
- SSMS-Dokumentation (Microsoft-Website)
- Erstellen einer Anmeldung in SQL Server (SQL-Server-Dokumentation)

Automatisieren der Reaktion auf Vorfälle und der Forensik

Erstellt von Lucas Kauffman (AWS) und Tomek Jakubowski (AWS)

Code-Repository: aws-automated-incident-response-und-forensische	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance
AWS-Services: Amazon EC2; AWS Lambda ;Amazon S3; AWS Security Hub; AWS Identity and Access Management		

Übersicht

Dieses Muster stellt eine Reihe von Prozessen bereit, die AWS Lambda-Funktionen verwenden, um Folgendes bereitzustellen:

- Eine Möglichkeit, den Vorfall-Reaktionsprozess mit minimalem Wissen zu initiieren
- Automatisierte, wiederholbare Prozesse, die dem AWS Security Incident Response Guide entsprechen
- Trennung von Konten für den Betrieb der Automatisierungsschritte, das Speichern von Artefakten und das Erstellen forensischer Umgebungen

Das Framework für automatisierte Vorfallreaktion und Forensik folgt einem standardmäßigen digitalen forensischen Prozess, der aus den folgenden Phasen besteht:

1. Bedingung
2. Zeitpunkt
3. Trichter
4. Analyse

Sie können Untersuchungen an statischen Daten (z. B. erworbenen Speicher- oder Datenträgerabbildern) und an dynamischen Daten durchführen, die live, aber auf getrennten Systemen sind.

Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei AWS-Konten:
  - Sicherheitskonto, das ein vorhandenes Konto sein kann, aber vorzugsweise neu ist
  - Forensik-Konto, vorzugsweise neu
- AWS Organizations einrichten
- In den Mitgliedskonten von Organizations:
  - Die Amazon Elastic Compute Cloud (Amazon EC2)-Rolle muss über Zugriff auf Amazon Simple Storage Service (Amazon S3) verfügen und von AWS Systems Manager zugänglich sein. Wir empfehlen die Verwendung der von `AmazonSSMManagedInstanceCore` AWS verwalteten Rolle. Beachten Sie, dass diese Rolle automatisch an die EC2-Instance angehängt wird, wenn die Reaktion auf Vorfälle initiiert wird. Nachdem die Antwort abgeschlossen ist, entfernt AWS Identity and Access Management (IAM) alle Rechte für die Instance.
  - Virtual Private Cloud (VPC)-Endpunkte im AWS-Mitgliedskonto und in den VPCs für Vorfallreaktion und Analyse . Diese Endpunkte sind: S3 Gateway, EC2 Messages, SSM und SSM Messages.
- AWS-Befehlszeilenschnittstelle (AWS CLI), die auf den EC2-Instances installiert ist. Wenn auf den EC2-Instances die AWS CLI nicht installiert ist, ist ein Internetzugang erforderlich, damit der Datenträger-Snapshot und die Speicherakquise funktionieren. In diesem Fall wenden sich die Skripts an das Internet, um die AWS CLI-Installationsdateien herunterzuladen, und installieren sie auf den Instances.

Einschränkungen

- Dieses Framework beabsichtigt nicht, Artefakte zu generieren, die als elektronische Beweise betrachtet werden können, die in der Frau unterdrückbar sind.
- Derzeit unterstützt dieses Muster nur Linux-basierte Instances, die auf der x86-Architektur ausgeführt werden.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- IAM
- Lambda
- Amazon S3
- AWS Key Management System (AWS KMS)
- AWS Security Hub
- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

Zielarchitektur

Zusätzlich zum Mitgliedskonto besteht die Zielumgebung aus zwei Hauptkonten: einem Sicherheitskonto und einem Forensics-Konto. Aus den folgenden Gründen werden zwei Konten verwendet:

- So trennen Sie sie von allen anderen Kundenkonten, um den Explosionsradius im Falle einer fehlgeschlagenen forensischen Analyse zu reduzieren
- Um die Isolation und den Schutz der Integrität der analysierten Artefakte sicherzustellen
- So halten Sie die Untersuchung vertraulich
- Um Situationen zu vermeiden, in denen die Bedrohungsakteure möglicherweise alle Ressourcen verwendet haben, die Ihrem kompromittierten AWS-Konto sofort zur Verfügung stehen, indem sie Service Quotas erreicht haben und Sie so daran hindern, eine Amazon EC2-Instance zu instanziieren, um Untersuchungen durchzuführen.

Darüber hinaus ermöglicht die Verwendung separater Sicherheits- und Forensikkonten die Erstellung separater Rollen – ein Responder für den Erhalt von Beweisen und ein Telefonie für deren Analyse. Jede Rolle hätte Zugriff auf ihr eigenes Konto.

Das folgende Diagramm zeigt nur die Interaktion zwischen den Konten. Details zu jedem Konto werden in nachfolgenden Diagrammen angezeigt, und es wird ein vollständiges Diagramm angehängt.

Das folgende Diagramm zeigt das Mitgliedskonto.

1. Ein Ereignis wird an das Slack-Amazon SNS-Thema gesendet.

Das folgende Diagramm zeigt das Sicherheitskonto.

2. Das SNS-Thema im Sicherheitskonto initiiert forensische Ereignisse.

Das folgende Diagramm zeigt das Forensics-Konto.

Im Sicherheitskonto werden die beiden wichtigsten AWS Step Functions-Workflows für die Speicher- und Datenträgerabbilderfassung erstellt. Nachdem die Workflows ausgeführt wurden, greifen sie auf das Mitgliedskonto zu, das die an einem Vorfall beteiligten EC2-Instances enthält, und initiieren eine Reihe von Lambda-Funktionen, die einen Speicherabbild oder einen Festplattenabbild sammeln. Diese Artefakte werden dann im Forensics-Konto gespeichert.

Das Forensics-Konto enthält die Artefakte, die vom Step Functions-Workflow im S3-Bucket Analyseartefakte gesammelt wurden. Das Forensics-Konto wird auch über eine EC2 Image Builder-Pipeline verfügen, die ein Amazon Machine Image (AMI) einer Forensics-Instance erstellt. Derzeit basiert das Image auf SANS SIFT Workstation.

Der Build-Prozess verwendet die Wartungs-VPC, die über Konnektivität zum Internet verfügt. Das Bild kann später zum Hochfahren der EC2-Instance zur Analyse der gesammelten Artefakte in der Analyse-VPC verwendet werden.

Die Analyse-VPC hat keine Internetverbindung. Standardmäßig erstellt das Muster drei private Analysesubnetze. Sie können bis zu 200 Subnetze erstellen, was dem Kontingent für die Anzahl der Subnetze in einer VPC entspricht. Die VPC-Endpunkte müssen jedoch diese Subnetze hinzugefügt haben, damit AWS Systems Manager Sessions Manager laufende Befehle in ihnen automatisieren kann.

Aus Sicht bewährter Methoden empfehlen wir, AWS CloudTrail und AWS Config zu verwenden, um Folgendes zu tun:

- Verfolgen von Änderungen, die in Ihrem Forensics-Konto vorgenommen wurden
- Überwachen des Zugriffs und der Integrität der Artefakte, die gespeichert und analysiert werden

Workflow

Das folgende Diagramm zeigt die wichtigsten Schritte eines Workflows, der den Prozess und den Entscheidungsbaum von dem Zeitpunkt umfasst, an dem eine Instance kompromittiert wurde, bis sie analysiert und enthalten ist.

1. Wurde das `SecurityIncidentStatus`Tag mit dem Wert Analysieren festgelegt? Wenn ja, gehen Sie wie folgt vor:
   a. Fügen Sie die richtigen IAM-Profile für AWS Systems Manager und Amazon S3 an.
   b. Senden Sie eine Amazon SNS-Nachricht an die Amazon SNS-Warteschlange in Slack.
   c. Senden Sie eine Amazon SNS-Nachricht an die `SecurityIncident` Warteschlange.
   d. Rufen Sie den Zustandsautomaten Speicher und Datenträger-Erkennung auf.
2. Wurde Arbeitsspeicher und Festplatte erworben? Wenn ja, liegt ein Fehler vor.
3. Markieren Sie die EC2-Instance mit dem -`Contain`Tag.
4. Fügen Sie die IAM-Rolle und die Sicherheitsgruppe an, um die Instance vollständig zu isolieren.

Automatisierung und Skalierung

Ziel dieses Musters ist es, eine skalierbare Lösung zur Reaktion auf Vorfälle und Forensik über mehrere Konten innerhalb einer einzigen AWS Organizations-Organisation hinweg bereitzustellen.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Key Management Service (AWS KMS) hilft Ihnen beim Erstellen und Steuern kryptografischer Schlüssel zum Schutz Ihrer Daten.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS-Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang.

Code

Den Code und spezifische Anleitungen zur Implementierung und Verwendung finden Sie im Repository GitHub für automatisierte Vorfallreaktion und Forensics Framework.

Sekunden

Bereitstellen der CloudFormation Vorlagen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie CloudFormation Vorlagen bereit.	Die CloudFormation Vorlagen sind mit 1 bis 7 gekennzeichnet, wobei das erste Wort des Skriptnamens angibt, in welchem Konto die Vorlage bereitgestellt werden muss. Beachten Sie, dass die Reihenfolge des Startens der CloudFormation Vorlagen wichtig ist. • `1-forensic-AnalysisVPCnS3Buckets.yaml` : Wird im forensischen Konto bereitgestellt. Es erstellt die S3-Buckets und die Analyse-VPC und aktiviert CloudTrail. • `2-forensic-MaintenanceVPCnEC2ImageBuilderPipeline.yaml` : Stellt die Wartungs-VPC und die Image Builder-Pipeline basierend auf SANS SIFT bereit. • `3-security_IR-Disk_Mem_automation.yaml` : Stellt die Funktionen im Sicherheitskonto bereit, die die Festplatten-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Speichererfassung ermöglichen. • `4-security_LiME_Volatility_Factory.yaml` : Initiiert eine Build-Funktion, um mit der Erstellung der Speichermodule basierend auf den angegebenen AMI-IDs zu beginnen. Beachten Sie, dass sich AMI-IDs zwischen AWS-Regionen unterscheiden. Wenn Sie neue Speichermodule benötigen, können Sie dieses Skript mit den neuen AMI-IDs erneut ausführen. Erwägen Sie, dies in Ihre goldenen Image-AMI-Builder-Pipelines zu integrieren (falls in Ihrer Umgebung verwendet). • `5-member-IR-automation.yaml` : Erstellt die Funktion zur Automatisierung von Mitgliedsvorfällen, die den Vorgang zur Reaktion auf Vorfälle initiiert. Sie ermöglicht die gemeinsame Nutzung von Amazon Elastic Block Store (Amazon EBS)-Volumes über -Konten hinweg, die automatische Veröffentlichung an Slack-Kanäle	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	während des Vorfallre aktionsprozesses, die Initiierung des forensischen Prozesses und die Isolierun g der Instances nach Abschluss des Prozesses. • `6-forensic-artifac t-s3-policies.yaml` : Nachdem alle Skripts bereitgestellt wurden, korrigiert dieses Skript die Berechtigungen, die für alle kontoübergreifenden Interaktionen erforderlich sind. • `7-security-IR-vpc. yaml` : Konfiguriert eine VPC, die für die Verarbeit ung des Reaktionsvolumens auf Vorfälle verwendet wird. Um das Framework zur Reaktion auf Vorfälle für eine bestimmte EC2-Instance zu initiieren, erstellen Sie ein Tag mit dem Schlüssel `SecurityIncidentSt atus` und dem Wert `Analyze`. Dadurch wird die Lambda-Funktion des Mitglieds initiiert, die automatis ch die Isolierung und den Speicher sowie die Festplatt enaufnahme startet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Betreiben Sie das Framework.	Die Lambda-Funktion markiert die Komponente auch am Ende (oder bei einem Fehler) mit `Contain`. Dadurch wird die Eindämmung initiiert, die die Instance vollständig isoliert, ohne INBOUND/OUTBOUND-Sicherheitsgruppe und mit einer IAM-Rolle, die den gesamten Zugriff verweigert. Folgen Sie den Schritten im GitHub Repository .	AWS-Administrator

Bereitstellen von benutzerdefinierten Security Hub-Aktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die benutzerdefinierten Security Hub-Aktionen mithilfe einer CloudFormation Vorlage bereit.	Um eine benutzerdefinierte Aktion zu erstellen, damit Sie die Dropdown-Liste von Security Hub verwenden können, stellen Sie die `Modules/SecurityHub Custom Actions/SecurityHubCustomActions.yaml` CloudFormation Vorlage bereit. Ändern Sie dann die `IRAutomation` Rolle in jedem Mitgliedskonto, damit die Lambda-Funktion, die die Aktion ausführt, die `IRAutomation` Rolle	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	übernehmen kann. Weitere Informationen finden Sie im GitHub Repository .	

Zugehörige Ressourcen

- AWS Security Incident Response Guide

Zusätzliche Informationen

Durch die Verwendung dieser Umgebung kann ein Security Operations Center (SOC)-Team seinen Prozess zur Reaktion auf Sicherheitsvorfälle folgendermaßen verbessern:

- Möglichkeit, forensische Untersuchungen in einer getrennten Umgebung durchzuführen, um eine versehentliche Kompromittierung von Produktionsressourcen zu vermeiden
- Ein standardisierter, wiederholbarer, automatisierter Prozess zur Eindämmung und Analyse.
- Jedem Kontoinhaber oder Administrator die Möglichkeit geben, den Vorfallreaktionsprozess mit minimalem Wissen über die Verwendung von Tags zu initiieren
- Eine standardisierte, saubere Umgebung für die Durchführung von Vorfallanalysen und Forensik ohne das Rauschen einer größeren Umgebung
- Möglichkeit, mehrere Analyseumgebungen parallel zu erstellen
- Fokussierung von SOC-Ressourcen auf die Reaktion auf Vorfälle statt auf Wartung und Dokumentation einer Cloud-Forensikumgebung
- Umstellung von einem manuellen Prozess auf einen automatisierten Prozess, um Skalierbarkeit zu erreichen
- Verwenden von CloudFormation Vorlagen für Konsistenz und zur Vermeidung wiederholbarer Aufgaben

Darüber hinaus vermeiden Sie die Verwendung einer persistenten Infrastruktur und zahlen für Ressourcen, wenn Sie sie benötigen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren der Behebung von AWS Security Hub-Standardergebnissen

Erstellt von Chandini Penmetsa (AWS) und Boll Raj Jayarajan (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance	Workload: Alle anderen Workloads
AWS-Services: AWS CloudFormation; Amazon CloudWatch; AWS Lambda ; AWS Security Hub; Amazon SNS		

Übersicht

Mit AWS Security Hub können Sie Prüfungen auf bewährte Standardmethoden wie die folgenden aktivieren:

- Bewährte Methoden für AWS Foundational Security
- CIS-EWS-Foundations-Benchmark
- Payment Card Industry Data Security Standard (PCI DSS)

Jeder dieser Standards verfügt über vordefinierte Kontrollen. Security Hub prüft auf die Kontrolle in einem bestimmten AWS-Konto und meldet die Ergebnisse.

AWS Security Hub sendet EventBridge standardmäßig alle Ergebnisse an Amazon. Dieses Muster bietet eine Sicherheitskontrolle, die eine - EventBridge Regel bereitstellt, um die Standardergebnisse von AWS Foundational Security Best Practices zu identifizieren. Die Regel identifiziert die folgenden Ergebnisse für Auto Scaling, Virtual Private Clouds (VPCs), Amazon Elastic Block Store (Amazon EBS) und Amazon Relational Database Service (Amazon RDS) aus dem AWS Foundational Security Best Practices-Standard:

- [AutoScaling.1] Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load-Balancer-Zustandsprüfungen verwenden

- [EC2.2] Die VPC-Standardsicherheitsgruppe sollte eingehenden und ausgehenden Datenverkehr nicht zulassen.
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [RDS.1] RDS-Snapshots sollten privat sein.
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances und -Cluster konfiguriert werden
- [RDS.7] Für RDS-Cluster sollte der Löschschutz aktiviert sein

Die EventBridge Regel leitet diese Ergebnisse an eine AWS Lambda-Funktion weiter, die das Ergebnis behebt. Die Lambda-Funktion sendet dann eine Benachrichtigung mit Korrekturinformationen an ein Amazon Simple Notification Service (Amazon SNS)-Thema.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Korrekturbenachrichtigung erhalten möchten
- Security Hub und AWS Config sind in der AWS-Region aktiviert, in der Sie die Kontrolle bereitstellen möchten
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket in derselben Region wie die Kontrolle zum Hochladen des AWS Lambda-Codes

Einschränkungen

- Diese Sicherheitskontrolle behebt automatisch neue Erkenntnisse, die nach der Bereitstellung der Sicherheitskontrolle gemeldet wurden. Um vorhandene Erkenntnisse zu beheben, wählen Sie die Erkenntnisse manuell in der Security Hub-Konsole aus. Wählen Sie dann unter Aktionen die benutzerdefinierte Aktion AFSBPRemedy aus, die im Rahmen der Bereitstellung von AWS erstellt wurde CloudFormation.
- Diese Sicherheitskontrolle ist regional und muss in den AWS-Regionen bereitgestellt werden, die Sie überwachen möchten.
- Um VPC-Flow-Protokolle zu aktivieren, wird für die EC2.6-Korrektur eine Amazon CloudWatch -Logs-Protokollgruppe im Format /VpcFlowLogs/vpc_id erstellt. Wenn eine Protokollgruppe mit demselben Namen vorhanden ist, wird die vorhandene Protokollgruppe verwendet.

- Für das EC2.7-Refix wird zur Aktivierung der Amazon EBS-Standardverschlüsselung der AWS Key Management Service (AWS KMS)-Standardschlüssel verwendet. Diese Änderung verhindert die Verwendung bestimmter Instances, die keine Verschlüsselung unterstützen.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- Amazon SNS-Thema
- EventBridge Regel
- AWS Identity and Access Management (IAM)-Rollen für Lambda-Funktion, VPC Flow Logs und Amazon Relational Database Service (Amazon RDS) Enhanced Monitoring

Zielarchitektur

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS CloudFormation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

Tools

- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung von AWS-Ressourcen unterstützt, indem Infrastruktur als Code verwendet wird.
- EventBridge – Amazon EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software as a Service (SaaS)-Anwendungen und AWS-Services bereit und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- Lambda – AWS Lambda unterstützt das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.

- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Bewährte Methoden

- Nine AWS Security Hub – Bewährte Methoden
- Bewährte Methoden für AWS Foundational Security

Polen

Bereitstellen der Sicherheitskontrolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben Region befinden wie die Security Hub-Ergebnisse, die ausgewertet werden.	Cloud-Architektur
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die ZIP-Datei des Lambda-Codes, die im Abschnitt „Anfügungen“ bereitgestellt wird, in den definierten S3-Bucket hoch.	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CloudFormation Vorlage bereit.	Stellen Sie die AWS-CloudFormation Vorlage bereit, die als Anhang zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an.	Cloud-Architektur

Vervollständigen der Parameter in der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen des S3-Buckets an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epos erstellt haben.	Cloud-Architektur
Geben Sie das Amazon S3-Präfix an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket an, ohne Schrägstriche voranzustellen (z. B. <directory>/<file-name>.zip).	Cloud-Architektur
Geben Sie den ARN des SNS-Themas an.	Geben Sie den Amazon-Ressourcennamen (ARN) des SNS-Themas an, wenn Sie ein vorhandenes SNS-Thema für Korrekturbenachrichtigungen verwenden möchten. Um ein neues SNS-Thema zu verwenden, belassen Sie den Wert als „Keine“ (Standardwert).	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie eine E-Mail-Ad resse an.	Geben Sie eine E-Mail-Ad resse an, an die Sie die Korrekturbenachrichtigungen erhalten möchten (nur erforderlich, wenn AWS das SNS- CloudFormation Thema erstellen soll).	Cloud-Architektur
Definieren Sie die Protokoll ierungsebene.	Definieren Sie die Protokoll ierungsebene und die Häufigkeit für Ihre Lambda-Funktion. „Informationen“ bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. „Fehler“ bezeichnet Fehlerere ignisse, die der Anwendung weiterhin die Ausführun g ermöglichen könnten. „Warnung“ bezeichnet potenziell schädliche Situation en.	Cloud-Architektur
Geben Sie den ARN der IAM-Rolle für VPC Flow Logs an.	Geben Sie den IAM-Rolle n-ARN an, der für VPC-Flow-Protokolle verwendet werden soll. (Wenn „Keine“ als Eingabe eingegeben wird, CloudFormation erstellt AWS eine IAM-Rolle und verwendet sie.)	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den ARN der IAM-Rolle für RDS Enhanced Monitoring an.	Geben Sie den ARN der IAM-Rolle an, der für RDS Enhanced Monitoring verwendet werden soll. (Wenn „Keine“ eingegeben wird, CloudFormation erstellt AWS eine IAM-Rolle und verwendet sie.)	Cloud-Architektur

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Amazon SNS-Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde und ein neues SNS-Thema erstellt wurde, wird eine Abonnemen tnachricht an die von Ihnen angegebene E-Mail-Adresse gesendet. Um Korrektur benachrichtigungen zu erhalten, müssen Sie diese Abonnement-E-Mail-Nachricht bestätigen.	Cloud-Architektur

Zugehörige Ressourcen

- Erstellen eines Stacks in der AWS- CloudFormation Konsole
- AWS Lambda
- AWS Security Hub

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren von Sicherheitsscans für kontoübergreifende Workloads mit Amazon Inspector und AWS Security Hub

Erstellt von Ramya Pulipaka (AWS) und Bolsh Khanal (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Betrieb	AWS-Services: Amazon Inspector ;Amazon SNS; AWS Lambda; AWS Security Hub; Amazon CloudWatch

Übersicht

Dieses Muster beschreibt, wie Sie automatisch auf Schwachstellen in kontoübergreifenden Workloads in der Amazon Web Services (AWS) Cloud scannen.

Das Muster hilft bei der Erstellung eines Zeitplans für hostbasierte Scans von Amazon Elastic Compute Cloud (Amazon EC2)-Instances, die nach Tags oder für netzwerkbasierte Amazon Inspector-Scans gruppiert sind. Ein AWS- CloudFormation Stack stellt alle erforderlichen AWS-Ressourcen und -Services für Ihre AWS-Konten bereit.

Die Erkenntnisse von Amazon Inspector werden in AWS Security Hub exportiert und bieten Einblicke in Schwachstellen in Ihren Konten, AWS-Regionen, Virtual Private Clouds (VPCs) und EC2-Instances. Sie können diese Ergebnisse per E-Mail erhalten oder ein Amazon Simple Notification Service (Amazon SNS)-Thema erstellen, das einen HTTP-Endpunkt verwendet, um die Ergebnisse an Ticketing-Tools, Sicherheitsinformationen und Ereignismanagement (SIEM)-Software oder andere Sicherheitslösungen von Drittanbietern zu senden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine vorhandene E-Mail-Adresse für den Empfang von E-Mail-Benachrichtigungen von Amazon SNS .
- Ein vorhandener HTTP-Endpunkt, der von Ticketing-Tools, SIEM-Software oder anderen Sicherheitslösungen von Drittanbietern verwendet wird.

- Aktive AWS-Konten, die kontoübergreifende Workloads hosten, einschließlich eines zentralen Audit-Kontos.
- Security Hub, aktiviert und konfiguriert. Sie können dieses Muster ohne Security Hub verwenden, wir empfehlen jedoch, Security Hub aufgrund der generierten Erkenntnisse zu verwenden. Weitere Informationen finden Sie unter Einrichten von Security Hub in der AWS Security Hub-Dokumentation.
- Auf jeder EC2-Instance, die Sie scannen möchten, muss ein Amazon Inspector-Agent installiert sein. Sie können den Amazon Inspector-Agenten auf mehreren EC2-Instances installieren, indem Sie AWS Systems Manager Run Command verwenden.

Fähigkeiten

- Erfahrung mit - `self-managed` und -`service-managed`Berechtigungen für Stack-Sets in AWS CloudFormation. Wenn Sie `self-managed` Berechtigungen zum Bereitstellen von Stack-Instances für bestimmte Konten in bestimmten Regionen verwenden möchten, müssen Sie die erforderlichen AWS Identity and Access Management (IAM)-Rollen erstellen. Wenn Sie `service-managed` Berechtigungen zum Bereitstellen von Stack-Instances für Konten verwenden möchten, die von AWS Organizations in bestimmten Regionen verwaltet werden, müssen Sie die erforderlichen IAM-Rollen nicht erstellen. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets in der AWS- CloudFormation Dokumentation.

Einschränkungen

- Wenn keine Tags auf EC2-Instances in einem Konto angewendet werden, scannt Amazon Inspector alle EC2-Instances in diesem Konto.
- Die AWS- CloudFormation Stack-Sets und die onboard-audit-account.yaml-Datei (angefügt) müssen in derselben Region bereitgestellt werden.
- Standardmäßig unterstützt Amazon Inspector Classic keine aggregierten Ergebnisse. Security Hub ist die empfohlene Lösung, um Bewertungen für mehrere Konten oder AWS-Regionen anzuzeigen.
- Der Ansatz dieses Musters kann unter das Veröffentlichungskontingent von 30 000 Transaktionen pro Sekunde (TPS) für ein SNS-Thema in der Region USA Ost (Nord-Virginia) (us-east-1) skaliert werden, obwohl die Grenzwerte je nach Region variieren. Um effektiver zu skalieren und Datenverlust zu vermeiden, empfehlen wir, Amazon Simple Queue Service (Amazon SQS) vor dem SNS-Thema zu verwenden.

Architektur

Das folgende Diagramm veranschaulicht den Workflow zum automatischen Scannen von EC2-Instances.

Der Workflow besteht aus folgenden Schritten:

1. Eine Amazon- EventBridge Regel verwendet einen Cron-Ausdruck, um sich nach einem bestimmten Zeitplan selbst zu initiieren und Amazon Inspector zu initiieren.

2. Amazon Inspector scannt die markierten EC2-Instances im Konto.

3. Amazon Inspector sendet die Ergebnisse an Security Hub, der Erkenntnisse für Workflow, Priorisierung und Abhilfe generiert.

4. Amazon Inspector sendet den Status der Bewertung auch an ein SNS-Thema im Auditkonto. Eine AWS Lambda-Funktion wird aufgerufen, wenn ein `findings reported` Ereignis im SNS-Thema veröffentlicht wird.

5. Die Lambda-Funktion ruft die Ergebnisse ab, formatiert sie und sendet sie an ein anderes SNS-Thema im Auditkonto.

6. Die Ergebnisse werden an die E-Mail-Adressen gesendet, die das SNS-Thema abonniert haben. Die vollständigen Details und Empfehlungen werden im JSON-Format an den abonnierten HTTP-Endpunkt gesendet.

Technologie-Stack

- AWS Control Tower
- EventBridge
- IAM
- Amazon Inspector
- Lambda
- Security Hub
- Amazon SNS

Tools

- AWS CloudFormation – AWS CloudFormation hilft Ihnen bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen müssen und sich mehr auf Ihre Anwendungen konzentrieren können.
- AWS CloudFormation StackSets – AWS CloudFormation StackSets erweitert die Funktionalität von Stacks, indem es Ihnen ermöglicht, Stacks in mehreren Konten und Regionen mit einer einzigen Operation zu erstellen, zu aktualisieren oder zu löschen.
- AWS Control Tower – AWS Control Tower erstellt eine Abstraktions- oder Orchestrierungsebene, die die Funktionen mehrerer anderer AWS-Services kombiniert und integriert, einschließlich AWS Organizations .
- Amazon EventBridge – EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen einfach mit Daten aus einer Vielzahl von Quellen verbinden können.
- AWS Lambda – Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen.
- AWS Security Hub – Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten bereitstellt.

Polen

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CloudFormation Vorlage im Auditkonto bereit.	Laden Sie die `onboard-audit-account.yaml` Datei (angefügt) herunter und speichern Sie sie in einem lokalen Pfad auf Ihrem Computer. Melden Sie sich bei der AWS-Managementkonsole für Ihr	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Audit-Konto an, öffnen Sie die AWS- CloudFormation Konsole und wählen Sie dann Stack erstellen aus. Wählen Sie im Abschnitt Voraussetzungen die Option Vorlage vorbereiten und dann Vorlage ist bereit aus. Wählen Sie im Abschnitt Vorlage angeben die Option Vorlagenquelle und dann Vorlage ist bereit aus. Laden Sie die `onboard-audit-account.yaml` Datei hoch und konfigurieren Sie dann die verbleibenden Optionen entsprechend Ihren Anforderungen. Wichtig: Stellen Sie sicher, dass Sie die folgenden Eingabeparameter konfigurieren: • `DestinationEmailAddress` – Geben Sie eine E-Mail-Adresse ein, um Ergebnisse zu erhalten. • `HTTPEndpoint` – Stellen Sie einen HTTP-Endpunkt für Ihr Ticketing oder Ihre SIEM-Tools bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können die AWS-CloudFormation Vorlage auch mithilfe der AWS Command Line Interface (AWS CLI) bereitstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Stacks in der AWS- CloudFormation Dokumentation.	
Bestätigen Sie das Amazon SNS-Abonnement.	Öffnen Sie Ihren E-Mail-Posteingang und wählen Sie in der E-Mail, die Sie von Amazon SNS erhalten, Abonnement bestätigen aus. Amazon SNS Dadurch wird ein Webbrowser-Fenster geöffnet und die Abonnementbestätigung wird angezeigt.	Entwickler, Sicherheitsingenieur

Erstellen von AWS- CloudFormation Stack-Sets zur Automatisierung des Amazon Inspector-Scan-Zeitplans

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Stack-Sets im Audit-Konto.	Laden Sie die `vulnerability-management-program.yaml` Datei (angefügt) in einen lokalen Pfad auf Ihrem Computer herunter. Wählen Sie in der AWS-CloudFormation Konsole Stacksets anzeigen und	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann Erstellen StackSet aus. ChooseTemplate ist bereit, wählen Sie Vorlagendatei hochladen und laden Sie dann die `vulnerability-management-program.yaml` Datei hoch. Wenn Sie `self-managed` Berechtigungen verwenden möchten, folgen Sie den Anweisungen unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen in der AWS-CloudFormation Dokumentation. Dadurch werden Stack-Sets in einzelnen Konten erstellt. Wenn Sie `service-managed` Berechtigungen verwenden möchten, folgen Sie den Anweisungen unter Erstellen eines Stack-Sets mit serviceverwalteten Berechtigungen in der AWS- CloudFormation Dokumentation. Dadurch werden Stack-Sets in Ihrer gesamten Organisation oder bestimmten Organisationseinheiten (OUs) erstellt. Wichtig: Stellen Sie sicher, dass die folgenden Eingabepa	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rameter für Ihre Stack-Sets konfiguriert sind: • `AssessmentSchedule` – Der Zeitplan für die EventBridge Verwendung von Cron-Ausdrücken. • `Duration` – Die Dauer des Amazon Inspector-Bewertungslaufs in Sekunden. • `CentralSNSTopicArn` – Der Amazon-Ressourcenname (ARN) für das zentrale SNS-Thema. • `Tagkey` – Der Tag-Schlüssel, der der Ressourcengruppe zugeordnet ist. • `Tagvalue` – Der Tag-Wert, der der Ressourcengruppe zugeordnet ist. Wenn Sie EC2-Instances im Audit-Konto scannen möchten, müssen Sie die `vulnerability-management-program.yaml` Datei als AWS- CloudFormation Stack im Audit-Konto ausführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Lösung.	Überprüfen Sie, ob Sie Ergebnisse per E-Mail oder HTTP-Endpunkt nach dem Zeitplan erhalten, den Sie für Amazon Inspector angegeben haben.	Entwickler, Sicherheitsingenieur

Zugehörige Ressourcen

- Skalieren Sie Ihre Schwachstellentests mit Amazon Inspector
- Automatische Behebung von Amazon Inspector-Sicherheitsergebnissen
- So vereinfachen Sie die Einrichtung der Sicherheitsbewertung mithilfe von Amazon EC2, AWS Systems Manager und Amazon Inspector

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Reaktivieren CloudTrail von AWS mithilfe einer benutzerdefinierten Behebungsregel in AWS Config

Erstellt von Manigandan Shri (AWS)

Umgebung: Produktion	Technologien: Infrastruktur; Betrieb; Sicherheit, Identität, Compliance	AWS-Services: Amazon S3; AWS Config; AWS KMS; AWS Identity and Access Management; AWS Systems Manager; AWS CloudTrail

Übersicht

Der Überblick über die Aktivitäten in Ihrem Amazon Web Services (AWS) -Konto ist eine wichtige bewährte Methode für Sicherheit und Betrieb. AWS CloudTrail unterstützt Sie bei der Verwaltung, Einhaltung von Vorschriften sowie bei der Betriebs- und Risikoprüfung Ihres Kontos.

Um sicherzustellen, dass dies in Ihrem Konto aktiviert CloudTrail bleibt, stellt AWS Config die `cloudtrail-enabled` verwaltete Regel bereit. Wenn sie deaktiviert CloudTrail ist, aktiviert die `cloudtrail-enabled` Regel sie mithilfe der automatischen Problembehebung automatisch wieder.

Sie müssen jedoch sicherstellen, dass Sie die bewährten Sicherheitsmethoden für den Fall befolgen, dass CloudTrail Sie die automatische Problembehebung verwenden. Zu diesen bewährten Methoden gehören die Aktivierung CloudTrail in allen AWS-Regionen, das Protokollieren von Lese- und Schreib-Workloads, das Aktivieren von Erkenntnissen und das Verschlüsseln von Protokolldateien mit serverseitiger Verschlüsselung mithilfe von verwalteten Schlüsseln (SSE-KMS) von AWS Key Management Service (AWS KMS).

Dieses Muster hilft Ihnen dabei, diese bewährten Sicherheitsmethoden zu befolgen, indem es eine benutzerdefinierte Abhilfemaßnahme bereitstellt, die in Ihrem Konto automatisch wieder aktiviert wird. CloudTrail

Wichtig: Wir empfehlen die Verwendung von Service Control Policies (SCPs), um jegliche Manipulation zu verhindern. CloudTrail Weitere Informationen dazu finden Sie im AWS-Sicherheitsblog im CloudTrail Abschnitt Verhinderung von Manipulationen mit AWS Organizations, um Sicherheit in großem Umfang zu vereinfachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Berechtigungen zum Erstellen eines AWS Systems Manager Automation Automation-Runbooks
- Ein vorhandener Trail für Ihr Konto

Einschränkungen

Dieses Muster unterstützt die folgenden Aktionen nicht:

- Einen Amazon Simple Storage Service (Amazon S3) -Präfixschlüssel für den Speicherort einrichten
- In einem Amazon Simple Notification Service (Amazon SNS) -Thema veröffentlichen
- Konfiguration von Amazon CloudWatch Logs zur Überwachung Ihrer CloudTrail Logs

Architektur

Technologie-Stack

- AWS Config
- CloudTrail
- Systems Manager
- Systems Manager Automation

Tools

- AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem Konto.
- AWS CloudTrail unterstützt Sie dabei, die Unternehmensführung, die Einhaltung von Vorschriften sowie die Betriebs- und Risikoprüfung Ihres Kontos zu ermöglichen.
- AWS Key Management Service (AWS KMS) ist ein Verschlüsselungs- und Schlüsselverwaltungsservice.
- Mit AWS Systems Manager können Sie Ihre Infrastruktur auf AWS anzeigen und steuern.

- AWS Systems Manager Automation vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von Amazon Elastic Compute Cloud (Amazon EC2) -Instances und anderen AWS-Ressourcen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Die Datei cloudtrail-remediation-action.yml (angehängt) hilft Ihnen dabei, ein Systems Manager Automation-Runbook zu erstellen, das Sie mithilfe von bewährten Sicherheitsmethoden einrichten und erneut aktivieren können. CloudTrail

Epen

Konfiguriere CloudTrail

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie dann einen S3-Bucket zum Speichern der CloudTrai l Protokolle. Weitere Informati onen finden Sie unter Erstellen eines S3-Buckets in der Amazon S3 S3-Dokume ntation.	Systemadministrator
Fügen Sie eine Bucket-Ri chtlinie hinzu, um CloudTrail die Übermittlung von Protokoll dateien an den S3-Bucket zu ermöglichen.	CloudTrail muss über die erforderlichen Berechtigungen verfügen, um Protokolldateien an Ihren S3-Bucket zu liefern. Wählen Sie in der Amazon S3 S3-Konsole den S3-Bucket aus, den Sie zuvor erstellt	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	haben, und wählen Sie dann Permissions aus. Erstellen Sie eine S3-Bucket-Richtlinie, indem Sie die Amazon S3 S3-Bucket-Richtlinie für CloudTrail aus der CloudTrail Dokumentation verwenden. Schritte zum Hinzufügen einer Richtlinie zu einem S3-Bucket finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole in der Amazon S3 S3-Dokumentation. Wichtig: Wenn Sie bei der Erstellung Ihres Trails in ein Präfix angegeben haben CloudTrail, stellen Sie sicher, dass Sie es in die S3-Bucket-Richtlinie aufnehmen. Das Präfix ist eine optionale Ergänzung zum S3-Objektschlüssel, die eine ordnerähnliche Organisation in Ihrem S3-Bucket erstellt. Weitere Informationen dazu finden Sie in der Dokumentation unter Creating a trail. CloudTrail	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines KMS-Schlüssels.	Erstellen Sie einen AWS-KMS-Schlüssel CloudTrail zum Verschlüsseln von Objekten, bevor Sie sie dem S3-Bucket hinzufügen. Hilfe zu dieser Geschichte finden Sie in der Dokumentation unter Verschlüsseln von CloudTrail Protokolldateien mit verwalteten AWS-KMS-Schlüsseln (SSE-KMS). CloudTrail	Systemadministrator
Fügen Sie dem KMS-Schlüssel eine Schlüsselrichtlinie hinzu.	Fügen Sie eine KMS-Schlüsselrichtlinie hinzu, um die Verwendung des KMS-Schlüssels CloudTrail zu ermöglichen. Hilfe zu dieser Geschichte finden Sie in der Dokumentation unter Verschlüsseln von CloudTrail Protokolldateien mit von AWS KMS verwalteten Schlüsseln (SSE-KMS). CloudTrail Wichtig: Erfordert keine Berechtigungen. CloudTrail `Decrypt`	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
AssumeRole Runbook für Systems Manager erstellen	Erstellen Sie ein `AssumeRole` für Systems Manager Automation, um das Runbook auszuführen. Anweisungen und weitere Informationen dazu finden Sie unter Automatisierung einrichten in der Systems Manager Manager-Dokumentation.	Systemadministrator

Das Systems Manager Automation-Runbook erstellen und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Systems Manager Automation-Runbook.	Verwenden Sie die `cloudtrail-remediation-action.yml` Datei (angehängt), um das Systems Manager Automation-Runbook zu erstellen. Weitere Informationen dazu finden Sie unter Systems Manager Manager-Dokumente erstellen in der Systems Manager Manager-Dokumentation.	Systemadministrator
Testen Sie das Runbook.	Testen Sie auf der Systems Manager-Konsole das Systems Manager Automation-Runbook, das Sie zuvor erstellt haben. Weitere Informationen dazu finden Sie in der Systems Manager Manager-Dokumentation unter	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausführen einer einfachen Automatisierung.	

Richten Sie die automatische Behebungsregel in AWS Config ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die CloudTrail -aktivierte Regel hinzu.	Wählen Sie in der AWS Config-Konsole Regeln und dann Regel hinzufügen aus. Klicken Sie auf der Seite Add Rule (Regel hinzufügen) auf Add Custom Rule (Benutzer definierte Regel hinzufüge n). Geben Sie auf der Seite „Regel konfigurieren“ einen Namen und eine Beschreib ung ein und fügen Sie die `cloudtrail-enabled` Regel hinzu. Weitere Informationen finden Sie unter Verwaltung Ihrer AWS Config-Regeln in der AWS Config-Do kumentation.	Systemadministrator
Fügen Sie die automatische Behebungsaktion hinzu.	Wählen Sie in der Dropdown-Liste Aktionen die Option Behebung verwalten aus. Wählen Sie Automatische Korrektur und dann das Systems Manager Manager-Runbook aus, das Sie zuvor erstellt haben.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die folgenden Eingabepa rameter sind erforderlich für: CloudTrail • `CloudTrailName` • `CloudTrailS3Bucket Name` • `CloudTrailKmsKeyId` • `AssumeRole` (optional) Die folgenden Eingabepa rameter sind standardmäßig auf true gesetzt: • `IsMultiRegionTrail` • `IsOrganizationTrail` • `IncludeGlobalServi ceEvents` • `EnableLogFileValid ation` Behalten Sie die Standardw erte für die Parameter Rate Limits und Resource ID bei. Wählen Sie Speichern. Weitere Informationen finden Sie unter Behebung nicht konformer AWS-Ressourcen mit AWS Config-Regeln in der AWS Config-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die automatische Behebungsregel.	Um die automatische Behebungsregel zu testen, öffnen Sie die CloudTrail Konsole, wählen Sie Trails und dann den Trail aus. Wählen Sie Protokollierung beenden, um die Protokoll ierung für den Trail zu deaktivieren. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Protokoll ierung beenden. CloudTrail beendet die Protokollierung der Aktivitäten für diesen Trail. Folgen Sie den Anweisung en unter Evaluieren Ihrer Ressourcen in der AWS Config-Dokumentation, um sicherzustellen, dass diese automatisch wieder aktiviert CloudTrail wurden.	Systemadministrator

Zugehörige Ressourcen

Konfigurieren CloudTrail

- Erstellen Sie einen S3-Bucket
- Amazon S3 S3-Bucket-Richtlinie für CloudTrail
- Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole
- Einen Trail erstellen
- Automatisierung einrichten
- Verschlüsselung von CloudTrail Protokolldateien mit verwalteten AWS KMS KMS-Schlüsseln (SSE-KMS)

Das Systems Manager Automation-Runbook erstellen und testen

- Systems Manager Manager-Dokumente erstellen
- Ausführen einer einfachen Automatisierung

Richten Sie die automatische Behebungsregel in AWS Config ein

- Verwaltung Ihrer AWS Config-Regeln
- Behebung nicht konformer AWS-Ressourcen mit AWS Config-Regeln

Weitere Ressourcen

- AWS CloudTrail — Bewährte Sicherheitsmethoden
- Erste Schritte mit AWS Systems Manager
- Erste Schritte mit AWS Config
- Erste Schritte mit AWS CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatische Behebung unverschlüsselter Amazon RDS-DB-Instances und -Cluster

Erstellt von Ajay R Bolt (AWS) und Josh Joy (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Datenbanken	AWS-Services: AWS Config; AWS KMS; AWS Identity and Access Management ;AWS Systems Manager; Amazon RDS

Übersicht

Dieses Muster beschreibt, wie unverschlüsselte Amazon Relational Database Service (Amazon RDS)-DB-Instances und -Cluster in Amazon Web Services (AWS) mithilfe von AWS Config-, AWS Systems Manager-Runbooks und AWS Key Management Service (AWS KMS)-Schlüsseln automatisch korrigiert werden.

Verschlüsselte RDS-DB-Instances bieten eine zusätzliche Datenschutzebene, indem Sie Ihre Daten vor unbefugtem Zugriff auf den zugrunde liegenden Speicher sichern. Sie können die Amazon RDS-Verschlüsselung verwenden, um den Datenschutz Ihrer in der AWS Cloud bereitgestellten Anwendungen zu erhöhen und die Compliance-Anforderungen für die Verschlüsselung im Ruhezustand zu erfüllen. Sie können die Verschlüsselung für eine RDS-DB-Instance aktivieren, wenn Sie sie erstellen, aber nicht nachdem sie erstellt wurde. Sie können jedoch einer unverschlüsselten RDS-DB-Instance Verschlüsselung hinzufügen, indem Sie einen Snapshot Ihrer DB-Instance erstellen und dann eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie eine DB-Instance aus dem verschlüsselten Snapshot wiederherstellen, um eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance zu erhalten.

Dieses Muster verwendet AWS Config-Regeln, um RDS-DB-Instances und -Cluster auszuwerten. Es wendet die Korrektur mithilfe von AWS Systems Manager-Runbooks an, die die Aktionen definieren, die auf nicht konformen Amazon RDS-Ressourcen ausgeführt werden sollen, und AWS KMS-Schlüsseln zum Verschlüsseln der DB-Snapshots. Anschließend werden Service-Kontrollrichtlinien (SCPs) durchgesetzt, um die Erstellung neuer DB-Instances und Cluster ohne Verschlüsselung zu verhindern.

Der Code für dieses Muster wird in bereitgestelltGitHub.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Dateien aus dem GitHub Quellcode-Repository für dieses Muster, das auf Ihren Computer heruntergeladen wurde
- Eine unverschlüsselte RDS-DB-Instance oder ein unverschlüsselter RDS-DB-Cluster
- Ein vorhandener AWS KMS-Schlüssel zum Verschlüsseln von RDS-DB-Instances und -Clustern
- Zugriff auf die Aktualisierung der KMS-Schlüsselressourcenrichtlinie
- AWS Config in Ihrem AWS-Konto aktiviert (siehe Erste Schritte mit AWS Config in der AWS-Dokumentation)

Einschränkungen

- Sie können die Verschlüsselung für eine RDS-DB-Instance nur aktivieren, wenn Sie sie erstellen, nicht nachdem sie erstellt wurde.
- Es ist nicht möglich, ein verschlüsseltes Lesereplikat einer unverschlüsselten DB-Instance oder ein unverschlüsseltes Lesereplikat einer verschlüsselten DB-Instance zu erstellen.
- Sie können ein unverschlüsseltes Backup oder einen solchen Snapshot nicht als verschlüsselte DB-Instance wiederherstellen.
- Amazon RDS-Verschlüsselung ist für die meisten DB-Instance-Klassen verfügbar. Eine Liste der Ausnahmen finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen in der Amazon-RDS-Dokumentation.
- Um einen verschlüsselten Snapshot von einer AWS-Region in eine andere zu kopieren, müssen Sie den KMS-Schlüssel in der AWS-Zielregion angeben. Dies liegt daran, dass KMS-Schlüssel spezifisch für die AWS-Region sind, in der sie erstellt werden.
- Der Quell-Snapshot bleibt den gesamten Kopiervorgang über verschlüsselt. Amazon RDS verwendet Envelope-Verschlüsselung, um Daten während des Kopiervorgangs zu schützen. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS KMS-Dokumentation.

- Sie können eine verschlüsselte DB-Instance nicht entschlüsseln. Sie können jedoch Daten aus einer verschlüsselten DB-Instance exportieren und die Daten in eine unverschlüsselte DB-Instance importieren.
- Sie sollten einen KMS-Schlüssel nur löschen, wenn Sie sicher sind, dass Sie ihn nicht mehr verwenden müssen. Wenn Sie sich nicht sicher sind, sollten Sie den KMS-Schlüssel deaktivieren, anstatt ihn zu löschen. Sie können einen deaktivierten KMS-Schlüssel erneut aktivieren, wenn Sie ihn später erneut verwenden müssen, aber Sie können einen gelöschten KMS-Schlüssel nicht wiederherstellen.
- Wenn Sie sich nicht dafür entscheiden, automatisierte Backups beizubehalten, werden Ihre automatisierten Backups gelöscht, die sich in derselben AWS-Region wie die DB-Instance befinden. Sie können nicht wiederhergestellt werden, nachdem Sie die DB-Instance gelöscht haben.
- Ihre automatisierten Backups werden für den Aufbewahrungszeitraum aufbewahrt, der zum Zeitpunkt des Löschens auf der DB-Instance festgelegt wurde. Dieser festgelegte Aufbewahrungszeitraum tritt unabhängig davon ein, ob Sie einen endgültigen DB-Snapshot erstellen möchten oder nicht.
- Wenn die automatische Behebung aktiviert ist, verschlüsselt diese Lösung alle Datenbanken, die denselben KMS-Schlüssel haben.

Architektur

Das folgende Diagramm veranschaulicht die Architektur für die AWS- CloudFormation Implementierung. Beachten Sie, dass Sie dieses Muster auch mithilfe des AWS Cloud Development Kit (AWS CDK) implementieren können.

Tools

Tools

- AWS CloudFormation unterstützt Sie bei der automatischen Einrichtung Ihrer AWS-Ressourcen. Damit können Sie eine Vorlagendatei verwenden, um eine Sammlung von Ressourcen als einzelne Einheit (einen Stack) zu erstellen und zu löschen.
- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework zur Definition Ihrer Cloud-Infrastruktur im Code und zur Bereitstellung mithilfe vertrauter Programmiersprachen.

AWS-Services und -Funktionen

- AWS Config verfolgt die Konfiguration Ihrer AWS-Ressourcen und deren Beziehungen zu Ihren anderen Ressourcen. Es kann diese AWS-Ressourcen auch auf Compliance überprüfen. Dieser Service verwendet Regeln, die so konfiguriert werden können, dass AWS-Ressourcen anhand der gewünschten Konfigurationen bewertet werden. Sie können eine Reihe von verwalteten AWS Config-Regeln für gängige Compliance-Szenarien verwenden oder eigene Regeln für benutzerdefinierte Szenarien erstellen. Wenn festgestellt wird, dass eine AWS-Ressource nicht konform ist, können Sie eine Abhilfemaßnahme über ein AWS Systems Manager-Runbook angeben und optional eine Warnung über ein Amazon Simple Notification Service (Amazon SNS)-Thema senden. Mit anderen Worten, Sie können Korrekturmaßnahmen AWS Config-Regeln zuordnen und sie automatisch ausführen, um nicht konforme Ressourcen ohne manuellen Eingriff zu beheben. Wenn eine Ressource nach der automatischen Korrektur immer noch nicht konform ist, können Sie die Regel so festlegen, dass die automatische Korrektur erneut versucht wird.
- Amazon Relational Database Service (Amazon RDS) erleichtert das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud. Der Grundbaustein für Amazon RDS ist die DB-Instance, eine isolierte Datenbankumgebung in der AWS Cloud. Amazon RDS bietet eine Auswahl von Instance-Typen, die für verschiedene Anwendungsfälle für relationale Datenbanken optimiert sind. Instance-Typen umfassen verschiedene Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazitäten und bieten Ihnen die Flexibilität, die richtige Mischung von Ressourcen für Ihre Datenbank auszuwählen. Jeder Instance-Typ umfasst mehrere Instance-Größen, sodass Sie Ihre Datenbank an die Anforderungen Ihrer Ziel-Workload anpassen können.
- AWS Key Management Service (AWS KMS) ist ein verwalteter Service, der es Ihnen erleichtert, AWS KMS-Schlüssel zu erstellen und zu steuern, die Ihre Daten verschlüsseln. Ein KMS-Schlüssel ist eine logische Darstellung eines Root-Schlüssels. Der KMS-Schlüssel enthält Metadaten wie die Schlüssel-ID, das Erstellungsdatum, die Beschreibung und den Schlüsselstatus.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- Service-Kontrollrichtlinien (SCPs)bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation. SCPs helfen Ihnen sicherzustellen, dass Ihre Konten die Zugriffskontrollrichtlinien Ihrer Organisation einhalten. SCPs haben keine Auswirkungen auf Benutzer oder Rollen im Verwaltungskonto. Sie wirken sich nur auf die Mitgliedskonten Ihrer Organisation aus. Wir raten Ihnen nachdrücklich davon ab, Service-Kontrollrichtlinien zum Root-Benutzer Ihrer Organisation zuzuordnen, ohne zuvor gründlich getestet zu haben, wie sich die Richtlinie auf Konten auswirkt. Erstellen Sie stattdessen eine Organisationseinheit (OU), in die

Sie Ihre Konten nacheinander oder zumindest in kleinen Nummern verschieben können, um sicherzustellen, dass Sie Benutzer nicht versehentlich von Schlüsselservices sperren.

Code

Der Quellcode und die Vorlagen für dieses Muster sind in einem GitHub Repository verfügbar. Das Muster bietet zwei Implementierungsoptionen: Sie können eine AWS- CloudFormation Vorlage bereitstellen, um die Korrekturrolle zu erstellen, die RDS-DB-Instances und -Cluster verschlüsselt, oder das AWS-CDK verwenden. Das Repository verfügt über separate Ordner für diese beiden Optionen.

Der Abschnitt „PiCs“ enthält step-by-step Anweisungen zur Bereitstellung der CloudFormation Vorlage. Wenn Sie das AWS-CDK verwenden möchten, folgen Sie den Anweisungen in der Datei README.md im GitHub Repository.

Bewährte Methoden

- Aktivieren Sie die Datenverschlüsselung sowohl im Ruhezustand als auch während der Übertragung.
- Aktivieren Sie AWS Config in allen Konten und AWS-Regionen.
- Aufzeichnen von Konfigurationsänderungen an allen Ressourcentypen.
- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.
- Nutzen Sie das Tagging für AWS Config , was das Verwalten, Suchen und Filtern von Ressourcen vereinfacht.

Polen

Erstellen der IAM-Korrekturrolle und des AWS Systems Manager-Runbooks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie die `unencrypted-to-encrypted-rds.template.json` Datei aus dem GitHub Repository herunter.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CloudFormation Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Starten Sie die `unencrypted-to-encrypted-rds.template.json` Vorlage, um einen neuen Stack zu erstellen. Weitere Informationen zum Bereitstellen von Vorlagen finden Sie in der AWS-CloudFormation Dokumentation.	DevOps Techniker
Überprüfen Sie CloudFormation Parameter und Werte.	1. Überprüfen Sie die Stack-Details und aktualisieren Sie die Werte basierend auf Ihren Umgebungsanforderungen. 2. Wählen Sie Stack erstellen, um die Vorlage bereitzustellen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ressourcen.	Wenn der Stack erstellt wurde, ändert sich sein Status in CREATE_COMPLETE . Überprüfen Sie die erstellten Ressourcen (IAM-Rolle, AWS Systems Manager-Runbook) in der - CloudFormation Konsole.	DevOps Techniker

Aktualisieren der AWS KMS-Schlüsselrichtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Ihre KMS-Schlüsselrichtlinie.	1. Stellen Sie sicher, dass der Schlüsselalias `alias/RDSEncryptionAtRestKMSAlias` vorhanden ist. 2. Die Schlüsselrichtlinienanweisung sollte die IAM-Korrekturrolle enthalten . (Überprüfen Sie die Ressourcen, die von der CloudFormation Vorlage erstellt wurden, die Sie im vorherigen Epic bereitgestellt haben.) 3. Aktualisieren Sie in der folgenden Schlüsselrichtlinie die fett gedruckten Teile so, dass sie Ihrem Konto und der erstellten IAM-Rolle entsprechen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	{
	"Sid": "Allow access through RDS for all principals in the account that are authorized to use RDS",
	"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam:: <your-AWS-account-ID>”:role/<your-IAM-remediation-role>"
	},
	"Action": [
	"kms:Encrypt",
	"kms:Decrypt",
	"kms:ReEncrypt*",
	"kms:GenerateDataKey*",
	"kms:CreateGrant",
	"kms:ListGrants",
	"kms:DescribeKey"
	],
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"kms:ViaService": "rds.us-east-1.amazonaws.com",
	"kms:CallerAccount": "<your-AWS-account-ID>"
	}
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`}`	

Suchen und Beheben von nicht konformen Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Anzeigen nicht konformer Ressourcen.	1. Um eine Liste der nicht konformen Ressourcen anzuzeigen, öffnen Sie die AWS Config-Konsole unter https://console.aws.amazon.com/config/. 2. Wählen Sie im Navigationsbereich Regeln und dann die `rds-storage-encrypted` Regel aus. Bei den in der AWS Config-Konsole aufgeführten nicht konformen Ressourcen handelt es sich um Instances, nicht um Cluster. Die Korrekturautomatisierung verschlüsselt Instances und Cluster und erstellt entweder eine neu verschlüsselte Instance oder einen neu erstellten Cluster. Achten Sie jedoch darauf, nicht mehrere Instances gleichzeitig zu beheben, die zu demselben Cluster gehören. Bevor Sie RDS-DB-Instances oder -Volumes korrigier	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en, stellen Sie sicher, dass die RDS-DB-Instance nicht verwendet wird. Vergewissern Sie sich, dass während der Snapshot-Erstellung keine Schreibvorgänge ausgeführt werden, um sicherzustellen, dass der Snapshot die Originaldaten enthält. Erwägen Sie, ein Wartungsfenster durchzusetzen, in dem die Korrektur ausgeführt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie nicht konforme Ressourcen.	1. Wenn Sie bereit sind und das Wartungsfenster in Kraft ist, wählen Sie die zu behebende Ressource und dann Korrigieren aus. In der Spalte Aktionsstatus sollte jetzt die Aktionsausführung in der Warteschlange angezeigt werden. 2. Zeigen Sie den Fortschritt und den Status der Behebung in Systems Manager an. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/. Wählen Sie im Navigationsbereich Automation und dann die Ausführungs-ID der entsprechenden Automatisierung aus, um weitere Details anzuzeigen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die RDS-DB-Instance verfügbar ist.	Nach Abschluss der Automatisierung wird die neu verschlüsselte RDS-DB-Instance verfügbar. Die verschlüsselte RDS-DB-Instance hat das Präfix `encrypted` gefolgt vom ursprünglichen Namen. Wenn der unverschlüsselte Name der RDS-DB-Instance beispielsweise lautet`database-1` , wäre die neu verschlüsselte RDS-DB-Instance `encrypted-database-1` .	DevOps Techniker
Beenden Sie die unverschlüsselte Instance.	Nachdem die Korrektur abgeschlossen und die neu verschlüsselte Ressource validiert wurde, können Sie die unverschlüsselte Instance beenden. Stellen Sie sicher, dass die neu verschlüsselte Ressource mit der unverschlüsselten Ressource übereinstimmt, bevor Sie Ressourcen beenden.	DevOps Techniker

SCPs erzwingen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
SCPs erzwingen.	Erzwingen Sie SCPs, um zu verhindern, dass DB-Instances und Cluster in Zukunft	Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ohne Verschlüsselung erstellt werden. Verwenden Sie zu diesem Zweck die im GitHub Repository bereitgestellte `rds_encrypted.json` Datei und folgen Sie den Anweisungen in der AWS-Dokumentation.	

Zugehörige Ressourcen

Referenzen

- Einrichten von AWS Config
- Benutzerdefinierte AWS Config-Regeln
- AWS KMS-Konzepte
- AWS Systems Manager-Dokumente
- Service-Kontrollrichtlinien

Tools

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK)

Anleitungen und Muster

- Automatisches erneutes Aktivieren CloudTrail von AWS mithilfe einer benutzerdefinierten Korrekturregel in AWS Config

Zusätzliche Informationen

HÄUFIG GESTELLTE FRAGEN

F: Wie funktioniert AWS Config?

A. Wenn Sie AWS Config aktivieren, erkennt es zunächst die unterstützten AWS-Ressourcen, die in Ihrem Konto vorhanden sind, und generiert ein Konfigurationselement für jede Ressource. AWS Config generiert auch Konfigurationselemente, wenn sich die Konfiguration einer Ressource ändert, und speichert historische Aufzeichnungen der Konfigurationselemente Ihrer Ressourcen ab dem Zeitpunkt, an dem Sie den Konfigurations-Recorder starten. Standardmäßig erstellt AWS Config Konfigurationselemente für jede unterstützte Ressource in der AWS-Region. Wenn Sie nicht möchten, dass AWS Config Konfigurationselemente für alle unterstützten Ressourcen erstellt, können Sie die Ressourcentypen angeben, die verfolgt werden sollen.

F: Wie beziehen sich AWS Config- und AWS Config-Regeln auf AWS Security Hub?

A. AWS Security Hub ist ein Sicherheits- und Compliance-Service, der als Service Sicherheits- und Compliance-Statusmanagement bietet. Es verwendet AWS Config- und AWS Config-Regeln als primären Mechanismus zur Bewertung der Konfiguration von AWS-Ressourcen. AWS Config-Regeln können auch verwendet werden, um die Ressourcenkonfiguration direkt auszuwerten. Konfigurationsregeln werden auch von anderen AWS-Services wie AWS Control Tower und AWS Firewall Manager verwendet.

Automatisches Rotieren von IAM-Benutzerzugriffsschlüsseln in großem Umfang mit AWS Organizations und AWS Secrets Manager

Erstellt von Tracy Hickey (AWS), Gaurav Verma (AWS), Laura Seletos (AWS), Bol Davie (AWS) und Arvindpatel (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance	AWS-Services: AWS CloudFormation; Amazon CloudWatch Events; AWS Identity and Access Management ; AWS Lambda ; AWS Organizations ; Amazon S3; Amazon SES ; AWS Secrets Manager

Übersicht

Wichtig: Als bewährte Methode empfiehlt AWS, dass Sie AWS Identity and Access Management (IAM)-Rollen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen wie Zugriffsschlüsseln verwenden. Der in diesem Muster dokumentierte Ansatz ist nur für Legacy-Implementierungen gedacht, die langlebige AWS-API-Anmeldeinformationen erfordern. Für diese Implementierungen empfehlen wir Ihnen weiterhin, Optionen für die Verwendung kurzfristiger Anmeldeinformationen in Betracht zu ziehen, z. B. die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Profilen oder IAM Roles Anywhere . Der Ansatz in diesem Artikel gilt nur für Fälle, in denen Sie nicht sofort zu kurzfristigen Anmeldeinformationen wechseln können und langfristige Anmeldeinformationen nach einem Zeitplan rotiert werden müssen. Bei diesem Ansatz sind Sie dafür verantwortlich, Ihren Legacy-Anwendungscode oder Ihre Konfiguration regelmäßig zu aktualisieren, um die rotierten API-Anmeldeinformationen zu verwenden.

Zugriffsschlüssel sind langfristige Anmeldeinformationen für einen IAM-Benutzer. Durch regelmäßiges Rotieren Ihrer IAM-Anmeldeinformationen wird verhindert, dass ein kompromittierter

Satz von IAM-Zugriffsschlüsseln auf Komponenten in Ihrem AWS-Konto zugreift. Das Rotieren von IAM-Anmeldeinformationen ist auch ein wichtiger Bestandteil bewährter Sicherheitsmethoden in IAM .

Dieses Muster hilft Ihnen, IAM-Zugriffsschlüssel automatisch zu rotieren, indem Sie AWS-CloudFormation Vorlagen verwenden, die im GitHub IAM-Schlüsselrotations-Repository bereitgestellt werden.

Das Muster unterstützt die Bereitstellung in einem einzelnen Konto oder mehreren Konten. Wenn Sie AWS Organizations verwenden, identifiziert diese Lösung alle AWS-Konto-IDs in Ihrer Organisation und skaliert dynamisch, wenn Konten entfernt oder neue Konten erstellt werden. Die zentrale AWS Lambda-Funktion verwendet eine angenommene IAM-Rolle, um die Rotationsfunktionen lokal über mehrere von Ihnen ausgewählte Konten auszuführen.

- Neue IAM-Zugriffsschlüssel werden generiert, wenn vorhandene Zugriffsschlüssel 90 Tage alt sind.
- Die neuen Zugriffsschlüssel werden als Secret in AWS Secrets Manager gespeichert. Eine ressourcenbasierte Richtlinie erlaubt nur dem angegebenen IAM-Prinzipal, auf das Secret zuzugreifen und es abzurufen. Wenn Sie Schlüssel im Verwaltungskonto speichern möchten, werden die Schlüssel für alle Konten im Verwaltungskonto gespeichert.
- Die E-Mail-Adresse, die dem Eigentümer des AWS-Kontos zugewiesen ist, in dem die neuen Zugriffsschlüssel erstellt wurden, erhält eine Benachrichtigung.
- Die vorherigen Zugriffsschlüssel werden bei einem Alter von 100 Tagen deaktiviert und dann bei einem Alter von 110 Tagen gelöscht.
- Eine zentrale E-Mail-Benachrichtigung wird an den AWS-Kontoinhaber gesendet.

Lambda-Funktionen und Amazon führen diese Aktionen CloudWatch automatisch aus. Anschließend können Sie das neue Zugriffsschlüsselpaar abrufen und es in Ihrem Code oder Ihren Anwendungen ersetzen. Die Rotations-, Lösch- und Deaktivierungszeiträume können angepasst werden.

Voraussetzungen und Einschränkungen

- Mindestens ein aktives AWS-Konto.
- AWS Organizations , konfiguriert und eingerichtet (siehe Tutorial).
- Berechtigungen zum Abfragen von AWS Organizations von Ihrem Verwaltungskonto. Weitere Informationen finden Sie unter AWS Organizations und serviceverknüpfte Rollen in der AWS Organizations-Dokumentation.

- Ein IAM-Prinzipal, der über Berechtigungen zum Starten der AWS- CloudFormation Vorlage und der zugehörigen Ressourcen verfügt. Weitere Informationen finden Sie unter Selbstverwaltete Berechtigungen erteilen in der AWS- CloudFormation Dokumentation.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3)-Bucket zur Bereitstellung der Ressourcen.
- Amazon Simple Email Service (Amazon SES) wurde aus der Sandbox verschoben. Weitere Informationen finden Sie unter Verlassen der Amazon SES-Sandbox in der Amazon SESDokumentation.
- Wenn Sie Lambda in einer Virtual Private Cloud (VPC) ausführen möchten, sollten die folgenden Ressourcen erstellt werden, bevor Sie die CloudFormation Hauptvorlage ausführen:
  - Eine VPC.
  - ein Subnetz.
  - Endpunkte für Amazon SES , AWS Systems Manager , AWS Security Token Service (AWS STS), Amazon S3 und AWS Secrets Manager . (Sie können die Endpunktvorlage ausführen, die im GitHub IAM-Schlüsselrotations-Repository bereitgestellt wird, um diese Endpunkte zu erstellen.)
- Der Simple Mail Transfer Protocol (SMTP)-Benutzer und das Passwort, die in AWS Systems Manager-Parametern (SSM-Parametern) gespeichert sind. Parameter müssen mit den CloudFormation Hauptvorlagenparametern übereinstimmen.

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon EventBridge
- IAM
- AWS Lambda
- AWS Organizations
- Amazon S3

Architektur

Die folgenden Diagramme zeigen die Komponenten und Workflows für dieses Muster. Die Lösung unterstützt zwei Szenarien zum Speichern der Anmeldeinformationen: in einem Mitgliedskonto und im Verwaltungskonto.

Option 1: Speichern der Anmeldeinformationen in einem Mitgliedskonto

Option 2: Speichern der Anmeldeinformationen im Verwaltungskonto

Die Diagramme zeigen den folgenden Workflow:

1. Ein EventBridge Ereignis initiiert alle 24 Stunden eine `account_inventory`Lambda-Funktion.
2. Diese Lambda-Funktion fragt AWS Organizations nach einer Liste aller AWS-Konto-IDs , Kontonamen und Konto-E-Mails ab.
3. Die `account_inventory`Lambda-Funktion initiiert eine `access_key_auto_rotation` Lambda-Funktion für jede AWS-Konto-ID und übergibt die Metadaten zur zusätzlichen Verarbeitung an sie.
4. Die `access_key_auto_rotation` Lambda-Funktion verwendet eine angenommene IAM-Rolle, um auf die AWS-Konto-ID zuzugreifen. Das Lambda-Skript führt eine Prüfung aller Benutzer und ihrer IAM-Zugriffsschlüssel im Konto durch.
5. Wenn das Alter des IAM-Zugriffsschlüssels den Schwellenwert für bewährte Methoden nicht überschritten hat, ergreift die Lambda-Funktion keine weiteren Maßnahmen.
6. Wenn das Alter des IAM-Zugriffsschlüssels den Schwellenwert für bewährte Methoden überschritten hat, bestimmt die `access_key_auto_rotation` Lambda-Funktion, welche Rotationsaktion ausgeführt werden soll.
7. Wenn eine Aktion erforderlich ist, erstellt und aktualisiert die `access_key_auto_rotation` Lambda-Funktion ein Secret in AWS Secrets Manager, wenn ein neuer Schlüssel generiert wird. Es wird auch eine ressourcenbasierte Richtlinie erstellt, die nur dem angegebenen IAM-Prinzipal den Zugriff auf und das Abrufen des Secrets erlaubt. Bei Option 1 werden die Anmeldeinformationen in Secrets Manager im jeweiligen Konto gespeichert. Bei Option 2 (wenn das `StoreSecretsInCentralAccount` Flag auf True gesetzt ist) werden die Anmeldeinformationen im Secrets Manager im Verwaltungskonto gespeichert.
8. Eine `notifier` Lambda-Funktion wird initiiert, um den Besitzer des Kontos über die Rotationsaktivität zu informieren. Diese Funktion empfängt die AWS-Konto-ID, den Kontonamen, die Konto-E-Mail und die ausgeführten Rotationsaktionen.

9. Die `notifier` Lambda-Funktion fragt den Bereitstellungs-S3-Bucket nach einer E-Mail-Vorlage ab und aktualisiert sie dynamisch mit den relevanten Aktivitätsmetadaten. Die E-Mail wird dann an die E-Mail-Adresse des Kontoinhabers gesendet.

Hinweise:

- Diese Lösung unterstützt Ausfallsicherheit in mehreren Availability Zones. Es unterstützt jedoch keine Ausfallsicherheit in mehreren AWS-Regionen. Zur Unterstützung in mehreren Regionen können Sie die Lösung in der zweiten Region bereitstellen und die EventBridge Schlüsselrotationsregel deaktiviert lassen. Sie können die Regel dann aktivieren, wenn Sie die Lösung in der zweiten Region ausführen möchten.
- Sie können diese Lösung im Audit-Modus ausführen. Im Prüfungsmodus werden IAM-Zugriffsschlüssel nicht geändert, aber eine E-Mail wird gesendet, um Benutzer zu benachrichtigen. Um die Lösung im Audit-Modus auszuführen, setzen Sie das `DryRunFlag` Flag auf True, wenn Sie die Schlüsselrotationsvorlage oder in der Umgebungsvariablen für die `access_key_auto_rotation` Lambda-Funktion ausführen.

Automatisierung und Skalierung

Die CloudFormation Vorlagen, die diese Lösung automatisieren, werden im GitHub IAM-Schlüsselrotations-Repository bereitgestellt und im Abschnitt Code aufgeführt. In AWS Organizations können Sie verwenden, CloudFormation StackSets um die `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` CloudFormation Vorlage in mehreren Konten bereitzustellen, anstatt die Lösung einzeln für jedes Mitgliedskonto bereitzustellen.

Tools

AWS-Services

- Amazon CloudWatch unterstützt Sie bei der Überwachung der Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie in AWS ausführen, in Echtzeit.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Email Service (Amazon SES) hilft Ihnen beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domänen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.
- Amazon VPC-Endpunkte bieten eine Schnittstelle für die Verbindung mit Services, die von AWS unterstützt werden PrivateLink, einschließlich vieler AWS-Services. Für jedes Subnetz, das Sie in Ihrer VPC angeben, wird eine Endpunkt-Netzwerkschnittstelle im Subnetz erstellt und eine private IP-Adresse aus dem Subnetz-Adressbereich zugewiesen.

Code

Die erforderlichen AWS- CloudFormation Vorlagen, Python-Skripte und Runbook-Dokumentation sind im GitHub IAM-Schlüsselrotations-Repository verfügbar. Die Vorlagen werden wie folgt bereitgestellt.

Vorlage	Bereitstellen in	Hinweise
`ASA-iam-key-auto-rotation-and-notifier-solution.yaml`	Bereitstellungskonto	Dies ist die Hauptvorlage für die Lösung.
`ASA-iam-key-auto-rotation-iam-assumed-roles.yaml`	Einzelne oder mehrere Mitgliedskonten, bei denen Sie die Anmeldeinformationen rotieren möchten	Sie können CloudFormation Stack-Sets verwenden, um diese Vorlage in mehreren Konten bereitzustellen.

`ASA-iam-key-auto-rotation-list-accounts-role.yaml`	Zentrales/Verwaltungskonto	Verwenden Sie diese Vorlage, um ein Inventar von Konten in AWS Organizations zu führen.
`ASA-iam-key-auto-rotation-vpc-endpoints.yaml`	Bereitstellungskonto	Verwenden Sie diese Vorlage, um die Erstellung von Endpunkten nur zu automatisieren, wenn Sie die Lambda-Funktionen in einer VPC ausführen möchten (in der Hauptvorlage den `RunLambdaInVPC` Parameter auf „True“ setzen).

Polen

Einrichten der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie Ihren Bereitstellungs-S3-Bucket aus.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Konto an, öffnen Sie die Amazon S3-Konsole und wählen Sie dann den S3-Bucket für Ihre Bereitstellung aus. Wenn Sie die Lösung für mehrere Konten in AWS Organizations implementieren möchten, melden Sie sich beim Verwaltungskonto für Ihre Organisation an.	Cloud-Architekt
Klonen Sie das Repository	Klonen Sie das GitHub IAM-Schlüsselrotations-Repository auf Ihren lokalen Desktop.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Dateien in den S3-Bucket hoch.	Laden Sie die geklonten Dateien in Ihren S3-Bucket hoch. Verwenden Sie die folgende Standardordnerstruktur, um alle geklonten Dateien und Verzeichnisse zu kopieren und einzufügen: `asa/asa-iam-rotation` Hinweis: Sie können diese Ordnerstruktur in den CloudFormation Vorlagen anpassen.	Cloud-Architekt
Ändern Sie die E-Mail-Vorlage.	Ändern Sie die `iam-auto-key-rotation-enforcement.html` E-Mail-Vorlage (im `template` Ordner) entsprechend Ihren Anforderungen. Ersetzen Sie `[Department Name Here]` am Ende der Vorlage durch den Namen Ihrer Abteilung.	Cloud-Architekt

Bereitstellen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für die Schlüsselrotation.	1. Starten Sie die `ASA-iam-key-auto-rotation-and-notifier-solution.yaml` Vorlage im Bereitstellungskonto.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Auswählen einer Stack-Vorlage in der - CloudFormation Dokumentation. 2. Geben Sie Werte für Parameter an, einschließlich: • CloudFormation S3-Bucket-Name (`S3BucketName`) – Der Name des Bereitstellungs-S3-Buckets, der Ihren Lambda-Code enthält. • CloudFormation S3-Bucket-Präfix (`S3BucketPrefix`) – Das Präfix des S3-Buckets. • Angenommener IAM-Rollenname (`IAMRoleName`) – Der Rollenname, den die `key-rotation` Lambda-Funktion zum Rotieren der Schlüssel übernimmt. • Name der IAM-Ausführungsrolle (`ExecutionRoleName`) – Der Name der IAM-Ausführungsrolle, die von der `key-rotation` Lambda-Funktion verwendet wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Name der Bestandsausführungsrolle (`Inventory Execution RoleName`) – Der Name der IAM-Ausführungsrolle, die von der `account_inventory` Lambda-Funktion verwendet wird. • Markierung für Testlauf (Auditmodus) (`DryRunFlag`) – Auf „true“ setzen, um den Auditmodus zu aktivieren (Standard). Setzen Sie den Wert auf False, um den Erzwingungsmodus zu aktivieren. • Konto zum Auflisten von Organisationskonten (`OrgListAccount`) – Die Konto-ID des zentralen/Verwaltungskontos, das zum Auflisten der Konten in der Organisation verwendet wird. • Rollenname auflisten (`OrgListRole`) – Der Rollenname, der zum Auflisten der Konten in der Organisation verwendet wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Secrets-Store-Flag für zentrales Konto (`StoreSecretsInCentralAccount`) – Setzen Sie auf True, um Secrets im zentralen Konto zu speichern. Setzen Sie den Wert auf False, um Secrets im jeweiligen Konto zu speichern. • Regionen zum Replizieren der Anmeldeinformationen (`CredentialReplicationRegions`) – Die AWS-Regionen, in denen Sie die Anmeldeinformationen replizieren möchten (Secrets Manager), getrennt durch Kommas, z. B. `us-east-2,us-west-1,us-west-2`. Überspringen Sie die Region, in der Sie den Stack erstellen. • Lambda in VPC ausführen (`RunLambdaInVpc`) – Auf „true“ setzen, um Lambda-Funktionen in einer angegebenen VPC	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auszuführen. Sie müssen VPC-Endpunkte erstellt haben und ein NAT-Gateway an das Subnetz anhängen, das die Lambda-Funktion enthält. Weitere Informationen finden Sie im re:Post-Artikel, der diese Option behandelt. • VPC-ID für Lambda-Funktionen (`VpcId`), VPC CIDR für die Sicherheitsgruppenregel (`VpcCidr`) und Subnetz-ID für Lambda-Funktionen (`SubnetId`) – Geben Sie Informationen über die VPC, CIDR und das Subnetz an, wenn Sie `RunLambdaInVpc` auf „True“ setzen. • Admin-E-Mail-Adresse (`AdminEmailAddress`) – Eine gültige E-Mail-Adresse, an die Benachrichtigungen gesendet werden sollen. • AWS Organization ID (`AWSOrgID`) – Die eindeutige ID Ihrer Organisation. Diese ID beginnt mit `o-` und gefolgt von 10–32	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kleinbuchstaben oder Ziffern. • Name der E-Mail-Vorlagendatei [Auditmodus] (`EmailTemplateAudit`) und [Modus durchsetzen] (`EmailTemplateEnforce`) – Der Dateiname der E-Mail-HTML-Vorlage, die vom `notifier` Modul für den Auditmodus und den Erzwingungsmodus gesendet werden soll. • SMTP User SSM Parameter Name (`SMTPUserParamName`) und SMTP Password SSM Parameter Name (`SMTPPasswordParamName`) – Benutzer- und Passwortinformationen für Simple Mail Transfer Protocol (SMTP).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für angenommene Rollen.	1. Starten Sie in der AWS-CloudFormation Konsole die `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` Vorlage für jedes Konto, in dem Sie Schlüssel rotieren möchten. Wenn Sie mehr als ein Konto haben, können Sie die CloudFormation Hauptvorlage in Ihrem Verwaltungskonto als Stack bereitstellen und die `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` Vorlage mit CloudFormation Stack-Sets für alle erforderlichen Konten bereitstellen. Weitere Informationen finden Sie unter Arbeiten mit AWS CloudFormation StackSets in der - CloudFormation Dokumentation. 2. Geben Sie Werte für die folgenden Parameter an: • Angenommener IAM-Rollenname (`IAMRoleName`) – IAM-Rollenname, der von der Lambda-`access_key_auto_rotation` Funktion	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	übernommen wird. Sie können den Standardwert beibehalten. • Name der IAM-Ausfü hrungsrolle (`Execution RoleName`) – Die IAM-Rolle, die die Unterkont orolle übernimmt, um die Lambda-Funktion auszuführen. • Primäre AWS-Konto-ID (`PrimaryAccountID`) – Die AWS-Konto-ID, in der die Hauptvorlage bereitgestellt wird. • IAM-Ausnahmegruppe (`IAMExemptionGroup`) – Der IAM-Gruppenname, der verwendet wird, um IAM-Konten zu erleichte rn, die Sie von der automatischen Schlüssel rotation ausschließen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für den Kontobestand.	1. Starten der `ASA-iam-key-auto-rotation-list-accounts-role.yaml` Vorlage im Verwaltungs-/Zentralkonto 2. Geben Sie Werte für die folgenden Parameter an: • Angenommener IAM-Rollenname (`IAMRoleName`) – IAM-Rollenname, den die Lambda-`access_key_auto_rotation` Funktion übernimmt. • Name der IAM-Ausführungsrolle für Konto Lambda (`AccountExecutionRoleName`) – Der Name der IAM-Rolle, die die Lambda-`notifier`Funktion übernehmen wird. • Name der IAM-Ausführungsrolle für Lambda (`RotationExecutionRoleName`) – Der Name der IAM-Rolle, die die Lambda-`access_key_auto_rotation` Funktion übernehmen wird.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Primäre AWS-Konto-ID (`PrimaryAccountID`) – Die AWS-Konto-ID, in der die Hauptvorlage bereitgestellt wird.	
Starten Sie die CloudFormation Vorlage für VPC-Endpunkte.	Diese Aufgabe ist optional. 1. Starten Sie die `ASA-iam-key-auto-rotation-vpc-endpoints.yaml` Vorlage im Bereitstellungskonto. 2. Geben Sie Werte für die folgenden Parameter an: • VPC-ID (`pVpcId`), Subnetz-ID (`pSubnetId`) und CIDR-Bereich für VPC (`pVPCCidr`) – Geben Sie Informationen über die VPC, CIDR und das Subnetz an. • Legen Sie den Parameter für jeden VPC-Endpunkt auf True fest. Wenn Sie bereits über Endpunkte verfügen, können Sie False auswählen.	Cloud-Architekt

Zugehörige Ressourcen

- Bewährte Methoden für die Sicherheit in IAM (IAM-Dokumentation)
- AWS Organizations und serviceverknüpfte Rollen (Dokumentation zu AWS Organizations)

- Auswählen einer Stack-Vorlage (CloudFormation Dokumentation)
- Arbeiten mit AWS CloudFormation StackSets (CloudFormation Dokumentation)

Automatische Validierung und Bereitstellung von IAM-Richtlinien und -Rollen in einem AWS-Konto mithilfe von CodePipeline, IAM Access Analyzer und AWS- CloudFormation Makros

Erstellt von Helton Henrique Boleiro (AWS) und Guilherme Simoes (AWS)

Code-Repository: Pipeline für IAM-Rollen	Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; DevOps
AWS-Services: AWS CloudFormation; AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; AWS Lambda ; AWS SAM		

Übersicht

Dieses Muster beschreibt die Schritte und bietet Code zum Erstellen einer Bereitstellungspipeline, mit der Ihre Entwicklungsteams AWS Identity and Access Management (IAM)-Richtlinien und -Rollen in Ihren Amazon Web Services (AWS)-Konten erstellen können. Dieser Ansatz hilft Ihrer Organisation, den Overhead für Ihre Betriebsteams zu reduzieren und den Bereitstellungsprozess zu beschleunigen. Es hilft Ihren Entwicklern auch, IAM-Rollen und -Richtlinien zu erstellen, die mit Ihren bestehenden Governance- und Sicherheitskontrollen kompatibel sind.

Der Ansatz dieses Musters verwendet AWS Identity and Access Management Access Analyzer, um die IAM-Richtlinien zu validieren, die Sie IAM-Rollen anfügen möchten, und verwendet AWS, CloudFormation um die IAM-Rollen bereitzustellen. Anstatt die AWS- CloudFormation Vorlagendatei jedoch direkt zu bearbeiten, erstellt Ihr Entwicklungsteam JSON-formatierte IAM-Richtlinien und -Rollen. Ein AWS- CloudFormation Makro wandelt diese Richtliniendateien im JSON-Format in AWS CloudFormation IAM-Ressourcentypen um, bevor die Bereitstellung gestartet wird.

Die Bereitstellungspipeline (`RolesPipeline`) hat Quell-, Validierungs- und Bereitstellungsphasen. Während der Quellphase überträgt Ihr Entwicklungsteam die JSON-Dateien, die die Definition der IAM-Rollen und -Richtlinien enthalten, in ein AWS- CodeCommit Repository. AWS führt CodeBuild dann ein Skript aus, um diese Dateien zu validieren und sie in einen Amazon Simple Storage Service

(Amazon S3)-Bucket zu kopieren. Da Ihre Entwicklungsteams keinen direkten Zugriff auf die AWS-CloudFormation Vorlagendatei haben, die in einem separaten S3-Bucket gespeichert ist, müssen sie dem Prozess der Erstellung und Validierung von JSON-Dateien folgen.

Schließlich CodeDeploy verwendet AWS während der Bereitstellungsphase einen AWS-CloudFormation Stack, um die IAM-Richtlinien und -Rollen in einem Konto zu aktualisieren oder zu löschen.

Wichtig: Der Workflow dieses Musters ist ein Machbarkeitsnachweis (POC) und wir empfehlen, ihn nur in einer Testumgebung zu verwenden. Wenn Sie den Ansatz dieses Musters in einer Produktionsumgebung verwenden möchten, finden Sie weitere Informationen unter Bewährte Methoden für die Sicherheit in IAM in der IAM-Dokumentation und nehmen Sie die erforderlichen Änderungen an Ihren IAM-Rollen und AWS-Services vor.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein neuer oder vorhandener S3-Bucket für die `RolesPipeline` Pipeline. Stellen Sie sicher, dass die von Ihnen verwendeten Anmeldeinformationen über Berechtigungen zum Hochladen von Objekten in diesen Bucket verfügen.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installieren, Aktualisieren und Deinstallieren der AWS CLI in der AWS CLI-Dokumentation.
- AWS Serverless Application Model (AWS SAM)-CLI, installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installieren der AWS SAM CLI in der AWS SAM-Dokumentation.
- Python 3, installiert auf Ihrem lokalen Computer. Weitere Informationen dazu finden Sie in der Python-Dokumentation.
- Ein Git-Client, installiert und konfiguriert.
- Das GitHub `IAM roles pipeline` auf Ihrem lokalen Computer geklonte Repository.
- Bestehende IAM-Richtlinien und -Rollen im JSON-Format. Weitere Informationen dazu finden Sie in der -ReadMeDatei im Github-`IAM roles pipeline`Repository.
- Ihr Entwicklerteam darf nicht über Berechtigungen zum Bearbeiten der AWS- CodePipeline CodeBuild, - und - CodeDeploy Ressourcen dieser Lösung verfügen.

Einschränkungen

- Der Workflow dieses Musters ist ein Machbarkeitsnachweis (POC) und wir empfehlen, ihn nur in einer Testumgebung zu verwenden. Wenn Sie den Ansatz dieses Musters in einer Produktionsumgebung verwenden möchten, lesen Sie Bewährte Methoden für die Sicherheit in IAM in der IAM-Dokumentation und nehmen Sie die erforderlichen Änderungen an Ihren IAM-Rollen und AWS-Services vor.

Architektur

Das folgende Diagramm zeigt Ihnen, wie Sie IAM-Rollen und -Richtlinien mithilfe von CodePipeline, IAM Access Analyzer und AWS- CloudFormation Makros automatisch validieren und für ein Konto bereitstellen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Entwickler schreibt JSON-Dateien, die die Definitionen für die IAM-Richtlinien und -Rollen enthalten. Der Entwickler überträgt den Code an ein CodeCommit Repository und initiiert CodePipeline dann die `RolesPipeline` Pipeline.
2. CodeBuild validiert die JSON-Dateien mithilfe von IAM Access Analyzer. Wenn Sicherheits- oder Fehlerergebnisse vorliegen, wird der Bereitstellungsprozess gestoppt.
3. Wenn keine Sicherheits- oder Fehlerergebnisse vorliegen, werden die JSON-Dateien an den `RolesBucket` S3-Bucket gesendet.
4. Ein AWS- CloudFormation Makro, das als AWS Lambda-Funktion implementiert ist, liest dann die JSON-Dateien aus dem `RolesBucket` Bucket und wandelt sie in AWS CloudFormation IAM-Ressourcentypen um.
5. Ein vordefinierter AWS- CloudFormation Stack installiert, aktualisiert oder löscht die IAM-Richtlinien und -Rollen im Konto.

Automatisierung und Skalierung

AWS- CloudFormation Vorlagen, die dieses Muster automatisch bereitstellen, werden im Pipeline-Repository für GitHub IAM-Rollen bereitgestellt.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- IAM Access Analyzer hilft Ihnen dabei, die Ressourcen in Ihrer Organisation und Ihren Konten zu identifizieren, z. B. S3-Buckets oder IAM-Rollen, die mit einer externen Entität geteilt werden. Auf diese Weise können Sie unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten identifizieren.
- AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie Serverless-Anwendungen in der AWS Cloud erstellen können.

Code

Der Quellcode und die Vorlagen für dieses Muster sind im GitHub Pipeline-Repository für IAM-Rollen verfügbar.

Sekunden

Klonen des Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispiel-Repository.	Klonen Sie das GitHub Pipeline-Repository für IAM-Rollen auf Ihren lokalen Computer.	App-Entwickler, Allgemeines AWS

Bereitstellen der RolesPipeline Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Pipeline bereit.	1. Navigieren Sie zu dem Verzeichnis, das das geklonte Repository enthält.	App-Entwickler, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Führen Sie den Befehl `make deploy bucket=<bucket_name>` aus. Wichtig: Sie müssen durch `<bucket_name>` den Bucket-Namen für Ihren vorhandenen S3-Bucket ersetzen. 3. Führen Sie den `aws codepipeline get-pipeline –name RolesPipeline` Befehl aus, um zu überprüfen, ob Ihre Bereitstellung erfolgreich ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository der Pipeline.	1. Der `RolesPipeline` AWS- CloudFormation Stack erstellt das `roles-pipeline-repo` CodeCommit Repository. 2. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS-CodeCommit Konsole und kopieren Sie dann die URL des CodeCommit Repositorys, um es auf Ihren lokalen Computer zu klonen. Weitere Informationen dazu finden Sie unter Herstellen einer Verbindung mit einem AWS- CodeCommit Repository in der AWS-CodeCommit Dokumentation.	App-Entwickler, Allgemeines AWS

Testen der RolesPipeline Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die RolesPipeline Pipeline mit gültigen IAM-Richtlinien und -Rollen.	1. Erstellen Sie JSON-Daten für Ihre IAM-Richtlinien und -Rollen. Sie können die Beispiele im `role-example` Verzeichnis aus dem GitHub `IAM roles pipeline` Repository verwenden.	App-Entwickler, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Definieren Sie Ihre IAM-Richtlinien und -Rollen mit den erforderlichen Konfigurationen. Wichtig: Stellen Sie sicher, dass Sie dem in der `ReadMe` Datei aus dem GitHub `IAM roles pipeline` Repository beschriebenen Format folgen. 3. Übertragen Sie die Änderungen in das `roles-pipeline-repo` CodeCommit Repository. 4. Überprüfen Sie die Implementierung der `RolesPipeline` Pipeline. 5. Stellen Sie sicher, dass die IAM-Richtlinien und -Rollen im Konto korrekt bereitgestellt sind. 6. Überprüfen Sie, ob den IAM-Richtlinien oder -Rollen eine Berechtigungsgrenze zugeordnet ist. Weitere Informationen dazu finden Sie unter Berechtigungsgrenzen für IAM-Entitäten in der IAM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die RolesPipeline Pipeline mit ungültigen IAM-Richtlinien und -Rollen.	1. Ändern Sie das `roles-pipeline-repo` CodeCommit Repository und schließen Sie ungültige IAM-Rollen oder -Richtlinien ein. Sie können beispielsweise eine nicht vorhandene Aktion oder eine ungültige IAM-Richtlinienversion verwenden. 2. Überprüfen Sie die Pipeline-Implementierung. IAM Access Analyzer stoppt die Pipeline während der Validierungsphase, wenn es ungültige IAM-Richtlinien oder -Rollen erkennt.	App-Entwickler, Allgemeines AWS

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie sich auf die Bereinigung vor.	Leeren Sie die S3-Buckets und führen Sie dann den `destroy` Befehl aus.	App-Entwickler, Allgemeines AWS
Löschen Sie den RolesStack Stack.	1. Die `RolesPipeline` Pipeline erstellt einen `RolesStack` AWS-CloudFormation Stack, der die IAM-Richtlinien und -Rollen bereitstellt. Sie müssen diesen Stack löschen, bevor Sie die	App-Entwickler, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`RolesPipeline` Pipeline löschen. 2. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS-CloudFormation Konsole, wählen Sie dann den `RolesStack` Stack und dann Löschen aus.	
Löschen Sie den RolesPipeline Stack.	Um den `RolesPipeline` AWS- CloudFormation Stack zu löschen, folgen Sie den Anweisungen aus der ReadMe Datei im Github-`IAM roles pipeline`Repository.	App-Entwickler, Allgemeines AWS

Zugehörige Ressourcen

- IAM Access Analyzer – Richtlinienvalidierung (AWS News Blog)
- Verwenden von AWS- CloudFormation Makros zur benutzerdefinierten Verarbeitung von Vorlagen (AWS- CloudFormation Dokumentation)
- Erstellen von Lambda-Funktionen mit Python (AWS Lambda-Dokumentation)

Bidirektionale Integration von AWS Security Hub mit Jura-Software

Erstellt von Joa Bol Man Rinaudo (AWS)

Code-Repository: Integration von Security Hub zu JIRA	Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance
Workload: Alle anderen Workloads	AWS-Services: AWS Lambda; AWS Security Hub; Amazon CloudWatch	

Übersicht

Diese Lösung unterstützt eine bidirektionale Integration zwischen AWS Security Hub und JSpeed. Mit dieser Lösung können Sie JIRA-Tickets anhand von Security Hub-Ergebnissen automatisch und manuell erstellen und aktualisieren. Sicherheitsteams können diese Integration verwenden, um Entwicklerteams über schwerwiegende Sicherheitserkenntnisse zu informieren, die Maßnahmen erfordern.

Die Lösung ermöglicht Ihnen Folgendes:

- Wählen Sie aus, welche Security Hub-Steuerelemente automatisch Tickets in Jura erstellen oder aktualisieren.
- Verwenden Sie in der Security-Hub-Konsole benutzerdefinierte Security-Hub-Aktionen, um Tickets in J Bol manuell zu eskalieren.
- Weisen Sie Tickets automatisch in Jpir zu, basierend auf den AWS-Konto-Tags, die in AWS Organizations definiert sind. Wenn dieses Tag nicht definiert ist, wird ein Standardzuweisungsempfänger verwendet.
- Unterdrücken Sie automatisch Security Hub-Ergebnisse, die in JSpeed als falsch positives oder akzeptiertes Risiko markiert sind.
- Schließen Sie ein JCCP-Ticket automatisch, wenn die zugehörige Erkenntnis in Security Hub archiviert wird.
- Öffnen Sie JCCP-Tickets erneut, wenn Security Hub-Ergebnisse erneut auftreten.

Jura-Workflow

Die Lösung verwendet einen benutzerdefinierten Jura-Workflow, mit dem Entwickler Risiken verwalten und dokumentieren können. Während das Problem den Workflow durchläuft, stellt die bidirektionale Integration sicher, dass der Status des JCCP-Tickets und der Security Hub-Erkenntnis über die Workflows in beiden Services hinweg synchronisiert wird. Dieser Workflow ist ein abgeleiteter SecDevOps Risiko-Workflow von Dinis Bolz, lizenziert unter CC BY 4.0. Wir empfehlen, eine Jura-Workflow-Bedingung hinzuzufügen, damit nur Mitglieder Ihres Sicherheitsteams den Ticketstatus ändern können.

Ein Beispiel für ein JSpeed-Ticket, das automatisch von dieser Lösung generiert wird, finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Wenn Sie diese Lösung in einer AWS-Umgebung mit mehreren Konten bereitstellen möchten:
  - Ihre Umgebung mit mehreren Konten ist aktiv und wird von AWS Organizations verwaltet.
  - Security Hub ist für Ihre AWS-Konten aktiviert.
  - In AWS Organizations haben Sie ein Security Hub-Administratorkonto festgelegt.
  - Sie haben eine kontoübergreifende IAM-Rolle, die über `AWSOrganizationsReadOnlyAccess` Berechtigungen für das AWS Organizations-Verwaltungskonto verfügt.
  - (Optional) Sie haben Ihre AWS-Konten mit markiert`SecurityContactID`. Dieses Tag wird verwendet, um JSpeed-Tickets den definierten Sicherheitskontakten zuzuweisen.
- Wenn Sie diese Lösung in einem einzigen AWS-Konto bereitstellen möchten:
  - Sie haben ein aktives AWS-Konto.
  - Security Hub ist in Ihrem AWS-Konto aktiviert.
- Eine Jura-Server-Instance

  Wichtig: Diese Lösung unterstützt die Verwendung von Jura Cloud. Jura Cloud unterstützt jedoch den Import von XML-Workflows nicht, daher müssen Sie den Workflow manuell in JSpeed neu erstellen.
- Administratorberechtigungen in J Bol
- Eines der folgenden JCCP-Token:

- Für Jura Enterprise ein persönliches Zugriffstoken (PAT). Weitere Informationen finden Sie unter Verwenden von persönlichen Zugriffstoken (Atlassischer Support).
- Für Jura Cloud ein JCCP-API-Token. Weitere Informationen finden Sie unter Verwalten von API-Token (Atlassischer Support).

Architektur

Dieser Abschnitt veranschaulicht die Architektur der Lösung in verschiedenen Szenarien, z. B. wenn der Entwickler und Sicherheitsingenieur das Risiko akzeptieren oder das Problem beheben.

Szenario 1: Entwickler behebt das Problem

1. Security Hub generiert eine Erkenntnis anhand einer bestimmten Sicherheitskontrolle, z. B. derjenigen im AWS Foundational Security Best Practices Standard .
2. Ein Amazon- CloudWatch Ereignis, das mit der Erkenntnis und der `CreateJIRA` Aktion verknüpft ist, initiiert eine AWS Lambda-Funktion.
3. Die Lambda-Funktion verwendet ihre Konfigurationsdatei und das `GeneratorId` Feld der Erkenntnis, um zu bewerten, ob sie die Erkenntnis eskalieren soll.
4. Die Lambda-Funktion bestimmt, dass die Erkenntnis eskaliert werden soll. Sie erhält das `SecurityContactID` Konto-Tag von AWS Organizations im AWS-Verwaltungskonto. Diese ID ist dem Entwickler zugeordnet und wird als Zuweisungsempfänger-ID für das JCCP-Ticket verwendet.
5. Die Lambda-Funktion verwendet die in AWS Secrets Manager gespeicherten Anmeldeinformationen, um ein Ticket in Jura zu erstellen. J Bol benachrichtigt den Entwickler.
6. Der Entwickler befasst sich mit der zugrunde liegenden Sicherheitserkenntnis und ändert in J Bol den Status des Tickets in `TEST FIX`.
7. Security Hub aktualisiert die Erkenntnis als `ARCHIVED`und es wird ein neues Ereignis generiert. Dieses Ereignis bewirkt, dass die Lambda-Funktion das JCCP-Ticket automatisch schließt.

Szenario 2: Der Entwickler entscheidet sich, das Risiko zu akzeptieren

1. Security Hub generiert eine Erkenntnis anhand einer bestimmten Sicherheitskontrolle, z. B. derjenigen im AWS Foundational Security Best Practices Standard .

2. Ein CloudWatch Ereignis, das mit der Erkenntnis und der `CreateJIRA` Aktion verknüpft ist, initiiert eine Lambda-Funktion.
3. Die Lambda-Funktion verwendet ihre Konfigurationsdatei und das `GeneratorId` Feld der Erkenntnis, um zu bewerten, ob sie die Erkenntnis eskalieren soll.
4. Die Lambda-Funktion bestimmt, dass die Erkenntnis eskaliert werden soll. Sie erhält das `SecurityContactID` Konto-Tag von AWS Organizations im AWS-Verwaltungskonto. Diese ID ist dem Entwickler zugeordnet und wird als Zuweisungsempfänger-ID für das JCCP-Ticket verwendet.
5. Die Lambda-Funktion verwendet die in Secrets Manager gespeicherten Anmeldeinformationen, um ein Ticket in Jura zu erstellen. J Bol benachrichtigt den Entwickler.
6. Der Entwickler entscheidet sich, das Risiko zu akzeptieren, und ändert in J Bol den Status des Tickets in `AWAITING RISK ACCEPTANCE`.
7. Der Sicherheitsingenieur überprüft die Anfrage und findet die entsprechende geschäftliche Begründung. Der Sicherheitsingenieur ändert den Status des Jura-Tickets in `ACCEPTED RISK`. Dadurch wird das JCCP-Ticket geschlossen.
8. Ein CloudWatch tägliches Ereignis initiiert die Aktualisierungs-Lambda-Funktion, die geschlossene JIRA-Tickets identifiziert und ihre zugehörigen Security Hub-Ergebnisse als aktualisiert`SUPPRESSED`.

Tools

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- Amazon CloudWatch Events hilft Ihnen bei der Überwachung von Systemereignissen für Ihre AWS-Ressourcen, indem Regeln verwendet werden, um Ereignisse abzugleichen und sie an Funktionen oder Streams weiterzuleiten.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- AWS Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS-Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.

Code-Repository

Der Code für dieses Muster ist auf GitHubim aws-securityhub-jira-software-Integrations-Repository verfügbar. Sie enthält den Beispielcode und den JSpeed-Workflow für diese Lösung.

Polen

Konfigurieren von Jura

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie den Workflow.	Importieren Sie als Administrator in JSpeed die `issue-workflow.xml` Datei in Ihre Jura-Server-Instance. Diese Datei finden Sie im aws-securityhub-jira-software-Integrations-Repository in GitHub. Anweisungen finden Sie unter Verwenden von XML zum Erstellen eines Workflows (Jura-Dokumentation).	Jura-Administrator
Aktivieren Sie den Workflow und weisen Sie ihn zu.	Workflows sind inaktiv, bis Sie sie einem Workflow-Schema zuweisen. Anschließend weisen Sie das Workflow-Schema einem Projekt zu. 1. Stellen Sie für Ihr Projekt sicher, dass Sie ein	Jura-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Problemtypschema für das Projekt identifiziert haben. Sie können einen neuen Problemtyp erstellen oder einen vorhandenen auswählen, z. B. Bug. 2. Weisen Sie den importier ten Workflow einem Workflow-Schema gemäß den Anweisungen unter Workflow aktivieren zu (Jaffin-Dokumentation). 3. Weisen Sie das Workflow-Schema einem Projekt gemäß den Anweisung en unter Zuordnen eines Workflow-Schemas zu einem Projekt zu (Jura-Dok umentation).	

Einrichten der Lösungsparameter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Lösungsparameter.	1. Öffnen Sie im Ordner conf `params_prod.shfile` . 2. Geben Sie Werte für die folgenden Parameter an: • `ORG_ACCOUNT_ID` – Die Konto-ID für Ihr AWS Organizations-Verwaltungskonto. Die Lösung liest Konto-Tag	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	s und weist Tickets den spezifischen Sicherheitskontakten zu, die in diesen AWS-Konto-Tags definiert sind. • `ORG_ROLE` – Der Name der IAM-Rolle, die für den Zugriff auf das AWS Organization-Verwaltungskonto verwendet wird. Diese Rolle muss über `-OrganizationsReadOnlyAccess` Berechtigungen verfügen. • `EXTERNAL_ID` – Ein optionaler Parameter, wenn Sie eine externe ID verwenden, um die in definierte IAM-Rolle zu übernehmen`ORG_ROLE`. Weitere Informationen finden Sie unter So verwenden Sie eine externe ID (IAM-Dokumentation). • `JIRA_DEFAULT_ASSIGNEE` – Dies ist die JCCP-ID für den Standard-Zuweisungsempfänger für alle Sicherheitsprobleme. Dieser zugewiesene Standard wird verwendet	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, falls das Konto nicht ordnungsgemäß markiert ist oder die Rolle nicht übernommen werden kann. • `JIRA_INSTANCE` – Die HTTPS-Adresse für Ihren JSpeed-Server im folgenden Format: `team-<team-id>.atlassian.net/` • `JIRA_PROJECT_KEY` – Der Name des JSpeed-Projektschlüssels, der zum Erstellen von Tickets verwendet wird, z. B. `SEC` oder `TEST`. Dieses Projekt muss bereits in Jira vorhanden sein. • `ISSUE_TYPE` – Der Name des Problemtypschemas, das dem Projekt in JSpeed zugewiesen ist, z. B. `Bug` oder `Security Issue`. • `REGIONS` – Liste der AWS-Regionscodes, in denen Sie diese Lösung bereitstellen möchten, z. B. `eu-west-1` . 3. Speichern und schließen Sie die Lösungsparameterdatei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Ergebnisse, die Sie automatisieren möchten.	1. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/ 2. Wählen Sie im Navigationsbereich des Security Hub die Option Erkenntnisse aus. 3. Wählen Sie den Titel der Erkenntnis aus. 4. Wählen Sie die Erkenntnis-ID aus. Dadurch wird der vollständige JSON-Code für die Erkenntnis angezeigt. 5. Kopieren Sie im JSON die Zeichenfolge in das `GeneratorId` Feld. Dieser Wert ist im AWS Security Finding Format (ASFF). Beispielsweise `aws-foundational-security-best-practices/v/1.0.0/S3.1` entspricht den Ergebnissen aus der SS3.1-Sicherheitskontrolleinstellung S3Öffentlichen Zugriff blockieren“ sollte aktiviert sein. 6. Wiederholen Sie diese Schritte, bis Sie alle `GeneratorID` Werte für alle Erkenntnisse kopiert	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	haben, die Sie automatis ieren möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Ergebnisse der Konfigurationsdatei hinzu.	1. Öffnen Sie in src/codeconfig.js onconfig die Datei . 2. Fügen Sie die Generator ID Werte, die Sie in der vorherigen Geschichte abgerufen haben, in den default Parameter ein und trennen Sie jede ID durch Kommas. 3. Speichern und schließen Sie die -Konfigurationsdatei. Das folgende Codebeispiel zeigt die Automatisierung der aws-foundational-security-best-practices/v/1.0.0/S3.1 Ergebnisse aws-foundational-security-best-practices/v/1.0.0/SNS.1 und . `{ "Controls" : { "eu-west-1": [ "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22" ], "default": [ aws-foundational-security-best-practices/v/1.0.0/SNS.1,`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>aws-foundational-
	security-best-p
	ractices/v/1.0.0/S3.1
	]
	}
	}</pre>
	Hinweis: Sie können verschied ene Erkenntnisse für jede AWS-Region automatisieren. Eine bewährte Methode zur Vermeidung duplizier ter Erkenntnisse besteht darin, eine einzelne Region auszuwählen, um die Erstellun g von IAM-bezogenen Kontrollen zu automatisieren.	

Bereitstellen der Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Integration bereit.	Geben Sie in einem Befehlsze ilen-Terminal den folgenden Befehl ein: <pre>./deploy.sh prod</pre>	AWS-Systemadministrator
Laden Sie Jura-Anme ldeinformationen in AWS Secrets Manager hoch.	1. Öffnen Sie die Secrets-Manager-Konsole unterhttps://console.a ws.amazon.com/sec retsmanager/.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie unter Secrets die Option Neues Secret speichern aus. 3. Als Secret-Typ wählen Sie Anderer Secret-Typ aus. 4. Wenn Sie Jura Enterprise verwenden, gehen Sie für Schlüssel/Wert-Paare wie folgt vor: • Geben Sie in der ersten Zeile `auth` in das Schlüsselfeld ein und geben Sie dann `token_auth` in das Wertfeld ein. • Fügen Sie eine zweite Zeile hinzu, geben Sie `token` in das Schlüssel feld ein und geben Sie dann Ihr persönliches Zugriffstoken in das Wertfeld ein. Wenn Sie Jura Cloud verwenden, gehen Sie für Schlüssel/Wert-Paare wie folgt vor: • Geben Sie in der ersten Zeile `auth` in das Schlüsselfeld ein und geben Sie dann `basic_auth` in das Wertfeld ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Fügen Sie eine zweite Zeile hinzu, geben Sie `token` in das Schlüssel feld ein und geben Sie dann Ihr API-Token in das Wertfeld ein. • Fügen Sie eine dritte Zeile hinzu, geben Sie `email` in das Schlüssel feld ein und geben Sie dann Ihre E-Mail-Adresse in das Wertfeld ein. 5. Wählen Sie Weiter aus. 6. Geben Sie für Secret-Na me ein `Jira-Token` und wählen Sie dann unten auf der Seite Weiter aus. 7. Behalten Sie auf der Seite Secret-Rotation die Option Automatische Drehung deaktivieren bei und wählen Sie dann unten auf der Seite Weiter aus. 8. Überprüfen Sie auf der Seite Überprüfen die Secret-Details und wählen Sie dann Speichern aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die benutzerd efinierte Security Hub-Aktion.	1. Verwenden Sie für jede AWS-Region in der AWS Command Line Interface (AWS CLI) den create-action-target Befehl , um eine benutzerdefinierte Security Hub-Aktion mit dem Namen zu erstellen`CreateJiraIssue` . `aws securityhub create-action-target --name "CreateJiraIssue" \ --description "Create ticket in JIRA" \ --id "CreateJiraIssue" --region $<aws-region>` 2. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/. 3. Wählen Sie im Navigationsbereich des Security Hub die Option Erkenntnisse aus. 4. Wählen Sie in der Liste der Ergebnisse die Ergebnisse aus, die Sie eskalieren möchten.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie im Menü Aktionen die Option aus`CreateJiraIssue` .	

Zugehörige Ressourcen

- AWS Service Management Connector für Jura Service Management
- AWS Foundational Security Best Practices-Standard

Zusätzliche Informationen

Beispiel für ein JSpeed-Ticket

Wenn eine bestimmte Security Hub-Erkenntnis auftritt, erstellt diese Lösung automatisch ein JCCP-Ticket. Das Ticket enthält die folgenden Informationen:

- Titel – Der Titel identifiziert das Sicherheitsproblem im folgenden Format:

```
AWS Security Issue :: <AWS account ID> :: <Security Hub finding title>
```

- Beschreibung – Der Beschreibungsabschnitt des Tickets beschreibt die Sicherheitskontrolle im Zusammenhang mit der Erkenntnis, enthält einen Link zu der Erkenntnis in der Security Hub-Konsole und enthält eine kurze Beschreibung, wie das Sicherheitsproblem im JSpeed-Workflow behandelt werden kann.

Im Folgenden finden Sie ein Beispiel für ein automatisch generiertes JSpeed-Ticket.

Titel	AWS-Sicherheitsproblem :: 012345678912 :: Lambda.1 Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten.
Beschreibung	Was ist das Problem? Wir haben innerhalb des AWS-Kontos012345678912, für das Sie verantwortlich sind, ein Sicherheitsergebnis festgestellt.

Diese Kontrolle prüft, ob die AWS Lambda-Fu nktionsrichtlinie, die der Lambda-Ressource zugeordnet ist, den öffentlichen Zugriff verbietet . Wenn die Lambda-Funktionsrichtlinie öffentlic hen Zugriff zulässt, schlägt die Kontrolle fehl.

<Link zur Security Hub-Erkenntnis>

Was muss ich mit dem Ticket machen?

- Greifen Sie auf das Konto zu und überprüfe n Sie die Konfiguration. Bestätigen Sie die Arbeit mit dem Ticket, indem Sie es in „Zugewiesen für Korrektur“ verschieben. Nach der Behebung wurde in den Testfix verschoben, sodass die Sicherheitsüberprü fung das Problem behoben hat.
- Wenn Sie der Meinung sind, dass Risiken akzeptiert werden sollten, verschieben Sie sie in „Warten auf Risikoakzeptanz“. Dies muss von einem Sicherheitsingenieur geprüft werden.
- Wenn Sie der Meinung sind, dass es sich um ein falsch positives Ergebnis handelt, wechseln Sie es zu „Als falsch positiv markieren“. Dies wird von einem Sicherhei tsingenieur überprüft und entsprechend wieder geöffnet/geschlossen.

Erstellen einer Pipeline für gehärtete Container-Images mit EC2 Image Builder und Terraform

Erstellt von Bolcross (AWS) und Bol Ranes (AWS)

Code-Repository: Terraform EC2 Image Builder Container Hardening Pipeline	Umgebung: Produktion	Quelle: Packer, Chef oder Bol Ansible
Ziel: EC2 Image Builder	R-Typ: Neuarchitektur	Workload: Open-Source
Technologien: Sicherheit, Identität, Compliance; DevOps	AWS-Services: Amazon EC2 Container Registry ;Amazon EC2 Image Builder	

Übersicht

Dieses Muster erstellt eine EC2 Image Builder-Pipeline, die ein gehärtetes Amazon Linux 2-Basiscontainer-Image erzeugt. Terraform wird als Infrastructure as Code (IaC)-Tool verwendet, um die Infrastruktur zu konfigurieren und bereitzustellen, die zum Erstellen von gehärteten Container-Images verwendet wird. Das Rezept hilft Ihnen bei der Bereitstellung eines Docker-basierten Amazon Linux 2 Container-Images, das gemäß Red Hat Enterprise Linux (RHEL) 7 STIG Version 3 Release 7 Medium gehärtet wurde. (Siehe STIG-Build-Linux-Medium Version 2022.2.1 im Abschnitt Linux-STIG-Komponenten der EC2 Image Builder-Dokumentation.) Dies wird als goldenes Container-Image bezeichnet.

Der Build umfasst zwei Amazon- EventBridge Regeln. Eine Regel startet die Container-Image-Pipeline, wenn die Amazon Inspector-Erkenntnis hoch oder kritisch ist, sodass unsichere Images ersetzt werden. Diese Regel erfordert, dass sowohl Amazon Inspector als auch Amazon Elastic Container Registry (Amazon ECR) erweitertes Scannen aktiviert sind. Die andere Regel sendet nach einem erfolgreichen Image-Push in das Amazon-ECR-Repository Benachrichtigungen an eine Amazon Simple Queue Service (Amazon SQS)-Warteschlange, um Ihnen bei der Verwendung der neuesten Container-Images zu helfen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto, in dem Sie die Infrastruktur bereitstellen können.
- AWS Command Line Interface (AWS CLI) installiert, um Ihre AWS-Anmeldeinformationen für die lokale Bereitstellung festzulegen.
- Terraform wurde heruntergeladen und eingerichtet, indem die Anweisungen in der Terraform-Dokumentation befolgt wurden.
- Git (wenn Sie von einem lokalen Computer aus bereitstellen).
- Eine Rolle innerhalb des AWS-Kontos, die Sie zum Erstellen von AWS-Ressourcen verwenden können.
- Alle Variablen, die in der .tfvars-Datei definiert sind. Oder Sie können alle Variablen definieren, wenn Sie die Terraform-Konfiguration anwenden.

Einschränkungen

- Diese Lösung erstellt eine Amazon Virtual Private Cloud (Amazon VPC)-Infrastruktur, die ein NAT-Gateway und ein Internet-Gateway für die Internetverbindung aus seinem privaten Subnetz enthält. Sie können keine VPC-Endpunkte verwenden, da der Bootstrap-Prozess von AWS Task Orchestrator und Executor (AWSTOE) AWS CLI Version 2 aus dem Internet installiert.

Produktversionen

- Amazon Linux 2
- AWS CLI Version 1.1 oder höher

Architektur

Zieltechnologie-Stack

Dieses Muster erstellt 43 Ressourcen, darunter:

- Zwei Amazon Simple Storage Service (Amazon S3)-Buckets: einer für die Pipeline-Komponentendateien und einer für Serverzugriff und Amazon VPC-Flow-Protokolle
- Ein Amazon-ECR-Repository

- Eine Virtual Private Cloud (VPC), die ein öffentliches Subnetz, ein privates Subnetz, Routing-Tabellen, ein NAT-Gateway und ein Internet-Gateway enthält
- Eine EC2 Image Builder-Pipeline, ein Rezept und Komponenten
- Ein Container-Image
- Ein AWS Key Management Service (AWS KMS)-Schlüssel für die Image-Verschlüsselung
- Eine SQS-Warteschlange
- Drei Rollen: eine zum Ausführen der EC2 Image Builder-Pipeline, ein Instance-Profil für EC2 Image Builder und ein für EventBridge Regeln
- Zwei EventBridge Regeln

Terraform-Modulstruktur

Den Quellcode finden Sie im GitHub Repository Terraform EC2 Image Builder Container Hardening Pipeline.

```
### components.tf
### config.tf
### dist-config.tf
### files
#   ###assumption-policy.json
### hardening-pipeline.tfvars
### image.tf
### infr-config.tf
### infra-network-config.tf
### kms-key.tf
### main.tf
### outputs.tf
### pipeline.tf
### recipes.tf
### roles.tf
### sec-groups.tf
### trigger-build.tf
### variables.tf
```

Moduldetails

- `components.tf` enthält eine Amazon S3-Upload-Ressource zum Hochladen des Inhalts des `/files` Verzeichnisses. Sie können auch hier modular benutzerdefinierte Komponenten-YAML-Dateien hinzufügen.

- `/files` enthält die `.yml` Dateien, die die in verwendeten Komponenten definierencomponents.tf.
- `image.tf` enthält die Definitionen für das Basis-Image-Betriebssystem. Hier können Sie die Definitionen für eine andere Basis-Image-Pipeline ändern.
- `infr-config.tf` und `dist-config.tf` enthalten die Ressourcen für die minimale AWS-Infrastruktur, die zum Hochfahren und Verteilen des Images erforderlich ist.
- `infra-network-config.tf` enthält die minimale VPC-Infrastruktur, in der das Container-Image bereitgestellt werden soll.
- `hardening-pipeline.tfvars` enthält die Terraform-Variablen, die zum Zeitpunkt der Anwendung verwendet werden sollen.
- `pipeline.tf` erstellt und verwaltet eine EC2 Image Builder-Pipeline in Terraform.
- `recipes.tf` Hier können Sie verschiedene Mischungen von Komponenten angeben, um Container-Rezepte zu erstellen.
- `roles.tf` enthält die AWS Identity and Access Management (IAM)-Richtliniendefinitionen für das Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Profil und die Pipeline-Bereitstellungsrolle.
- `trigger-build.tf` enthält die EventBridge Regeln und SQS-Warteschlangenressourcen.

Zielarchitektur

Das Diagramm veranschaulicht den folgenden Workflow:

1. EC2 Image Builder erstellt ein Container-Image mithilfe des definierten Rezepts, das Betriebssystem-Updates installiert und den RHEL Medium STIG auf das Amazon Linux 2-Basis-Image anwendet.
2. Das gehärtete Image wird in einer privaten Amazon-ECR-Registrierung veröffentlicht, und eine - EventBridge Regel sendet eine Nachricht an eine SQS-Warteschlange, wenn das Image erfolgreich veröffentlicht wurde.
3. Wenn Amazon Inspector für erweitertes Scannen konfiguriert ist, scannt es die Amazon-ECR-Registrierung.
4. Wenn Amazon Inspector ein Ergebnis mit kritischem oder hohem Schweregrad für das Image generiert, löst eine - EventBridge Regel die erneute Ausführung der EC2 Image Builder-Pipeline aus und veröffentlicht ein neu gehärtetes Image.

Automatisierung und Skalierung

- Dieses Muster beschreibt, wie Sie die Infrastruktur bereitstellen und die Pipeline auf Ihrem Computer erstellen. Es soll jedoch in großem Umfang verwendet werden. Anstatt die Terraform-Module lokal bereitzustellen, können Sie sie in einer Umgebung mit mehreren Konten verwenden, z. B. in einem AWS Control Tower mit Account Factory für Terraform-Umgebung. In diesem Fall sollten Sie einen S3-Bucket mit Backend-Status verwenden, um Terraform-Statusdateien zu verwalten, anstatt den Konfigurationsstatus lokal zu verwalten.
- Stellen Sie die Lösung für die skalierte Verwendung in einem zentralen Konto bereit, z. B. einem Shared Services- oder Common Services-Konto, von einem Control Tower- oder Landing Zone-Kontomodell aus, und erteilen Sie Verbraucherkonten die Berechtigung für den Zugriff auf das Amazon ECR-Repository und den AWS KMS-Schlüssel. Weitere Informationen zur Einrichtung finden Sie im re:Post-Artikel Wie kann ich einem sekundären Konto erlauben, Images in meinem Amazon-ECR-Image-Repository zu pushen oder abzurufen? Fügen Sie beispielsweise in einem -Kontoverkaufsautomaten oder Account Factory für Terraform jeder Kontobasis oder Kontoanpassungsbasis Berechtigungen hinzu, um Zugriff auf dieses Amazon-ECR-Repository und diesen Verschlüsselungsschlüssel zu gewähren.
- Nachdem die Container-Image-Pipeline bereitgestellt wurde, können Sie sie mithilfe von EC2 Image Builder-Funktionen wie Komponenten ändern, die Ihnen helfen, weitere Komponenten in den Docker-Build zu packen.
- Der AWS KMS-Schlüssel, der zum Verschlüsseln des Container-Images verwendet wird, sollte für alle Konten freigegeben werden, in denen das Image verwendet werden soll.
- Sie können Unterstützung für andere Bilder hinzufügen, indem Sie das gesamte Terraform-Modul duplizieren und die folgenden `recipes.tf` Attribute ändern:
  - Ändern Sie `parent_image = "amazonlinux:latest"` zu einem anderen Bildtyp.
  - Ändern Sie `repository_name` so, dass es auf ein vorhandenes Amazon-ECR-Repository verweist. Dadurch wird eine weitere Pipeline erstellt, die einen anderen übergeordneten Image-Typ in Ihrem vorhandenen Amazon ECR-Repository bereitstellt.

Tools

Tools

- Terraform (IaC-Bereitstellung)
- Git (bei lokaler Bereitstellung)

- AWS CLI Version 1 oder Version 2 (bei lokaler Bereitstellung)

Code

Der Code für dieses Muster befindet sich im GitHub Repository Terraform EC2 Image Builder Container Hardening Pipeline . Um den Beispielcode zu verwenden, folgen Sie den Anweisungen im nächsten Abschnitt.

Polen

Bereitstellen der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie lokale Anmeldeinformationen ein.	Richten Sie Ihre temporären AWS-Anmeldeinformationen ein.
	1. Überprüfen Sie, ob die AWS CLI installiert ist:
	`$ aws --version aws-cli/1.16.249 Python/3.6.8...`
	• Die AWS CLI-Version sollte 1.1 oder höher sein.
	• Wenn der Befehl nicht gefunden wird, installieren Sie die AWS CLI .
	2. Führen Sie aus `aws configure` und geben Sie die folgenden Werte an:
	`$ aws configure AWS Access Key ID [**********xxxx]: <Your AWS access key ID>`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`AWS Secret Access Key [**********xxxx]: <Your AWS secret access key>`
	`Default region name: [us-east-1]: <Your desired Region for deployment>`
	`Default output format [None]: <Your desired output format>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	1. Klonen Sie das Repository, das mit diesem Muster bereitgestellt wird. Sie können HTTPS oder Secure Shell (SSH) verwenden.
	
	HTTPS:
	
	`git clone https://github.com/aws-samples/terraform-ec2-image-builder-container-hardening-pipeline`
	
	SSH:
	
	`git clone git@github.com:aws-samples/terraform-ec2-image-builder-container-hardening-pipeline.git`
	
	2. Navigieren Sie zu Ihrem lokalen Verzeichnis, das diese Lösung enthält:
	
	`cd terraform-ec2-image-builder-container-hardening-pipeline`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie Variablen.	Aktualisieren Sie die Variablen in der `hardening-pipeline.tfvars` Datei, damit sie Ihrer Umgebung und Ihrer gewünschten Konfiguration entsprech en. Sie müssen Ihr eigenes angeben`account_id` . Sie sollten jedoch auch die restlichen Variablen an die gewünschte Bereitstellung anpassen. Alle Variablen sind erforderlich.
	`account_id = "<DEPLOYMENT-ACCOUNT-ID>"`
	`aws_region = "us-east-1"`
	`vpc_name = "example-hardening-pipeline-vpc"`
	`kms_key_alias = "image-builder-con tainer-key"`
	`ec2_iam_role_name = "example-hardening-instance-role"`
	`hardening_pipeline_r ole_name = "example-hardening-pipeline-role"`
	`aws_s3_ami_resources _bucket = "example-hardening-ami-reso urces-bucket-0123"`
	`image_name = "example-hardening-al2-cont ainer-image"`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`ecr_name = "example-hardening-container-repo"`
	`recipe_version = "1.0.0"`
	`ebs_root_vol_size = 10`
	
	Im Folgenden finden Sie eine Beschreibung der einzelnen Variablen:
	
	• `account_id` Die AWS-Kontonummer, in der Sie die Lösung bereitstellen möchten.
	• `aws_region` Die AWS-Region, in der Sie die Lösung bereitstellen möchten.
	• `vpc_name` Der Name für Ihre VPC-Infrastruktur.
	• `kms_key_alias` Der AWS KMS-Schlüsselname, der von der EC2 Image Builder-Infrastrukturkonfiguration verwendet werden soll.
	• `ec2_iam_role_name` Der Name für die Rolle, die als EC2-Instance-Profil verwendet wird.
	• `hardening_pipeline_role_name` Der Name für die Rolle, die zur	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung der Hardening -Pipeline verwendet wird. • `aws_s3_ami_resources_bucket` Der Name für einen S3-Bucket, der alle Dateien hostet, die zum Erstellen der Pipeline- und Container-Images erforderlich sind. • `image_name` Der Name des Container-Images. Dieser Wert muss zwischen 3 und 50 Zeichen lang sein und darf nur alphanumerische Zeichen und Bindestriche enthalten. • `ecr_name` Der Name der Amazon-ECR-Registrierung, in der die Container-Images gespeichert werden sollen. • `recipe_version` Die Version des Image-Rezepts. Der Standardwert ist 1.0.0. • `ebs_root_vol_size` Die Größe des Amazon Elastic Block Store (Amazon EBS)-Root-Volumes (in Gigabyte). Der Standardwert ist 10 Gigabyte.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Terraform.	Nachdem Sie Ihre Variablen werte aktualisiert haben, können Sie das Terraform -Konfigurationsverzeichnis initialisieren. Durch die Initialisierung eines Konfigura tionsverzeichnisses wird der AWS-Anbieter herunterg eladen und installiert, der in der Konfiguration definiert ist. `terraform init` Sie sollten eine Meldung sehen, die besagt, dass Terraform erfolgreich initialis iert wurde und die installierte Version des Anbieters identifiz iert.	AWS DevOps
Stellen Sie die Infrastruktur bereit und erstellen Sie ein Container-Image.	Verwenden Sie den folgenden Befehl, um die Terraform-Module mithilfe der in Ihrer `-.tfvars`Datei definierten Variablen zu initialisieren, zu validieren und auf die Umgebung anzuwenden: `terraform init && terraform validate && terraform apply -var-file *.tfvars -auto-approve`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie den Container an.	Sie können eine neue Version eines Container-Rezepts erstellen, nachdem EC2 Image Builder die Pipeline und das ursprüngliche Rezept bereitgestellt hat. Sie können jede der mehr als 31 Komponenten hinzufüge n, die in EC2 Image Builder verfügbar sind, um den Container-Build anzupassen. Weitere Informationen finden Sie im Abschnitt Komponent en von Erstellen einer neuen Version eines Container-Rezepts in der EC2 Image Builder-Dokumentation.	AWS-Administrator

Validieren von Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitste llung der AWS-Infrastruktur.	Wenn Sie den ersten Terraform-`apply`Befehl erfolgreich abgeschlossen haben und lokal bereitste llen, sollte dieser Ausschnit t im Terminal Ihres lokalen Computers angezeigt werden: `Apply complete! Resources: 43 added, 0 changed, 0 destroyed.`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie einzelne AWS-Infrastrukturressourcen.	Um die einzelnen bereitgestellten Ressourcen zu validieren, können Sie bei lokaler Bereitstellung den folgenden Befehl ausführen: `terraform state list` Dieser Befehl gibt eine Liste von 43 Ressourcen zurück.	AWS DevOps

Entfernen von Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Infrastruktur und das Container-Image.	Wenn Sie mit der Arbeit mit Ihrer Terraform-Konfiguration fertig sind, können Sie den folgenden Befehl ausführen, um Ressourcen zu entfernen: `terraform init && terraform validate && terraform destroy -var-file *.tfvars -auto-approve`	AWS DevOps

Fehlerbehebung

Problem	Lösung
Fehler bei der Validierung der Anmeldeinformationen des Anbieters	Wenn Sie den Terraform-`apply`Befehl oder `destroy` von Ihrem lokalen Computer aus

Problem	Lösung
	ausführen, kann ein Fehler ähnlich dem folgenden auftreten: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Dieser Fehler wird durch den Ablauf des Sicherheitstokens für die Anmeldeinformationen verursacht, die in der Konfiguration Ihres lokalen Computers verwendet werden. Informationen zur Behebung des Fehlers finden Sie unter Festlegen und Anzeigen von Konfigurationseinstellungen in der AWS CLI-Dokumentation.

Zugehörige Ressourcen

- Terraform EC2 Image Builder Container Hardening Pipeline (GitHub Repository)
- EC2 Image Builder-Dokumentation
- AWS Control Tower Account Factory für Terraform (AWS-Blogbeitrag)
- S3-Bucket mit Backend-Status (Terraform-Dokumentation)
- Installieren oder Aktualisieren der neuesten Version der AWS CLI (AWS CLI-Dokumentation)
- Terraform herunterladen

Zentralisieren der IAM-Zugriffsschlüsselverwaltung in AWS Organizations mithilfe von Terraform

Erstellt von Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Pradip kumar Pandey (AWS), Mayuri Shinde (AWS) und Pratap Kumar N Bol (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Infrastruktur	AWS-Services: Amazon EventBridge; AWS Lambda ; AWS Organizations ; AWS Secrets Manager ; Amazon SES

Übersicht

Die Durchsetzung von Sicherheitsregeln für Schlüssel und Passwörter ist für jede Organisation eine wesentliche Aufgabe. Eine wichtige Regel besteht darin, AWS Identity and Access Management (IAM)-Schlüssel in regelmäßigen Abständen zu rotieren, um die Sicherheit zu erzwingen. AWS-Zugriffsschlüssel werden im Allgemeinen lokal erstellt und konfiguriert, wenn Teams über die AWS Command Line Interface (AWS CLI) oder von Anwendungen außerhalb von AWS auf AWS zugreifen möchten. Um eine hohe Sicherheit in der gesamten Organisation zu gewährleisten, müssen alte Sicherheitsschlüssel geändert oder gelöscht werden, nachdem die Anforderung erfüllt wurde oder in regelmäßigen Abständen. Die Verwaltung von Schlüsselrotationen über mehrere Konten in einer Organisation hinweg ist zeitaufwändig und mühsam. Dieses Muster hilft Ihnen, den Drehungsprozess mithilfe von Account Factory for Terraform (AFT) und AWS-Services zu automatisieren.

Das Muster bietet folgende Vorteile:

- Verwaltet Ihre Zugriffsschlüssel-IDs und geheimen Zugriffsschlüssel für alle Konten in Ihrer Organisation von einem zentralen Ort aus.
- Rotiert die `AWS_SECRET_ACCESS_KEY` Umgebungsvariablen `AWS_ACCESS_KEY_ID` und automatisch.
- Erzwingt die Verlängerung, wenn Benutzeranmeldeinformationen kompromittiert werden.

Das Muster verwendet Terraform, um AWS Lambda-Funktionen, Amazon- EventBridge Regeln und IAM-Rollen bereitzustellen. Eine - EventBridge Regel wird in regelmäßigen Abständen ausgeführt

und ruft eine Lambda-Funktion auf, die alle Benutzerzugriffsschlüssel basierend auf dem Zeitpunkt ihrer Erstellung auflistet. Zusätzliche Lambda-Funktionen erstellen eine neue Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel, wenn der vorherige Schlüssel älter als der von Ihnen definierte Drehungszeitraum ist (z. B. 45 Tage), und benachrichtigen einen Sicherheitsadministrator mithilfe von Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Email Service (Amazon SES). Secrets werden in AWS Secrets Manager für diesen Benutzer erstellt, der alte geheime Zugriffsschlüssel wird in Secrets Manager gespeichert und Berechtigungen für den Zugriff auf den alten Schlüssel werden konfiguriert. Um sicherzustellen, dass der alte Zugriffsschlüssel nicht mehr verwendet wird, wird er nach einem inaktiven Zeitraum deaktiviert (z. B. 60 Tage, was 15 Tage nach dem Rotieren der Schlüssel in unserem Beispiel dauern würde). Nach einer inaktiven Pufferphase (z. B. 90 Tage oder 45 Tage nach dem Rotieren der Schlüssel in unserem Beispiel) werden die alten Zugriffsschlüssel aus AWS Secrets Manager gelöscht. Eine detaillierte Architektur und einen detaillierten Workflow finden Sie im Abschnitt Architektur.

Voraussetzungen und Einschränkungen

- Eine Landing Zone für Ihre Organisation, die mit AWS Control Tower (Version 3.1 oder höher) erstellt wurde
- Account Factory for Terraform (AFT) ,konfiguriert mit drei Konten:
  - Das Verwaltungskonto der Organisation verwaltet die gesamte Organisation von einem zentralen Ort aus.
  - Das AFT-Verwaltungskonto hostet die Terraform-Pipeline und stellt die Infrastruktur im Bereitstellungskonto bereit.
  - Das Bereitstellungskonto stellt diese vollständige Lösung bereit und verwaltet IAM-Schlüssel von einem zentralen Ort aus.
- Terraform Version 0.15.0 oder höher für die Bereitstellung der Infrastruktur im Bereitstellungskonto.
- Eine E-Mail-Adresse, die in Amazon Simple Email Service (Amazon SES) konfiguriert ist.
- (Empfohlen) Stellen Sie diese Lösung in einem privaten Subnetz (Bereitstellungskonto) in einer Virtual Private Cloud (VPC) bereit, um die Sicherheit zu erhöhen. Sie können die Details der VPC und des Subnetzes angeben, wenn Sie die Variablen anpassen (siehe Parameter für die Code-Pipeline anpassen im Abschnitt „Epics“).

Architektur

AFT-Repositorys

Dieses Muster verwendet Account Factory for Terraform (AFT), um alle erforderlichen AWS-Ressourcen zu erstellen, und die Code-Pipeline, um die Ressourcen in einem Bereitstellungskonto bereitzustellen. Die Code-Pipeline wird in zwei Repositorys ausgeführt:

- Die globale Anpassung enthält Terraform-Code, der für alle bei AFT registrierten Konten ausgeführt wird.
- Kontoanpassungen enthalten Terraform-Code, der im Bereitstellungskonto ausgeführt wird.

Ressourcendetails

AWS- CodePipeline Aufträge erstellen die folgenden Ressourcen im Bereitstellungskonto:

- AWS- EventBridge Regel und konfigurierte Regel
- `account-inventory` Lambda-Funktion
- `IAM-access-key-rotation` Lambda-Funktion
- `Notification` Lambda-Funktion
- Amazon Simple Storage Service (Amazon S3)-Bucket, der eine E-Mail-Vorlage enthält
- Erforderliche IAM-Richtlinie

Architektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Eine - EventBridge Regel ruft die `account-inventory` Lambda-Funktion alle 24 Stunden auf.
2. Die `account-inventory` Lambda-Funktion fragt AWS Organizations nach einer Liste aller AWS-Konto-IDs , Kontonamen und Konto-E-Mails ab.
3. Die `account-inventory`Lambda-Funktion initiiert eine `IAM-access-key-auto-rotation` Lambda-Funktion für jedes AWS-Konto und übergibt die Metadaten zur zusätzlichen Verarbeitung an sie.
4. Die `IAM-access-key-auto-rotation` Lambda-Funktion verwendet eine angenommene IAM-Rolle, um auf das AWS-Konto zuzugreifen. Das Lambda-Skript führt eine Prüfung aller Benutzer und ihrer IAM-Zugriffsschlüssel im Konto durch.
5. Der Schwellenwert für die IAM-Schlüsselrotation (Rotationszeitraum) wird als Umgebungsvariable konfiguriert, wenn die `IAM-access-key-auto-rotation` Lambda-Funktion bereitgestellt

wird. Wenn der Drehungszeitraum geändert wird, wird die `IAM-access-key-auto-rotation` Lambda-Funktion mit einer aktualisierten Umgebungsvariablen erneut bereitgestellt. Sie können Parameter konfigurieren, um den Drehungszeitraum, den inaktiven Zeitraum für alte Schlüssel und den inaktiven Puffer festzulegen, nach dem alte Schlüssel gelöscht werden (siehe Parameter für die Code-Pipeline anpassen im Abschnitt „Epics“).

6. Die `IAM-access-key-auto-rotation` Lambda-Funktion validiert das Alter des Zugriffsschlüssels basierend auf seiner Konfiguration. Wenn das Alter des IAM-Zugriffsschlüssels den von Ihnen definierten Drehungszeitraum nicht überschritten hat, ergreift die Lambda-Funktion keine weiteren Maßnahmen.
7. Wenn das Alter des IAM-Zugriffsschlüssels den von Ihnen definierten Drehungszeitraum überschritten hat, erstellt die `IAM-access-key-auto-rotation` Lambda-Funktion einen neuen Schlüssel und rotiert den vorhandenen Schlüssel.
8. Die Lambda-Funktion speichert den alten Schlüssel in Secrets Manager und beschränkt die Berechtigungen auf den Benutzer, dessen Zugriffsschlüssel von den Sicherheitsstandards abweichen. Die Lambda-Funktion erstellt auch eine ressourcenbasierte Richtlinie, die nur dem angegebenen IAM-Prinzipal den Zugriff auf und das Abrufen des Secrets erlaubt.
9. Die `IAM-access-key-rotation` Lambda-Funktion ruft die `Notification` Lambda-Funktion auf.
10. Die `Notification` Lambda-Funktion fragt den S3-Bucket nach einer E-Mail-Vorlage ab und generiert dynamisch E-Mail-Nachrichten mit den relevanten Aktivitätsmetadaten.
11. Die `Notification` Lambda-Funktion ruft Amazon SES für weitere Aktionen auf.
12. Amazon SES sendet eine E-Mail mit den relevanten Informationen an die E-Mail-Adresse des Kontoinhabers.

Tools

AWS-Services

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist. Dieser Benutzer benötigt IAM-Rollen und -Berechtigungen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

- AWS Secrets Manager hilft Ihnen dabei, fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Secret programmgesteuert abzurufen.
- Amazon Simple Email Service (Amazon SES) hilft Ihnen beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domänen.

Andere Tools

- Terraform ist ein Infrastructure as Code (IaC HashiCorp)-Tool von , mit dem Sie Cloud- und On-Premises-Ressourcen erstellen und verwalten können.

Code-Repository

Die Anweisungen und der Code für dieses Muster sind im GitHub IAM-Zugriffsschlüssel-Rotations-Repository verfügbar. Sie können den Code im zentralen Bereitstellungskonto von AWS Control Tower bereitstellen, um die Schlüsselrotation von einem zentralen Ort aus zu verwalten.

Bewährte Methoden

- Informationen zu IAM finden Sie unter Bewährte Methoden für die Sicherheit in der IAM-Dokumentation.
- Informationen zur Schlüsselrotation finden Sie in den Richtlinien zum Aktualisieren von Zugriffsschlüsseln in der IAM-Dokumentation.

Sekunden

Einrichten von Quelldateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	1. Klonen Sie das IAM-Zugriffsschlüssel-Rotations GitHub -Repository: `$ git clone https://github.com/aws-samp`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`les/centralized-ia m-key-management-a ws-organizations-t erraform.git`
	2. Vergewissern Sie sich, dass Ihre lokale Kopie des Repositorys drei Ordner enthält:
	`$ cd Iam-Access-keys-Rotation`
	`$ ls`
	`org-account-cus tomization`
	`global-account-c ustomization`
	`account-custom ization`	

Konfigurieren Sie Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Bootstrapping-Konto.	Im Rahmen des AFT-Boots trapping-Prozesses sollten Sie einen Ordner namens `aft-bootstrap` auf Ihrem lokalen Computer haben. 1. Kopieren Sie alle Terraform -Dateien manuell aus Ihrem lokalen GitHub org-accou nt-customization Ordner in Ihren `aft-bootstrap` Ordner.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Führen Sie Terraform-Befehle aus, um die globale kontoübergreifende Rolle im AWS Control Tower-Verwaltungskonto zu konfigurieren:
	`$ cd aft-bootstrap`
	`$ terraform init`
	`$ terraform apply –auto-approve`	

Konfigurieren Sie globale Anpassungen.	Im Rahmen der AFT-Ordnereinrichtung sollte `aft-global-customizations` auf Ihrem lokalen Computer ein Ordner mit dem Namen vorhanden sein.
	1. Kopieren Sie manuell alle Terraform-Dateien aus Ihrem lokalen GitHub global-account-customization Ordner in Ihren `aft-global-customizations/terraform` Ordner.
	2. Übertragen Sie den Code an AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Kontoanpassungen.	Im Rahmen der AFT-Ordnereinrichtung sind Sie ein Ordner namens `aft-account-customizations` auf Ihrem lokalen Computer.
	1. Erstellen Sie einen Ordner mit Ihrer verkauften Kontonummer.
	2. Kopieren Sie manuell alle Terraform GitHub -Dateien aus Ihrem lokalen Ordner für die Kontoanpassung in Ihren `aft-account-customizations/<vended account>/terraform` Ordner.
	3. Übertragen Sie den Code an AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps Techniker

Anpassen der Parameter für die Code-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die Code-Pipeline-Parameter, die kein Terraform-Code sind, für alle Konten an.	Erstellen Sie eine Datei mit dem Namen `input.auto.tfvars` im `aft-global-customizations/terraform/` Ordner und	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	geben Sie die erforderlichen Eingabedaten an. Standardwerte finden Sie in der Datei im GitHub Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die Code-Pipeline-Parameter für das Bereitstellungskonto an.	Erstellen Sie eine Datei mit dem Namen `input.auto.tfvars` im `aft-account-customizations/<AccountName>/terraform/` Ordner und übertragen Sie den Code an AWS CodeCommit. Wenn Code an AWS übertragen wird, wird die Code-Pipeline CodeCommit automatisch initiiert. Geben Sie Werte für Parameter an, die auf den Anforderungen Ihrer Organisation basieren, einschließlich der folgenden (Standardwerte finden Sie in der Datei im Github-Repository): • `s3_bucket_name` – Ein eindeutiger Bucket-Name für die E-Mail-Vorlage. • `s3_bucket_prefix` – Ein Ordnername innerhalb des S3-Buckets. • `admin_email_address` – Die E-Mail-Adresse des Administrators, der die Benachrichtigung erhalten soll.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `org_list_account` – Die Kontonummer des Verwaltungskontos. • `rotation_period` – Die Anzahl der Tage, nach denen ein Schlüssel von aktiv zu inaktiv gedreht werden soll. • `inactive_period` – Die Anzahl der Tage, nach denen rotierte Schlüssel deaktiviert werden sollen. Dieser Wert muss größer als der Wert von sein`rotation_period` . • `inactive_buffer` – Die Übergangsfrist zwischen der Rotation und der Deaktivie rung eines Schlüssels. • `recovery_grace_per iod` – Die Übergangsfrist zwischen der Deaktivierung und dem Löschen eines Schlüssels. • `dry_run_flag` – Auf „true“ setzen, wenn Sie eine Benachrichtigung an den Administrator zu Testzweck en senden möchten, ohne die Schlüssel zu rotieren. • `store_secrets_in_c entral_account` – Auf „true“ setzen, wenn Sie das	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Secret im Bereitstellungskonto speichern möchten. Wenn die Variable auf „false“ (Standard) gesetzt ist, wird das Secret im Mitgliedskonto gespeichert. • `credential_replication_region` – Die AWS-Region, in der Sie die Lambda-Funktion und die S3-Buckets für die E-Mail-Vorlage bereitstellen möchten. • `run_lambda_in_vpc` – Legen Sie den Wert auf „true“ fest, um die Lambda-Funktion innerhalb der VPC auszuführen. • `vpc_id` – Die VPC-ID des Bereitstellungskontos, wenn Sie die Lambda-Funktion innerhalb der VPC ausführen möchten. • `vpc_cidr` – Der CIDR-Bereich für das Bereitstellungskonto. • `subnet_id` – Die Subnetz-IDs für das Bereitstellungskonto. • `create_smtp_endpoint` – Wird auf „true“ gesetzt, wenn Sie den E-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mail-Endpunkt aktivieren möchten.	

Validieren der Schlüsselrotation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Lösung.	1. Melden Sie sich über die AWS-Managementkonsole beim Bereitstellungskonto an. 2. Öffnen Sie die IAM-Konsole und überprüfen Sie, ob Benutzeranmeldeinformationen (Zugriffsschlüssel-IDs und geheime Schlüssel) wie angegeben rotiert werden. 3. Nachdem ein IAM-Schlüssel gedreht wurde, bestätigen Sie Folgendes: • Der alte Wert wird in AWS Secrets Manager gespeichert. • Der Secret-Name hat das Format `Account_<account ID>_User_<username>_AccessKey` . • Der Benutzer, den Sie im `admin_email_address` Parameter angegeben haben, erhält eine E-Mail-	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Benachrichtigung über die Schlüsselrotation.	

Erweitern der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Datum der E-Mail-Benachrichtigung an.	Wenn Sie E-Mail-Benachrichtigungen an einem bestimmten Tag senden möchten, bevor Sie den Zugriffsschlüssel deaktivieren, können Sie die `IAM-access-key-auto-rotation` Lambda-Funktion mit diesen Änderungen aktualisieren: 1. Definieren Sie eine Variable namens `notify-period` . 2. Fügen Sie eine `if` Bedingung in hinzu, `main.py` bevor Sie den Schlüssel deaktivieren: `If (keyage>rotation-period-notify-period){ send_to_notifier(context, aws_account_id, account_name, resource_owner, resource_actions[resource_owner], dryrun, config.emailTemplateAudit)`	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`}`	

Fehlerbehebung

Problem	Lösung
Der `account-inventory` Lambda-Auftrag schlägt `AccessDenied` beim Auflisten von Konten mit fehl.	Wenn dieses Problem auftritt, müssen Sie die Berechtigungen überprüfen: 1. Melden Sie sich beim neu angeboten en Konto an, öffnen Sie die Amazon-CloudWatch Konsole und zeigen Sie dann die CloudWatch Protokollgruppe an `/aws/lambda/account-inventory-lambda` . 2. Identifizieren Sie in den neuesten CloudWatc h Protokollen die Kontonummer, die das Problem der Zugriffsverweigerung verursach t. 3. Melden Sie sich beim AWS Control Tower-Verwaltungskonto an und bestätigen Sie, dass die Rolle erstellt `allow-list-account` wurde. 4. Wenn die Rolle nicht vorhanden ist, führen Sie den Terraform-Code mit dem `terraform apply` Befehl erneut aus. 5. Wählen Sie die Registerkarte Vertrauen swürdiges Konto und überprüfen Sie, ob dasselbe Konto vertrauenswürdig ist.

Zugehörige Ressourcen

- Empfohlene Methoden für Terraform (Terraform-Dokumentation)
- Bewährte Methoden für die Sicherheit in IAM (IAM-Dokumentation)
- Bewährte Methoden für die Schlüsselrotation (IAM-Dokumentation)

Zentralisierte Protokollierung und Sicherheitsleitplanken für mehrere Konten

Erstellt von Ankush Verma (AWS) und Tracy (Pierce) Hickey (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Management und Governance	AWS-Services: AWS CloudFormation; AWS Config ; Amazon CloudWatch; AWS CodePipeline; Amazon GuardDuty; AWS Lambda ; Amazon Macie ; AWS Security Hub; Amazon S3

Übersicht

Der in diesem Muster behandelte Ansatz eignet sich für Kunden, die über mehrere Amazon Web Services (AWS)-Konten bei AWS Organizations verfügen und jetzt auf Herausforderungen stoßen, wenn sie AWS Control Tower, eine Landing Zone oder Services für -Kontenverkaufsautomaten verwenden, um Basisleitplanken in ihren Konten einzurichten.

Dieses Muster zeigt die Verwendung einer optimierten Architektur mit mehreren Konten, um eine zentrale Protokollierung und standardisierte Sicherheitskontrollen auf gut strukturierte Weise einzurichten. Mithilfe von AWS- CloudFormation Vorlagen, AWS CodePipelineund Automatisierungsskripten wird diese Einrichtung in allen Konten bereitgestellt, die zu einer Organisation gehören.

Die Architektur mit mehreren Konten umfasst die folgenden Konten:

- Zentralisiertes Protokollierungskonto – Das Konto, in dem alle Virtual Private Cloud (VPC)-Flow-Protokolle, AWS- CloudTrail Protokolle, das AWS Config-Protokoll und alle Protokolle von Amazon CloudWatch Logs (mit Abonnements) aus allen anderen Konten gespeichert werden.
- Übergeordnetes Sicherheitskonto – Das Konto, das als übergeordnetes Konto für die folgenden Sicherheitsservices dient, die über mehrere Konten hinweg verwaltet werden.
  - Amazon GuardDuty
  - AWS Security Hub

  - Amazon Macie
  - Amazon Detective
- Untergeordnete Konten – Die anderen Konten in der Organisation. Diese Konten speichern alle nützlichen Protokolle im zentralen Protokollierungskonto. Die untergeordneten Konten treten dem übergeordneten Sicherheitskonto als Mitglieder der Sicherheitsservices bei.

Nachdem Sie die CloudFormation Vorlage (angefügt) gestartet haben, stellt sie drei Amazon Simple Storage Service (Amazon S3)-Buckets im zentralen Protokollierungskonto bereit. Ein Bucket wird verwendet, um alle AWS-bezogenen Protokolle (z. B. Protokolle aus VPC-Flow-Protokollen CloudTrailund AWS Config) aus allen Konten zu speichern. Der zweite Bucket dient zum Speichern der CloudFormation Vorlagen aus allen Konten. Der dritte Bucket dient zum Speichern von Amazon S3-Zugriffsprotokollen.

Eine separate CloudFormation Vorlage erstellt die Pipeline, die AWS verwendet CodeCommit. Nachdem der aktualisierte Code in das CodeCommit Repository übertragen wurde, kümmert er sich um das Starten von Ressourcen und das Einrichten von Sicherheitsservices in allen Konten. Weitere Informationen zur Dateistruktur der Dateien, die in das CodeCommit Repository hochgeladen werden, finden Sie in der Datei README.md (angefügt).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine AWS Organizations-Organisations-ID, wobei alle Konten derselben Organisation zugeordnet sind.
- Eine aktive E-Mail-Adresse für den Empfang von Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen.
- Bestätigte Kontingente für Amazon Simple Storage Service (Amazon S3)-Buckets in jedem Ihrer Konten. Standardmäßig hat jedes Konto 100 S3-Buckets. Wenn Sie zusätzliche Buckets benötigen, fordern Sie eine Kontingenterhöhung an, bevor Sie diese Lösung bereitstellen.

Einschränkungen

Alle Konten sollten Teil derselben Organisation sein. Wenn Sie AWS Organizations nicht verwenden, müssen Sie bestimmte Richtlinien ändern, z. B. die S3-Bucket-Richtlinie, um den Zugriff von den AWS Identity and Access Management (IAM)-Rollen für jedes Konto zu erlauben.

Hinweis: Während die Lösung bereitgestellt wird, müssen Sie das Amazon SNS-Abonnement bestätigen. Die Bestätigungsnachricht wird an die E-Mail-Adresse gesendet, die Sie während des Bereitstellungsprozesses angeben. Dadurch werden einige E-Mail-Warnmeldungen an diese E-Mail-Adresse ausgelöst, da diese Alarme jedes Mal ausgelöst werden, wenn IAM-Rollenrichtlinien im Konto erstellt oder geändert werden. Während des Bereitstellungsprozesses können Sie diese Warnmeldungen ignorieren.

Architektur

Zieltechnologie-Stack

- Amazon- CloudWatch Alarme und -Protokolle
- AWS- CodeCommit Repository
- AWS CodePipeline
- AWS Config
- Amazon Detective
- Amazon GuardDuty
- IAM-Rollen und -Berechtigungen
- Amazon Macie
- S3-Buckets
- AWS Security Hub
- Amazon SNS

Zielarchitektur

1. Andere Konten, die als untergeordnete Konten des übergeordneten Sicherheitskontos für die Sicherheitsservices registriert sind
2. Sicherheitserkenntnisse von allen untergeordneten Konten, einschließlich des übergeordneten Kontos

Ressourcen

Die folgenden Ressourcen werden automatisch bereitgestellt, wenn der aktualisierte Code in jedes Konto und jede AWS-Region in das CodeCommit Repository übertragen wird.

CloudFormation Stack 1 – Protokollieren des übergeordneten Stacks

– Verschachtelter Stack 1 – Standard-IAM-Rollen und -Richtlinien

– Verschachtelter Stack 2 – AWS Config-Einrichtung im Konto

– Verschachtelter Stack 3 – CloudWatch Alarme

- SecurityGroupChangesAlarm

- UnauthorizedAttemptAlarm

- RootActivityAlarm

- NetworkAclChangesAlarm

– IAMUserManagementAlarm

– IAMPolicyChangesAlarm

- CloudTrailChangeAlarm

– IAMCreateAccessKeyAlarm

– Metrikfilter zum Erstellen von Metriken aus CloudTrail Protokollen und deren Verwendung für Alarme

– SNS-Thema

CloudFormation Stack 2 – übergeordneter Integritätsschutz-Stack

– Verschachtelter Stack 1 – AWS Lambda-Funktion zum Einrichten der Kontopasswortrichtlinie

– Verschachtelter Stack 2 – Grundlegende AWS Config-Regeln

– CIS-SecurityGroupsMustRestrictSshTraffic

- OpenSecurityGroupRuleCheck zusammen mit der Lambda-Funktion für die Auswertung von Sicherheitsgruppenregeln

– check-ec2-for-required-tag

- check-for-unrestricted-ports

CloudFormation Stack 3 – CloudWatch Protokollexport

– Exportieren von CloudWatch Protokollen von Protokollgruppen nach Amazon S3 mithilfe eines Amazon Kinesis-Abonnements

Tools

- AWS CloudFormation – AWS CloudFormation verwendet -Vorlagen, um alle Ressourcen, die für Ihre Anwendungen in allen AWS-Regionen und -Konten benötigt werden, automatisiert und sicher zu modellieren und bereitzustellen.
- Amazon CloudWatch – Amazon CloudWatch überwacht Ihre AWS-Ressourcen und die Anwendungen, die Sie auf AWS ausführen, in Echtzeit. Sie können verwenden, CloudWatch um Metriken zu erfassen und zu verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können.
- AWS CodeCommit – AWS CodeCommit ist ein von AWS gehosteter Service zur Versionskontrolle. Sie können verwenden CodeCommit , um Komponenten (wie Dokumente, Quellcode und Binärdateien) privat in der Cloud zu speichern und zu verwalten.
- AWS CodePipeline – AWS CodePipeline ist ein kontinuierlicher Bereitstellungsservice, mit dem Sie die Schritte zur Veröffentlichung Ihrer Software modellieren, visualisieren und automatisieren können.
- AWS Config – AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.
- Amazon Detective – Amazon Detective wird verwendet, um die Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren. Detective sammelt automatisch Protokolldaten von Ihren AWS-Ressourcen. Anschließend werden Machine Learning, statistische Analysen und Diagrammtheorie verwendet, um Ihnen zu helfen, schnellere und effizientere Sicherheitsuntersuchungen zu visualisieren und durchzuführen.
- Amazon GuardDuty – Amazon GuardDuty ist ein Service zur kontinuierlichen Sicherheitsüberwachung, der Flow-Protokolle, CloudTrail Verwaltungsereignisprotokolle, CloudTrail Datenereignisprotokolle und DNS-Protokolle (Domain Name System) analysiert und verarbeitet. Er verwendet Bedrohungsdaten, z. B. Listen bösartiger IP-Adressen und Domänen, ebenso wie maschinelles Lernen, um unerwartete und potenziell nicht autorisierte bösartige Aktivitäten in Ihrer AWS-Umgebung zu identifizieren.

- AWS Identity and Access Management – AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- Amazon Macie – Amazon Macie automatisiert die Erkennung sensibler Daten wie persönlich identifizierbarer Informationen (PII) und Finanzdaten, um Ihnen ein besseres Verständnis der Daten zu bieten, die Ihre Organisation in Amazon S3 speichert.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- AWS Security Hub – AWS Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden zu überprüfen.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten (auch bekannt als Produzenten und Verbraucher) bereitstellt.

Polen

Schritt 1: Einrichten der IAM-Rollen in allen Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage Childaccount_IAM_role_All_Accounts.yaml, um die IAM-Rolle in der Region us-east-1 zu erstellen.	Um die erforderlichen IAM-Rollen und -Berechtigungen zu erstellen, müssen Sie diese Vorlage manuell in jedem Konto starten, nacheinander (zentralisiertes Protokollierungskonto, übergeordnetes Sicherheitskonto und alle anderen AWS-Konten in der Organisation) in der Region us-east-1. Die `Childaccount_IAM_role_All_Accounts.yaml` Vorlage	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	befindet sich im `-/templates/initial_deployment_templates` Verzeichnis des Pakets. Die IAM-Rolle wird verwendet, wenn API-Aufrufe für die Bereitstellung und Einrichtung des Rests der Architektur ausgeführt werden. Stellen Sie sicher, dass der Name der IAM-Rolle, die als Parameter übergeben wird, für alle Konten konsistent ist.	
Geben Sie in den Vorlagenparametern den Namen der IAM-Rolle an.	Geben Sie die IAM-Rolle an CodeBuild, die im übergeordneten Sicherheitskonto in allen anderen untergeordneten Konten übernehmen kann. Der Standardrollenname ist `security_execute_child_stack_role` .	Cloud-Architekt
Geben Sie in den Parametern die Konto-ID für das übergeordnete Sicherheitskonto an.	Das übergeordnete Sicherheitskonto ist das Konto, in dem CodeBuild ausgeführt wird.	Cloud-Architekt

Schritt 2: Einrichten von S3-Buckets im zentralen Protokollierungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie im zentralen Protokollierungskonto in us-east-1 die CloudFormation	Um die S3-Buckets im zentralen Protokollierungskonto zu erstellen, starten Sie die `S3Buckets-Centrali`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vorlage S3Buckets-Centrali zed -LoggingAccount.yaml.	`zed-LoggingAccount .yaml` . Die Vorlage befindet sich im `-/templates/ initial_deployme nt_templates` Verzeichn is des Pakets. Die S3-Bucket s speichern alle Protokolle, Vorlagen und Amazon S3-Zugriffsprotokolle. Notieren Sie sich alle S3-Bucket-Namen, mit denen Sie die Parameterdateien in den folgenden Schritten ändern.	
Geben Sie in den Vorlagenp arametern den Namen des S3-Buckets für den AWS-Protokollspeicher an.	Geben Sie einen Namen für den `S3 Bucket Name for Centralized Logging in Logging Account` Parameter ein. Dieser Bucket fungiert als zentraler Speicherort zum Speichern von AWS-Protokollen, z. B. Flow-Protokollen und CloudTrail Protokollen, von allen Konten aus. Notieren Sie sich sowohl den Bucket-Na men als auch den Amazon-Re ssourcennamen (ARN).	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen des S3-Buckets zum Speichern von Zugriffsprotokollen an.	Geben Sie einen S3-Bucket-Namen für den `S3 Bucket Name for Access Logs in Logging Account` Parameter ein. Dieser S3-Bucket speichert Zugriffsprotokolle für Amazon S3.	Cloud-Architekt
Geben Sie den Namen des S3-Buckets zum Speichern von Vorlagen an.	Geben Sie einen S3-Bucket-Namen in den `S3 Bucket Name for CloudFormation Template storage in Logging Account` Parameter ein.	Cloud-Architekt
Geben Sie die Organisations-ID an.	Um Zugriff auf S3-Buckets innerhalb der Organisation zu gewähren, geben Sie die ID für die Organisation im `Organization Id for Non-AMS accounts` Parameter ein.	Cloud-Architekt

Schritt 3: Bereitstellen der CI/CD-Infrastruktur im übergeordneten Sicherheitskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage security-guard-rails-codepipeline-CentralizedSecurityAccount.yml.	Um die CI/CD-Pipeline bereitzustellen, starten Sie die `security-guard-rails-codepipeline-CentralizedSecurityAccount.yml` Vorlage manuell im übergeordneten	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sicherheitskonto in us-east-1 . Die Vorlage befindet sich im `-/templates/initial_deployment_templates` Verzeichnis des Pakets. Diese Pipeline stellt die gesamte Infrastruktur in allen untergeordneten Konten bereit.	
Geben Sie einen Namen für den S3-Bucket an, der Vorlagen im zentralen Protokollierungskonto speichert.	Geben Sie den Namen des S3-Buckets ein, den Sie für den `S3 Bucket Name for the CloudFormation Template storage in Logging Account` Parameter in Schritt 2 angegeben haben.	Cloud-Architekt
Geben Sie den Namen der IAM-Rolle an, die in den untergeordneten Konten verwendet werden soll.	Geben Sie den Namen ein, den Sie für den `Name of the IAM role` Parameter in Schritt 1 angegeben haben.	Cloud-Architekt
Geben Sie eine aktive E-Mail-Adresse für den Empfang von CodePipeline Fehlerben achrichtigungen an.	Geben Sie die E-Mail-Adresse ein, die Sie für den Empfang von CodePipeline Fehlerben achrichtigungen und anderen CloudWatch Alarmbena chrichtigungen verwenden möchten.	Cloud-Architekt

Schritt 4: Aktualisieren von Dateien mit Kontoinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie Accountlist.json.	Fügen Sie der `Accountlist.json` Datei, die sich auf der obersten Ebene im Paket befindet, die übergeordnete Sicherheitskontonummer und die untergeordneten Kontonummern hinzu. Beachten Sie, dass das `ChildAccountList` Feld auch die übergeordnete Sicherheitskontonummer enthält. Sehen Sie sich das Beispiel in der `-deployment-instructions.md` Datei im -Paket an.	Cloud-Architekt
Ändern von accounts.csv	Fügen Sie in der `-accounts.csv` Datei, die sich auf der obersten Ebene im -Paket befindet, alle untergeordneten Konten zusammen mit der bei den Konten registrierten E-Mail hinzu. Sehen Sie sich das Beispiel in der `-deployment-instructions.md` Datei an.	Cloud-Architekt
Ändern Sie parameters.config.	Aktualisieren Sie in der `parameters.config` Datei , die sich im `/templates` Ordner befindet, die folgenden sechs Parameter:	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `pNotifyEmail` : Die E-Mail-Adresse, die Sie beim Einrichten der Pipeline angegeben haben (siehe Schritt 3) • `pstackNameLogging` : Der Name des CloudFormation Stacks für die zentrale Protokollierung • `pS3LogsBucket` : Der Name des S3-Buckets, in dem Protokolle von allen Konten gespeichert werden (siehe Schritt 2) • `pBucketName` : Der ARN für den S3-Bucket, der zum Speichern der Protokolle verwendet wird • `pTemplateBucketName` : Der Name der S3-Buckets, in denen Vorlagen gespeichert werden (siehe Schritt 2) • `pAllowedAccounts` : Konto-IDs für die übergeordneten und untergeordneten Konten Für die anderen Parameter können Sie die Standardwerte beibehalten. Ein Beispiel finden Sie in der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`-deployment-instruc tions.md` Datei im -Paket.	

Schritt 5: Zugriff auf das CodeCommit Repository und Übertragen der aktualisierten Dateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf das CodeCommit Repo zu, das Sie in Schritt 3 erstellt haben.	Notieren Sie sich im Abschnitt Outputs des CI/CD Infrastru cture CloudFormation Stacks (Start in Schritt 3) den Namen der CodeCommit Repositor y-URL. Erstellen Sie Zugriff auf das Repository, damit die Dateien dorthin übertragen werden können, damit die Infrastruktur in allen Zielkonte n bereitgestellt werden kann. Weitere Informationen finden Sie unter Einrichten von für AWS CodeCommit.	Cloud-Architekt
Übertragen Sie die Dateien in das CodeCommit Repository.	Installieren Sie Git auf Ihrem Computer. Führen Sie dann die Git-Befehle aus, um das leere Repository zu klonen, die Dateien von Ihrem Laptop in den Repository-Ordner zu kopieren und die Artefakte in das Repository zu verschieb en. Suchen Sie nach den Git-Beispielbefehlen in der `-deployment-instruc tions.md` Datei im -Paket. Grundlegende Git-Befeh	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	le finden Sie im Abschnitt Verwandte Ressourcen.	

Schritt 6: Bestätigen des CodeBuild Status CodePipeline und

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie den Status von CodePipeline und CodeBuild.	Nachdem Sie die Artefakte in das CodeCommit Repo übertragen haben, bestätige n Sie, dass die CodePipeline Pipeline, die Sie in Schritt 3 erstellt haben, initiiert wurde. Überprüfen Sie dann die CodeBuild Protokolle, um den Status oder die Fehler zu bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Bereitstellen von AWS- CloudFormation Vorlagen
- Einrichten von für AWS CodeCommit
- Hochladen von Dateien in den S3-Bucket
- Grundlegende Git-Befehle

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Suchen Sie in einer CloudFront Amazon-Distribution nach Zugriffsprotokollierung, HTTPS- und TLS-Version

Umgebung: Produktion	Technologien: Bereitstellung von Inhalten; Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon SNS; AWS; Amazon CloudForm ation CloudWatch; AWS Lambda		

Übersicht

Dieses Muster überprüft eine CloudFront Amazon-Distribution, um sicherzustellen, dass sie HTTPS verwendet, Transport Layer Security (TLS) Version 1.2 oder höher verwendet und die Zugriffsprotokollierung aktiviert ist. CloudFront ist ein von Amazon Web Services (AWS) bereitgestellter Service, der die Verteilung Ihrer statischen und dynamischen Webinhalte wie .html-, .css-, .js- und Bilddateien an Ihre Benutzer beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden. Wenn ein Benutzer Inhalte anfordert, die Sie bereitstellen CloudFront, wird die Anfrage an den Edge-Standort weitergeleitet, der die niedrigste Latenz (Zeitverzögerung) bietet, sodass der Inhalt mit der bestmöglichen Leistung bereitgestellt wird.

Dieses Muster stellt eine AWS-Lambda-Funktion bereit, die ausgelöst wird, wenn Amazon CloudWatch Events den CloudFront API-Aufruf CreateDistribution, CreateDistributionWithTags, oder UpdateDistributionerkennt. Die benutzerdefinierte Logik in der Lambda-Funktion wertet alle CloudFront Verteilungen aus, die im AWS-Konto erstellt oder aktualisiert wurden. Es sendet mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Benachrichtigung über Verstöße, wenn es die folgenden Verstöße feststellt:

- Globale Prüfungen:
  - Das benutzerdefinierte Zertifikat verwendet keine TLS-Version 1.2
  - Die Protokollierung ist für die Verteilung deaktiviert
- Herkunftsüberprüfungen:

  - Origin ist nicht mit TLS Version 1.2 konfiguriert
  - Die Kommunikation mit Origin ist über ein anderes Protokoll als HTTPS erlaubt
- Verhaltensprüfungen:
  - Kommunikation mit Standardverhalten ist auf einem anderen Protokoll als HTTPS zulässig
  - Kommunikation mit benutzerdefiniertem Verhalten ist in einem anderen Protokoll als HTTPS zulässig

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Benachrichtigungen über Verstöße erhalten möchten

Einschränkungen

- Diese Sicherheitskontrolle sucht nicht nach vorhandenen Cloudfront-Distributionen, es sei denn, die Distribution wurde aktualisiert.
- CloudFront gilt als globaler Service und ist nicht an eine bestimmte AWS-Region gebunden. Die CloudWatch Protokollierung von Amazon Logs und der AWS Cloudtrail API für globale Dienste erfolgt jedoch in der Region USA Ost (Nord-Virginia) (`us-east-1`). Daher CloudFront muss diese Sicherheitskontrolle für in `us-east-1` bereitgestellt und aufrechterhalten werden. Bei CloudFront dieser einzelnen Bereitstellung werden alle Distributionen auf überwacht. Stellen Sie die Sicherheitskontrolle nicht in anderen AWS-Regionen bereit. (Die Bereitstellung in anderen Regionen führt dazu, dass CloudWatch Ereignisse und die Lambda-Funktion nicht initiiert werden können und es werden keine SNS-Benachrichtigungen angezeigt.)
- Diese Lösung wurde umfangreichen Tests mit Distributionen von CloudFront Webinhalten unterzogen. Sie deckt keine RTMP-Streaming-Distributionen (Real-Time Messaging Protocol) ab.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- SNS-Thema

- EventBridge Amazon-Regel

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um die angehängte Vorlage für mehrere Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation — CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung von AWS-Ressourcen unterstützt, indem Infrastruktur als Code verwendet wird.
- Amazon EventBridge — EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services bereit und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambda — Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon SNS koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Der beigefügte Code beinhaltet:

- Eine ZIP-Datei, die den Lambda-Code enthält (index.py)
- Eine CloudFormation Vorlage (.yml-Datei), die Sie ausführen, um den Lambda-Code bereitzustellen

Epen

Laden Sie die Sicherheitskontrolle hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket für den Lambda-Code.	Erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konte n gemeinsam genutzt. Ihr S3-Bucket muss sich in der Region befinden, in der Sie den Lambda-Code bereitste llen möchten.	Cloud-Architekt
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den Lambda-Co de (Datei cloudfront_ssl_log _lambda.zip), der im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch, den Sie im vorherigen Schritt erstellt haben.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudForm ation Vorlage bereit.	Stellen Sie auf der CloudForm ation AWS-Konsole, in derselben AWS-Region wie der S3-Bucket, die CloudForm ation Vorlage (cloudfront-ssl-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	logging.yml) bereit, die im Abschnitt Anlagen bereitgestellt wird.	
Geben Sie den S3-Bucket-Namen an.	Geben Sie für den S3-Bucket-Parameter den Namen des S3-Buckets an, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie den Amazon S3 S3-Schlüsselnamen für die Lambda-Datei an.	Geben Sie für den Parameter S3 Key den Amazon S3 S3-Speicherort der Lambda-Code-.zip-Datei in Ihrem S3-Bucket an. Fügen Sie keine führenden Schrägstriche ein (Sie können beispielsweise lambda.zip oder controls/lambda.zip eingeben).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse für Benachrichtigungen an.	Geben Sie für den Parameter Benachrichtigungs-E-Mail eine E-Mail-Adresse an, an die Sie die Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Protokollierungsebene.	Definieren Sie für den Parameter Lambda Logging Level den Logging-Level für Ihre Lambda-Funktion. Wählen Sie einen der folgenden Werte aus: • INFO, um detaillierte Informationsmeldungen über den Fortschritt der Anwendung zu erhalten. • ERROR, um Informationen über Fehlerereignisse abzurufen, die dazu führen könnten, dass die Anwendung weiterhin ausgeführt werden kann. • WARNUNG, um Informationen über potenziell schädliche Situationen zu erhalten.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, wird ein neues SNS-Thema erstellt und eine Abonnementnachricht an die von Ihnen angegebene E-Mail-Adresse gesendet. Sie müssen dieses E-Mail-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- CloudFormation AWS-Informationen
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation Dokumentation)
- CloudFront Protokollierung (CloudFront Dokumentation)
- Informationen zu Amazon S3
- Informationen zu AWS Lambda

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Suchen Sie nach Netzwerkeinträgen mit einem Host in den Eingangsregeln für Sicherheitsgruppen für IPv4 und IPv6

Erstellt von SaiJeevan Devireddy (AWS), Ganesh Kumar (AWS) und John Reynolds (AWS)

Umgebung: Produktion	Technologien: Netzwerk, Sicherheit, Identität, Compliance	AWS-Services: Amazon SNS ; AWS CloudFormation; Amazon CloudWatch; AWS Lambda ; Amazon VPC

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die Sie benachrichtigt, wenn Amazon Web Services (AWS)-Ressourcen nicht Ihren Spezifikationen entsprechen. Sie bietet eine AWS Lambda-Funktion, die sowohl in den Feldern Internet Protocol Version 4 (IPv4) als auch in der Quelladresse der IPv6-Sicherheitsgruppe nach Netzwerkeinträgen mit einem Host sucht. Die Lambda-Funktion wird initiiert, wenn Amazon CloudWatch Events den Amazon Elastic Compute Cloud (Amazon EC2)AuthorizeSecurityGroupIngress-API-Aufruf erkennt. Die benutzerdefinierte Logik in der Lambda-Funktion wertet die Subnetzmaske des CIDR-Blocks der Sicherheitsgruppenregel für eingehenden Datenverkehr aus. Wenn festgestellt wird, dass die Subnetzmaske etwas anderes als /32 (IPv4) oder /128 (IPv6) ist, sendet die Lambda-Funktion mithilfe des Amazon Simple Notification Service (Amazon SNS) eine Benachrichtigung über Verstöße.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Benachrichtigungen über Verstöße erhalten möchten

Einschränkungen

- Diese Sicherheitsüberwachungslösung ist regional und muss in jeder AWS-Region bereitgestellt werden, die Sie überwachen möchten.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- SNS-Thema
- Amazon- EventBridge Regel

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage für mehrere Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung von AWS-Ressourcen unterstützt, indem Infrastruktur als Code verwendet wird.
- Amazon EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software as a Service (SaaS)-Anwendungen und AWS-Services bereit und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambda unterstützt das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Der angehängte Code umfasst:

- Eine ZIP-Datei, die den Lambda-Sicherheitskontrollcode (`index.py`) enthält
- Eine CloudFormation Vorlage (`security-control.yml`-Datei), die Sie ausführen, um den Lambda-Code bereitzustellen

Polen

Hochladen der Sicherheitskontrolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket für den Lambda-Code.	Erstellen Sie in der Amazon S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in der AWS-Region befinden, in der Sie die Eingangsprüfung der Sicherheitsgruppe bereitstellen möchten.	Cloud-Architekt
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den Lambda-Code (`security-control-lambda.zip`-Datei), der im Abschnitt Anhänge bereitgestellt wird, in den S3-Bucket hoch, den Sie im vorherigen Schritt erstellt haben.	Cloud-Architekt

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Python-Version.	Laden Sie die CloudFormation Vorlage (`security-control.yml`) herunter, die im Abschnitt Anhänge bereitgestellt wird. Öffnen Sie die Datei und ändern Sie die Python-Version so, dass sie der neuesten Version entspricht, die von Lambda unterstützt wird (aktuell Python 3.9). Sie können beispielsweise `python` im Code nach suchen und den Wert für `Runtime` von `python3.6` in ändern`python3.9` . Die neuesten Informationen zur Unterstützung der Python-Laufzeitversion finden Sie in der AWS Lambda-Dokumentation.	Cloud-Architekt
Stellen Sie die AWS-CloudFormation Vorlage bereit.	Stellen Sie in der AWS-CloudFormation Konsole in derselben AWS-Region wie der S3-Bucket die CloudFormation Vorlage bereit (`security-control.yml`).	Cloud-Architekt
Geben Sie den Namen des S3-Buckets an.	Geben Sie für den S3-Bucket -Parameter den Namen des	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S3-Buckets an, den Sie im ersten Epi erstellt haben.	
Geben Sie den Amazon S3-Schlüsselnamen für die Lambda-Datei an.	Geben Sie für den Parameter S3 Key den Amazon S3-Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket an. Fügen Sie keine führenden Schrägstr iche ein (Sie können beispiels weise `lambda.zip` oder eingeben`controls/lambda.zip`).	Cloud-Architekt
Geben Sie eine E-Mail-Ad resse für Benachrichtigungen an.	Geben Sie für den Parameter E-Mail-Benachrichtigung eine E-Mail-Adresse an, an die Sie die Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Protokollierungsebene.	Definieren Sie für den Parameter Lambda-Protokollierungsebene die Protokollierungsebene für Ihre Lambda-Funktion. Wählen Sie einen der folgenden Werte aus: • INFO, um detaillierte Informationsmeldungen über den Fortschritt der Anwendung zu erhalten. • FEHLER, um Informationen zu Fehlerereignissen zu erhalten, die der Anwendung weiterhin die Ausführung ermöglichen könnten. • WARNUNG, um Informationen über potenziell schädliche Situationen zu erhalten.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, wird ein neues SNS-Thema erstellt und eine Abonnementnachricht an die von Ihnen angegebene E-Mail-Adresse gesendet.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- AWS- CloudFormation Informationen
- Erstellen eines Stacks in der AWS CloudFormation -Konsole (AWS- CloudFormation Dokumentation)
- Sicherheitsgruppen für Ihre VPC (Amazon-VPC-Dokumentation)
- Amazon S3-Informationen
- AWS Lambda-Informationen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Wählen Sie einen Amazon Cognito Cognito-Authentifizierungsablauf für Unternehmensanwendungen

Erstellt von Michael Daehnert (AWS) und Fabian Jahnke (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance	AWS-Dienste: Amazon Cognito

Übersicht

Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und Mobilanwendungen. Es bietet nützliche Funktionen für die Authentifizierung von föderierten Identitäten. Um es zum Laufen zu bringen, müssen technische Architekten entscheiden, wie sie diese Funktionen verwenden möchten.

Amazon Cognito unterstützt mehrere Abläufe für Authentifizierungsanfragen. Diese Abläufe definieren, wie Ihre Benutzer ihre Identität überprüfen können. Die Entscheidung, welcher Authentifizierungsablauf verwendet werden soll, hängt von den spezifischen Anforderungen Ihrer Anwendung ab und kann komplex werden. Dieses Muster hilft Ihnen bei der Entscheidung, welcher Authentifizierungsablauf für Ihre Unternehmensanwendung am besten geeignet ist. Es wird davon ausgegangen, dass Sie bereits über Grundkenntnisse in Amazon Cognito, OpenID Connect (OIDC) und Federation verfügen, und führt Sie durch Einzelheiten zu den verschiedenen föderierten Authentifizierungsabläufen.

Diese Lösung richtet sich an technische Entscheidungsträger. Sie hilft Ihnen dabei, die verschiedenen Authentifizierungsabläufe zu verstehen und sie Ihren Anwendungsanforderungen zuzuordnen. Technische Leiter sollten die erforderlichen Erkenntnisse sammeln, um die Amazon Cognito Cognito-Integrationen zu starten. Da sich Unternehmensorganisationen hauptsächlich auf den SAML-Verbund konzentrieren, enthält dieses Muster Beschreibungen für Amazon Cognito Cognito-Benutzerpools mit SAML-Föderation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Rollen und Berechtigungen von AWS Identity and Access Management (IAM) mit vollem Zugriff auf Amazon Cognito
- (Optional) Zugriff auf Ihren Identitätsanbieter (IdP), z. B. Microsoft Entra ID, Active Directory Federation Service (AD FS) oder Okta
- Ein hohes Maß an Fachwissen für Ihre Anwendung
- Grundkenntnisse in Amazon Cognito, OpenID Connect (OIDC) und Federation

Einschränkungen

- Dieses Muster konzentriert sich auf Amazon Cognito Cognito-Benutzerpools und Identitätsanbieter. Informationen zu Amazon Cognito Cognito-Identitätspools finden Sie im Abschnitt Zusätzliche Informationen.

Architektur

Verwenden Sie die folgende Tabelle, um Ihnen bei der Auswahl eines Authentifizierungsablaufs zu helfen. Weitere Informationen zu den einzelnen Datenströmen finden Sie in diesem Abschnitt.

Benötigen Sie eine machine-to-machine Authentifizierung?	Ist Ihre App eine webbasierte Anwendung, bei der das Frontend auf dem Server gerendert wird?	Handelt es sich bei Ihrer App um eine einseitige Anwendung (SPA) oder um eine Frontend-Anwendung auf Mobilgeräten?	Benötigt Ihre Anwendung Aktualisierungstoken für die Funktion „Ich möchte angemeldet bleiben“?	Bietet das Frontend einen browserbasierten Umleitungsmechanismus?	Empfohlener Amazon Cognito Cognito-Flow
Ja	Nein	Nein	Nein	Nein	Ablauf der Kundenanmeldedaten

Nein	Ja	Nein	Ja	Ja	Ablauf des Autorisierungscodes
Nein	Nein	Ja	Ja	Ja	Ablauf des Autorisierungscodes mit Proof Key for Code Exchange (PKCE)
Nein	Nein	Nein	Nein	Nein	Passwortfluss für Ressourceneigentümer*

* Der Passwortfluss für den Ressourcenbesitzer sollte nur verwendet werden, wenn dies unbedingt erforderlich ist. Weitere Informationen finden Sie im Abschnitt „Passwortfluss für Ressourcenbesitzer“ in diesem Muster.

Ablauf der Kundenanmeldedaten

Der Client Credentials Flow ist der kürzeste der Amazon Cognito Cognito-Flows. Er sollte verwendet werden, wenn Systeme oder Dienste ohne Benutzerinteraktion miteinander kommunizieren. Das anfragende System verwendet die Client-ID und das Client-Geheimnis, um ein Zugriffstoken abzurufen. Da beide Systeme ohne Benutzerinteraktion funktionieren, ist kein zusätzlicher Zustimmungsschritt erforderlich.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Anwendung 1 sendet eine Authentifizierungsanfrage mit der Client-ID und dem geheimen Client-Schlüssel an den Amazon Cognito Cognito-Endpunkt und ruft ein Zugriffstoken ab.
2. Anwendung 1 verwendet dieses Zugriffstoken für jeden nachfolgenden Aufruf von Anwendung 2.
3. Anwendung 2 validiert das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Für die Kommunikation zwischen Anwendungen ohne Benutzerinteraktion

Dieser Ablauf sollte nicht verwendet werden:

- Für jede Kommunikation, bei der Benutzerinteraktionen möglich sind

Ablauf des Autorisierungscodes

Der Ablauf des Autorisierungscodes dient der klassischen webbasierten Authentifizierung. In diesem Ablauf kümmert sich das Backend um den gesamten Austausch und die Speicherung von Token. Der browserbasierte Client sieht die tatsächlichen Token nicht. Diese Lösung wird für Anwendungen verwendet, die in Frameworks wie.NET Core, Jakarta Faces oder Jakarta Server Pages (JSP) geschrieben wurden.

Der Autorisierungscodefluss ist ein Fluss, der auf Umleitungen basiert. Der Client muss in der Lage sein, mit dem Webbrowser oder einem ähnlichen Client zu interagieren. Der Client wird zu einem Authentifizierungsserver umgeleitet und authentifiziert sich bei diesem Server. Wenn sich der Client erfolgreich authentifiziert, wird er zurück zum Server umgeleitet.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Der Client sendet eine Anfrage an den Webserver.
2. Der Webserver leitet den Client mithilfe eines HTTP 302-Statuscodes zu Amazon Cognito weiter. Der Client folgt automatisch dieser Weiterleitung zum konfigurierten IdP-Login.
3. Der IdP sucht nach einer bestehenden Browsersitzung auf der IdP-Seite. Wenn keine vorhanden ist, wird der Benutzer aufgefordert, sich zu authentifizieren, indem er seinen Benutzernamen und sein Passwort eingibt. Der IdP antwortet mit einem SAML-Token auf Amazon Cognito.
4. Amazon Cognito meldet Erfolg mit einem JSON-Webtoken (JWT), insbesondere einem Code-Token. Der Webserver ruft /oauth2/token auf, um das Code-Token gegen ein Zugriffstoken auszutauschen. Der Webserver sendet die Client-ID und das Client-Geheimnis zur Überprüfung an Amazon Cognito.
5. Das Zugriffstoken wird für jeden nachfolgenden Aufruf anderer Anwendungen verwendet.
6. Andere Anwendungen validieren das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Wenn der Benutzer mit dem Webbrowser oder Client interagieren kann. Der Anwendungscode wird auf dem Server ausgeführt und gerendert, um sicherzustellen, dass dem Browser keine Geheimnisse offengelegt werden.

Dieser Ablauf sollte nicht verwendet werden:

- Für Single-Page-Anwendungen (SPAs) oder mobile Apps, da sie auf dem Client gerendert werden und keine Client-Geheimnisse verwenden sollten.

Ablauf des Autorisierungscodes mit PKCE

Der Autorisierungscodefluss mit Proof Key for Code Exchange (PKCE) sollte für einseitige Anwendungen und mobile Anwendungen verwendet werden. Er ist der Nachfolger des impliziten Ablaufs und ist sicherer, da er PKCE verwendet. PKCE ist eine Erweiterung des OAuth 2.0-Autorisierungscodes, der öffentlichen Kunden gewährt wird. PKCE schützt vor der Rücknahme abgefangener Autorisierungscodes.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Die Anwendung erstellt einen Code-Verifier und eine Code-Challenge. Dies sind klar definierte, eindeutige Werte, die zur future Verwendung an Amazon Cognito gesendet werden.
2. Die Anwendung ruft den Endpunkt /oauth2/authorization von Amazon Cognito auf. Es leitet den Benutzer automatisch zum konfigurierten IdP-Login weiter.
3. Der IdP sucht nach einer bestehenden Sitzung. Wenn keine vorhanden ist, wird der Benutzer aufgefordert, sich zu authentifizieren, indem er seinen Benutzernamen und sein Passwort eingibt. Der IdP antwortet mit einem SAML-Token auf Amazon Cognito.
4. Nachdem Amazon Cognito den Erfolg mit einem Code-Token zurückgibt, ruft der Webserver / oauth2/token auf, um das Code-Token gegen ein Zugriffstoken auszutauschen.
5. Das Zugriffstoken wird für jeden nachfolgenden Aufruf anderer Anwendungen verwendet.
6. Die anderen Anwendungen validieren das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Für SPAs oder mobile Anwendungen

Dieser Flow sollte nicht verwendet werden:

- Wenn das Anwendungs-Backend die Authentifizierung abwickelt

Ablauf des Kennworts des Ressourcenbesitzers

Der Passwortfluss für den Ressourcenbesitzer ist für Anwendungen ohne Umleitungsfunktionen vorgesehen. Er wird erstellt, indem Sie ein Anmeldeformular in Ihrer eigenen Anwendung erstellen. Die Anmeldung wird auf Amazon Cognito über einen CLI- oder SDK-Aufruf überprüft, anstatt sich auf Umleitungsflüsse zu verlassen. Ein Verbund ist in diesem Authentifizierungsablauf nicht möglich, da für den Verbund browserbasierte Weiterleitungen erforderlich sind.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Der Benutzer gibt seine Anmeldeinformationen in ein von der Anwendung bereitgestelltes Anmeldeformular ein.
2. Die AWS-Befehlszeilenschnittstelle (AWS CLI) admin-initiated-authruft Amazon Cognito auf.

   Hinweis: Alternativ können Sie AWS-SDKs anstelle der AWS-CLI verwenden.
3. Amazon Cognito gibt ein Zugriffstoken zurück.
4. Das Zugriffstoken wird für jeden nachfolgenden Aufruf anderer Anwendungen verwendet.
5. Die anderen Anwendungen validieren das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Bei der Migration vorhandener Clients, die direkte Authentifizierungslogik verwenden (z. B. Standardzugriffsauthentifizierung oder Digest-Zugriffsauthentifizierung), zu OAuth, indem die gespeicherten Anmeldeinformationen in ein Zugriffstoken konvertiert werden

Dieser Ablauf sollte nicht verwendet werden:

- Wenn Sie föderierte Identitäten verwenden möchten
- Wenn Ihre Anwendung Weiterleitungen unterstützt

Tools

AWS-Services

- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.

Andere Tools

- Der JSON-Web-Token-Debugger (JWT) ist ein webbasiertes JWT-Validierungstool.

Epen

Beurteilen Sie Ihre Bewerbung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Authentifizierungsanforderungen.	Beurteilen Sie Ihre Anwendung anhand Ihrer spezifischen Authentifizierungsanforderungen.	App-Entwickler, App-Architekt
Passen Sie die Anforderungen an die Authentifizierungsabläufe an.	Verwenden Sie im Abschnitt Architektur die Entscheidungstabelle und die Erläuterungen der einzelnen Abläufe, um Ihren Amazon Cognito Cognito-Authentifizierungsablauf auszuwählen.	App-Entwickler, General AWS, App-Architekt

Den Amazon Cognito Cognito-Benutzerpool einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzerpool.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Cognito Cognito-Konsole. 2. Erstellen Sie einen neuen Cognito-Benutzerpool. Anweisungen finden Sie unter Amazon Cognito Cognito-Benutzerpools. 3. Aktualisieren Sie die Einstellungen und Attribute des Benutzerpools nach Bedarf. Legen Sie beispielsweise eine Kennwortrichtlinie für den Benutzerpool fest. Erstellen Sie noch keine App-Clients.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Konfigurieren Sie einen Identitätsanbieter.	1. Erstellen Sie einen SAML-Identitätsanbieter im Amazon Cognito Cognito-Benutzerpool. Anweisungen finden Sie unter Hinzufügen und Verwalten von SAML-Identitätsanbietern in einem Benutzerpool. 2. Konfigurieren Sie Ihren externen SAML-Identitätsanbieter so, dass er mit dem Verbund für Amazon Cognito Cognito-Benutzerpools funktioniert. Weitere Informationen finden Sie unter Konfiguration Ihres externen SAML-Identitätsanbieters. Wenn Sie AD FS verwenden, finden Sie weitere Informationen unter Aufbau eines AD FS-Verbunds für Ihre Web-App mithilfe von Amazon Cognito Cognito-Benutzerpools (AWS-Blogbeitrag).	Allgemeiner AWS, Verbundadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen App-Client.	1. Erstellen Sie einen App-Client für den Benutzerpool. Anweisungen finden Sie unter Einen App-Client erstellen. Beachten Sie Folgendes: • Ändern Sie die Einstellungen nach Bedarf, z. B. die Ablaufzeiten von Tokens. • Wenn für Ihren Authentifizierungsablauf kein Client-Geheimnis erforderlich ist, deaktivieren Sie das Kontrollkästchen Clientgeheimnis generieren. 2. Wählen Sie App-Client-Einstellungen, um die Integration in eine Benutzerpool-Anmeldung (Benutzername und Passwort) oder eine Verbundanmeldung über einen SAML-basierten IdP zu ändern. 3. Aktivieren Sie Ihren IdP, indem Sie nach Bedarf URLs und OAuth-Flows oder -Bereiche definieren.	Allgemeines AWS

Integrieren Sie die Anwendung in Amazon Cognito

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Details zur Exchange Amazon Cognito Cognito-Integration.	Teilen Sie je nach Ihrem Authentifizierungsablauf Amazon Cognito Cognito-Informationen mit der Anwendung, z. B. die Benutzerpool-ID und die App-Client-ID.	App-Entwickler, General AWS
Implementieren Sie die Amazon Cognito Cognito-Authentifizierung.	Dies hängt von Ihrem ausgewählten Authentifizierungsablauf, Ihrer Programmiersprache und den von Ihnen verwendeten Frameworks ab. Einige Links für den Einstieg finden Sie im Abschnitt Verwandte Ressourcen.	App-Developer

Zugehörige Ressourcen

AWS-Dokumentation

- Ablauf der Benutzerpool-Authentifizierung
- Überprüfen eines JSON-Web-Tokens
- Greifen Sie über eine ASP.NET Core-App mithilfe von Amazon Cognito Cognito-Identitätspools auf AWS-Services zu
- Frameworks und SDKs:
  - Amazon Amplify-Authentifizierung
  - Beispiele für Amazon Cognito Identity Provider (Dokumentation zum AWS SDK for Java 2.x)
  - Authentifizierung von Benutzern mit Amazon Cognito (AWS SDK for .NET .NET-Dokumentation)

AWS-Blogbeiträge

- Authorization @Edge mithilfe von Cookies: Schützen Sie Ihre CloudFront Amazon-Inhalte davor, von nicht authentifizierten Benutzern heruntergeladen zu werden
- Aufbau eines AD FS-Verbunds für Ihre Web-App mithilfe von Amazon Cognito Cognito-Benutzerpools

Implementierungspartner

- AWS-Partner für Authentifizierungslösungen

Zusätzliche Informationen

HÄUFIG GESTELLTE FRAGEN

Warum ist der implizite Flow veraltet?

Seit der Veröffentlichung des OAuth 2.1-Frameworks ist der Implicit Flow aus Sicherheitsgründen als veraltet markiert. Als Alternative verwenden Sie bitte den Autorisierungscodefluss mit PKCE, der im Abschnitt Architektur beschrieben ist.

Was ist, wenn Amazon Cognito einige Funktionen, die ich benötige, nicht bietet?

AWS-Partner bieten verschiedene Integrationen für Authentifizierungs- und Autorisierungslösungen an. Weitere Informationen finden Sie unter AWS-Partner für Authentifizierungslösungen.

Was ist mit Amazon Cognito Cognito-Identitätspool-Flows?

Amazon Cognito Cognito-Benutzerpools und föderierte Identitäten dienen der Authentifizierung. Amazon Cognito Cognito-Identitätspools werden für die Autorisierung des Zugriffs auf AWS-Ressourcen verwendet, indem temporäre AWS-Anmeldeinformationen angefordert werden. Der Austausch von ID-Token und Zugriffstoken für Identitätspools wird in diesem Muster nicht behandelt. Weitere Informationen finden Sie unter Was ist der Unterschied zwischen Amazon Cognito-Benutzerpools und Identitätspools und Allgemeine Amazon Cognito-Szenarien.

Nächste Schritte

Dieses Muster bietet einen Überblick über die Amazon Cognito Cognito-Authentifizierungsabläufe. Als nächster Schritt muss die detaillierte Implementierung für die Programmiersprache der

Anwendung ausgewählt werden. Mehrere Sprachen bieten SDKs und Frameworks, die Sie mit Amazon Cognito verwenden können. Hilfreiche Referenzen finden Sie im Abschnitt Verwandte Ressourcen.

Erstellen Sie benutzerdefinierte AWS Config-Regeln mithilfe von AWS CloudFormation Guard-Richtlinien

Quellcode-Repository: aws-config-custom-rule-cloudformation-guard	Umgebung: PoC oder Pilot	Technologien: Sicherheit, Identität, Compliance; Management und Unternehmensführung
AWS-Dienste: AWS CloudFormation; AWS Config		

Übersicht

AWS Config-Regeln helfen Ihnen dabei, Ihre AWS-Ressourcen und ihren Zielkonfigurationsstatus zu bewerten. Es gibt zwei Arten von AWS Config-Regeln: verwaltete und benutzerdefinierte. Sie können benutzerdefinierte Regeln mit AWS Lambda Lambda-Funktionen oder mit AWS CloudFormation Guard (GitHub), einer policy-as-code Sprache, erstellen.

Mit Guard erstellte Regeln bieten eine detailliertere Steuerung als verwaltete Regeln und sind in der Regel einfacher zu konfigurieren als vollständig benutzerdefinierte Lambda-Regeln. Dieser Ansatz bietet Ingenieuren und Architekten die Möglichkeit, Regeln zu erstellen, ohne Python, NodeJS oder Java kennen zu müssen, die für die Bereitstellung benutzerdefinierter Regeln über Lamdba erforderlich sind.

Dieses Muster bietet praktikable Vorlagen, Codebeispiele und Bereitstellungsansätze, die Sie bei der Einführung benutzerdefinierter Regeln mit Guard unterstützen. Mithilfe dieses Musters kann ein Administrator mithilfe von AWS Config benutzerdefinierte Compliance-Regeln mit Attributen für Konfigurationselemente erstellen. Entwickler können beispielsweise Guard-Richtlinien für AWS Config-Konfigurationselemente verwenden, um den Status bereitgestellter AWS- und Nicht-AWS-Ressourcen kontinuierlich zu überwachen, Regelverstöße zu erkennen und automatisch Abhilfemaßnahmen einzuleiten.

Ziele

Nachdem Sie dieses Muster gelesen haben, sollten Sie in der Lage sein:

- Erfahren Sie, wie der Guard-Richtliniencode mit dem AWS Config-Service interagiert.
- Stellen Sie Szenario 1 bereit, eine benutzerdefinierte AWS Config-Regel, die die Guard-Syntax verwendet, um die Konformität für verschlüsselte Volumes zu überprüfen. Diese Regel überprüft, ob das Laufwerk verwendet wird, und stellt sicher, dass der Laufwerkstyp gp3 ist.
- Stellen Sie Szenario 2 bereit, eine benutzerdefinierte AWS Config-Regel, die die Guard-Syntax verwendet, um die GuardDuty Amazon-Konformität zu überprüfen. Diese Regel überprüft, ob bei GuardDuty Rekordern Amazon S3 S3-Schutz und Amazon EKS-Schutz aktiviert sind.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Config, in Ihrem AWS-Konto eingerichtet

Einschränkungen

- Benutzerdefinierte Guard-Regeln können nur Schlüssel-Wert-Paare in einem JSON-Datensatz für ein Zielkonfigurationselement abfragen

Architektur

Sie wenden die Guard-Syntax als benutzerdefinierte Richtlinie auf eine AWS Config-Regel an. AWS Config erfasst das hierarchische JSON jeder der angegebenen Ressourcen. Das JSON des AWS Config-Konfigurationselements enthält Schlüssel-Wert-Paare. Diese Attribute werden in der Guard-Syntax als Variablen verwendet, die ihrem entsprechenden Wert zugewiesen werden.

Im Folgenden wird die Guard-Syntax erklärt. Die Variablen aus dem Konfigurationselement JSON werden verwendet und ihnen wird ein % Zeichen vorangestellt.

```
# declare variable
let <variable name> = <'value'>

# create rule and assign condition and policy
    rule <rule name> when
        <CI json key> == <"CI json value"> {
            <top level CI json key>.<next level CI json key> == %<variable name>
```

```
        }
```

Szenario 1: Amazon EBS-Volumes

Szenario 1 stellt eine benutzerdefinierte AWS Config-Regel bereit, die die Guard-Syntax verwendet, um die Konformität für verschlüsselte Volumes zu überprüfen. Diese Regel überprüft, ob das Laufwerk verwendet wird, und stellt sicher, dass der Laufwerkstyp gp3 ist.

Das Folgende ist ein Beispiel für ein AWS Config-Konfigurationselement für Szenario 1. Dieses Konfigurationselement enthält drei Schlüssel-Wert-Paare, die als Variablen in der Guard-Richtlinie verwendet werden: `volumestatusvolumeencryptionstatus`, und. `volumetype` Außerdem wird der `resourceType` Schlüssel in der Guard-Richtlinie als Filter verwendet.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-01-15T19:04:45.402Z",
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "4444444444444",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:ec2:us-west-2:111111111111:volume/vol-222222222222",
  "resourceType": "AWS::EC2::Volume",
  "resourceId": "vol-222222222222",
  "awsRegion": "us-west-2",
  "availabilityZone": "us-west-2b",
  "resourceCreationTime": "2023-01-15T19:03:22.247Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-33333333333333333",
      "relationshipName": "Is attached to Instance"
    }
  ],
  "configuration": {
    "attachments": [
      {
        "attachTime": "2023-01-15T19:03:22.000Z",
        "device": "/dev/xvda",
        "instanceId": "i-33333333333333333",
        "state": "attached",
```

```
        "volumeId": "vol-222222222222",
        "deleteOnTermination": true,
        "associatedResource": null,
        "instanceOwningService": null
      }
    ],
    "availabilityZone": "us-west-2b",
    "createTime": "2023-01-15T19:03:22.247Z",
    "encrypted": false,
    "kmsKeyId": null,
    "outpostArn": null,
    "size": 8,
    "snapshotId": "snap-55555555555555555",
    "state": "in-use",
    "volumeId": "vol-222222222222",
    "iops": 100,
    "tags": [],
    "volumeType": "gp2",
    "fastRestored": null,
    "multiAttachEnabled": false,
    "throughput": null,
    "sseType": null
  },
  "supplementaryConfiguration": {}
}
```

Das Folgende ist ein Beispiel für die Verwendung der Guard-Syntax zur Definition der Variablen und Regeln in Szenario 1. Beachten Sie im folgenden Beispiel Folgendes:

- Die ersten drei Zeilen definieren die Variablen mithilfe des `let` Befehls. Ihnen wird ein Name und ein Wert zugewiesen, die von den Attributen des Konfigurationselements abgeleitet sind.
- Der `compliancecheck` Regelblock fügt eine Abhängigkeit vom Typ when hinzu, die nach einem übereinstimmenden `resourceType` Schlüssel-Wert-Paar sucht. `AWS::EC2::Volume` Wenn eine Übereinstimmung gefunden wird, durchsucht die Regel die restlichen JSON-Attribute und sucht unter den folgenden drei Bedingungen nach Übereinstimmungen: `stateencrypted`, und. `volumeType`

```
let volumestatus = 'available'
let volumetype = 'gp3'
let volumeencryptionstatus = true
```

```
    rule compliancecheck when
        resourceType == "AWS::EC2::Volume" {
            configuration.state == %volumestatus
            configuration.encrypted == %volumeencryptionstatus
            configuration.volumeType == %volumetype
        }
```

Die vollständige benutzerdefinierte CloudFormation Guard-Richtlinie, die diese benutzerdefinierte Regel implementiert, finden Sie unter awsconfig-guard-cft.yaml oder awsconfig-guard-tf-ec2vol.json im Code-Repository. GitHub Terraform-Code, HashiCorp der diese CloudFormation benutzerdefinierte Richtlinie in Guard bereitstellt, finden Sie unter awsconfig-guard-tf-example.json im Code-Repository.

GuardDuty Szenario 2: Einhaltung

Szenario 2 stellt eine benutzerdefinierte AWS Config-Regel bereit, die die Guard-Syntax verwendet, um die GuardDuty Amazon-Konformität zu überprüfen. Diese Regel überprüft, ob bei GuardDuty Rekordern Amazon S3 S3-Schutz und Amazon EKS-Schutz aktiviert sind. Außerdem wird überprüft, ob die GuardDuty Ergebnisse alle 15 Minuten veröffentlicht werden. Dieses Szenario könnte für alle AWS-Konten und AWS-Regionen in einer Organisation (in AWS Organizations) bereitgestellt werden.

Im Folgenden finden Sie ein Beispiel für ein AWS Config-Konfigurationselement für Szenario 2. Dieses Konfigurationselement enthält drei Schlüssel-Wert-Paare, die als Variablen in der Guard-Richtlinie verwendet werden: `FindingPublishingFrequency`S3Logs, und. `Kubernetes` Außerdem wird der `resourceType` Schlüssel in der Richtlinie als Filter verwendet.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-11-27T13:34:28.888Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "7777777777777",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:guardduty:us-
west-2:111111111111:detector/66666666666666666666666666666666",
  "resourceType": "AWS::GuardDuty::Detector",
  "resourceId": "66666666666666666666666666666666",
  "resourceName": "66666666666666666666666666666666",
  "awsRegion": "us-west-2",
  "availabilityZone": "Regional",
  "resourceCreationTime": "2020-02-17T02:48:04.511Z",
```

```
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "Enable": true,
    "FindingPublishingFrequency": "FIFTEEN_MINUTES",
    "DataSources": {
      "S3Logs": {
        "Enable": true
      },
      "Kubernetes": {
        "AuditLogs": {
          "Enable": true
        }
      }
    },

    "Id": "66666666666666666666666666666666",
    "Tags": []
  },
  "supplementaryConfiguration": {
    "CreatedAt": "2020-02-17T02:48:04.511Z"
  }
}
```

Im Folgenden finden Sie ein Beispiel für die Verwendung der Guard-Syntax zur Definition der Variablen und Regeln in Szenario 2. Beachten Sie im folgenden Beispiel Folgendes:

- Die ersten drei Zeilen definieren die Variablen mithilfe des `let` Befehls. Ihnen wird ein Name und ein Wert zugewiesen, die von den Attributen des Konfigurationselements abgeleitet sind.
- Der `compliancecheck` Regelblock fügt eine Abhängigkeit vom Typ when hinzu, die nach einem übereinstimmenden `resourceType` Schlüssel-Wert-Paar sucht. `AWS::GuardDuty::Detector` Wenn eine Übereinstimmung gefunden wird, durchsucht die Regel die restlichen JSON-Attribute und sucht unter den folgenden drei Bedingungen nach Übereinstimmungen: `S3Logs.Enable`Kubernetes.AuditLogs.Enable, und. `FindingPublishingFrequency`

```
let s3protection = true
let kubernetesprotection = true
let publishfrequency = 'FIFTEEN_MINUTES'

    rule compliancecheck when
```

```
        resourceType == "AWS::GuardDuty::Detector" {
            configuration.DataSources.S3Logs.Enable == %s3protection
            configuration.DataSources.Kubernetes.AuditLogs.Enable ==
%kubernetesprotection
            configuration.FindingPublishingFrequency == %publishfrequency
        }
```

Die vollständige benutzerdefinierte CloudFormation Guard-Richtlinie, die diese benutzerdefinierte Regel implementiert, finden Sie unter awsconfig-guard-cft-gd.yaml im Code-Repository. GitHub HashiCorp Terraform-Code, der diese benutzerdefinierte Richtlinie in Guard bereitstellt, finden Sie unter awsconfig-guard-tf-gd.json im Code-Repository. CloudFormation

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.

Andere Tools

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastruktur als Code (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub AWS Config with CloudFormation Guard verfügbar. Dieses Code-Repository enthält Beispiele für beide in diesem Muster beschriebenen Szenarien.

Epen

Benutzerdefinierte AWS Config-Regeln erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Wählen Sie Schlüssel-Wert-Paare für die Regel aus.	Gehen Sie wie folgt vor, wenn Sie eine benutzerdefinierte Guard-Richtlinie definieren. Wenn Sie eine der Beispielr ichtlinien für Szenario 1 oder 2 verwenden, überspringen Sie diese Schritte. 1. Melden Sie sich bei der AWS-Managementkons ole an und öffnen Sie die AWS Config-Konsole unter https://console.aw s.amazon.com/config/. 2. Wählen Sie in der linken Navigationsleiste Ressourcen aus. 3. Wählen Sie im Ressource ninventar den Ressource ntyp aus, für den Sie eine benutzerdefinierte AWS Config-Regel erstellen möchten. 4. Wählen Sie die Option View details aus. 5. Wählen Sie Konfigura tionselement anzeigen (JSON). Dieser Abschnitt wird erweitert und zeigt das	AWS-Administrator, Sicherhei tsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konfigurationselement im JSON-Format an. 6. Identifizieren Sie die Schlüssel-Wert-Paare, für die Sie eine benutzerd efinierte AWS Config-Regel erstellen möchten.	
Erstellen Sie die benutzerd efinierte Regel.	Verwenden Sie die zuvor identifizierten Schlüssel-Wert-Paare oder verwenden Sie eine der bereitgestellten Guard-Beispielrichtlinien und folgen Sie den Anweisung en unter Benutzerdefinierte AWS-Config-Richtlinienregel n erstellen, um eine benutzerd efinierte Regel zu erstellen.	AWS-Administrator, Sicherhei tsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die benutzerdefinierte Regel.	Führen Sie einen der folgenden Schritte aus, um die benutzerdefinierte Guard-Regel zu validieren: • Geben Sie den folgenden Befehl in die AWS-Befehlszeilenschnittstelle (AWS CLI) ein. `cfn-guard validate -r guard-s3.guard -d s3bucket-prod-pass.json` • Folgen Sie den Anweisungen im Modus Detective unter Evaluating Your Resources with AWS Config Rules, um die Regel in AWS Config bereitzustellen. Vergewissern Sie sich, dass die Guard-Syntax korrekt mit den entsprechenden Ressourcen im Zielkonto oder in der Zieldatei übereinstimmt.	AWS-Administrator, Sicherheitsingenieur

Fehlerbehebung

Problem	Lösung
Testen Sie die CloudFormation Guard-Richtlinie außerhalb von AWS Config	Unit-Tests können auf Ihrem lokalen Gerät oder in einer integrierten Entwicklungsumgebung (IDE) wie einer AWS Cloud9 Cloud9-IDE

Problem	Lösung

	durchgeführt werden. Gehen Sie wie folgt vor, um Komponententests durchzuführen:
	1. Installieren Sie die AWS CloudFormation Guard CLI und ihre Abhängigkeiten.
	2. Speichern Sie ein CI-Beispiel im JSON-Form at als JSON-Datei auf Ihrer Workstation.
	3. Speichern Sie die GuardDuty Richtlinie als .guard-Datei auf Ihrer Workstation.
	4. Geben Sie in der Guard-CLI den folgenden Befehl ein, um die JSON-Beispieldatei mithilfe der Guard-Richtlinie zu validieren.
	`cfn-guard validate \`
	`-r guard-s3.guard \`
	`-d s3bucket-prod-pass.json`

Debuggen einer benutzerdefinierten AWS Config-Regel	Ändern Sie den `EnableDebugLogDeli very` Wert in Ihrer Guard-Richtlinie in `true`. Der Standardwert ist `false`. Die Protokoll nachrichten werden in Amazon gespeichert CloudWatch.

Zugehörige Ressourcen

AWS-Dokumentation

- Benutzerdefinierte AWS Config-Richtlinienregeln erstellen (AWS Config-Dokumentation)
- AWS CloudFormation Guard-Regeln schreiben (CloudFormation Guard-Dokumentation)

AWS-Blogbeiträge und Workshops

- Einführung in AWS CloudFormation Guard 2.0 (AWS-Blogbeitrag)

Sonstige Ressourcen

- CloudFormation AWS-Schutz (GitHub)
- CloudFormation Guard CLI-Dokumentation (GitHub)

Erstellen Sie einen konsolidierten Bericht mit den Sicherheitsergebnissen von Prowler aus mehreren AWS-Konten

Quellcode-Repository: multi-account-security-assessment-via-prowler	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance
Arbeitslast: Open Source	AWS-Services: AWS CloudFormation; Amazon EC2; AWS Identity and Access Management	

Übersicht

Prowler (GitHub) ist ein Open-Source-Befehlszeilentool, mit dem Sie Ihre Amazon Web Services (AWS) -Konten bewerten, prüfen und überwachen können, um sicherzustellen, dass sie die bewährten Sicherheitsmethoden einhalten. Bei diesem Muster setzen Sie Prowler in einem zentralen System AWS-Konto in Ihrer Organisation ein, das von verwaltet wird AWS Organizations, und verwenden dann Prowler, um eine Sicherheitsbewertung aller Konten in der Organisation durchzuführen.

Es gibt zwar viele Methoden, um Prowler für eine Bewertung einzusetzen und zu nutzen, aber diese Lösung wurde für eine schnelle Implementierung, eine vollständige Analyse aller Konten in der Organisation oder definierter Zielkonten und eine leicht zugängliche Berichterstattung über die Sicherheitsergebnisse konzipiert. Bei dieser Lösung werden die Ergebnisse konsolidiert, sobald Prowler die Sicherheitsbeurteilung aller Konten im Unternehmen abgeschlossen hat. Außerdem werden alle erwarteten Fehlermeldungen herausgefiltert, z. B. Fehler im Zusammenhang mit Einschränkungen, die Prowler daran hindern, Amazon Simple Storage Service (Amazon S3) -Buckets in Konten zu scannen, die über bereitgestellt wurden. AWS Control Tower Die gefilterten, konsolidierten Ergebnisse werden in einer Microsoft Excel-Vorlage gemeldet, die in diesem Muster enthalten ist. Sie können diesen Bericht verwenden, um potenzielle Verbesserungen der Sicherheitskontrollen in Ihrem Unternehmen zu ermitteln.

Bei der Entwicklung dieser Lösung wurde Folgendes berücksichtigt:

- Die AWS CloudFormation Vorlagen reduzieren den Aufwand, der für die Bereitstellung der AWS Ressourcen in diesem Muster erforderlich ist.
- Sie können die Parameter in den CloudFormation Vorlagen und im Skript prowler_scan.sh zum Zeitpunkt der Bereitstellung anpassen, um die Vorlagen an Ihre Umgebung anzupassen.
- Die Geschwindigkeit der Bewertung und Berichterstattung durch Prowler wird durch die parallel Verarbeitung aggregierter Ergebnisse AWS-Konten, konsolidierte Berichte mit empfohlenen Abhilfemaßnahmen und automatisch generierte Visualisierungen optimiert.
- Der Benutzer muss den Scanfortschritt nicht überwachen. Wenn die Bewertung abgeschlossen ist, wird der Benutzer über ein Amazon Simple Notification Service (Amazon SNS) -Thema benachrichtigt, sodass er den Bericht abrufen kann.
- Die Berichtsvorlage hilft Ihnen dabei, nur die relevanten Ergebnisse für Ihr gesamtes Unternehmen zu lesen und zu bewerten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine AWS-Konto zum Hosten von Sicherheitsdiensten und -tools, die als Mitgliedskonto einer Organisation in verwaltet AWS Organizations werden. In diesem Muster wird dieses Konto als Sicherheitskonto bezeichnet.
- Im Sicherheitskonto müssen Sie über ein privates Subnetz mit ausgehendem Internetzugang verfügen. Anweisungen finden Sie unter VPC mit Servern in privaten Subnetzen und NAT in der Dokumentation zu Amazon Virtual Private Cloud (Amazon VPC). Sie können den Internetzugang mithilfe eines NAT-Gateways einrichten, das in einem öffentlichen Subnetz bereitgestellt wird.
- Zugriff auf das AWS Organizations Verwaltungskonto oder ein Konto, für das delegierte Administratorrechte erteilt wurden. CloudFormation Anweisungen finden Sie in der Dokumentation unter Registrieren eines delegierten Administrators. CloudFormation
- Aktivieren Sie den vertrauenswürdigen Zugriff zwischen AWS Organizations und CloudFormation. Anweisungen finden Sie AWS Organizations in der CloudFormation Dokumentation unter Vertrauenswürdigen Zugriff aktivieren mit.

Einschränkungen

- Das Ziel AWS-Konten muss als Organisation in verwaltet werden AWS Organizations. Wenn Sie die Vorlage nicht verwenden AWS Organizations, können Sie die CloudFormation Vorlage

ProwlerExecIAM-role.YAML und das Skript prowler_scan.sh für Ihre Umgebung aktualisieren. Stattdessen geben Sie eine Liste mit AWS-Konto IDs und Regionen an, in denen Sie das Skript ausführen möchten.

- Die CloudFormation Vorlage ist für die Bereitstellung der Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einem privaten Subnetz mit ausgehendem Internetzugang konzipiert. Der AWS Systems Manager Agent (SSM Agent) benötigt ausgehenden Zugriff, um den AWS Systems Manager Service-Endpunkt zu erreichen, und Sie benötigen ausgehenden Zugriff, um das Code-Repository zu klonen und Abhängigkeiten zu installieren. Wenn Sie ein öffentliches Subnetz verwenden möchten, müssen Sie die Vorlage prowler-resources.yaml ändern, um der EC2-Instance eine Elastic IP-Adresse zuzuordnen.

Produktversionen

- Prowler Version 3.0 oder höher

Architektur

Das Diagramm zeigt den folgenden Prozess:

1. Mithilfe von Session Manager, einer Fähigkeit von AWS Systems Manager, authentifiziert sich der Benutzer bei der EC2-Instance und führt das Skript prowler_scan.sh aus. Dieses Shell-Skript führt die Schritte 2 bis 8 aus.
2. Die EC2-Instance übernimmt die `ProwlerEC2Role` IAM-Rolle, die Berechtigungen für den Zugriff auf den S3-Bucket und für die Übernahme der `ProwlerExecRole` IAM-Rollen in den anderen Konten in der Organisation gewährt.
3. Die EC2-Instance übernimmt die `ProwlerExecRole` IAM-Rolle im Verwaltungskonto der Organisation und generiert eine Liste der Konten in der Organisation.
4. Die EC2-Instance übernimmt die `ProwlerExecRole` IAM-Rolle in den Mitgliedskonten der Organisation (im Architekturdiagramm als Workload-Konten bezeichnet) und führt für jedes Konto eine Sicherheitsbewertung durch. Die Ergebnisse werden als CSV- und HTML-Dateien auf der EC2-Instance gespeichert.

Hinweis: HTML-Dateien sind eine Ausgabe des Prowler-Assessments. Aufgrund der Natur von HTML werden sie nicht direkt in diesem Muster verkettet, verarbeitet oder verwendet. Diese können jedoch für die Überprüfung einzelner Kontoberichte nützlich sein.

5. Die EC2-Instance verarbeitet alle CSV-Dateien, um bekannte, erwartete Fehler zu entfernen, und konsolidiert die verbleibenden Ergebnisse in einer einzigen CSV-Datei.
6. Die EC2-Instance führt das Skript generateVisualizations.py aus. Dieses Skript verarbeitet die CSV-Datei mit den aggregierten Ergebnissen und generiert PNG-Dateien mit Grafiken und Diagrammen, die Ihnen helfen können, die Ergebnisse zu verstehen und zu dokumentieren. Es erstellt auch eine HTML-Datei, die Informationen über den Scan und die PNG-Dateien enthält.
7. Die EC2-Instance verpackt die Ergebnisse der einzelnen Konten, die aggregierten Ergebnisse und die generierten Visualisierungen in einer ZIP-Datei.
8. Die EC2-Instance lädt die Zip-Datei in den S3-Bucket hoch.
9. Eine EventBridge Regel erkennt den Datei-Upload und verwendet ein Amazon SNS SNS-Thema, um dem Benutzer eine E-Mail zu senden, in der er darüber informiert wird, dass die Bewertung abgeschlossen ist.
10. Der Benutzer lädt die Zip-Datei aus dem S3-Bucket herunter. Der Benutzer importiert die Ergebnisse in die Excel-Vorlage und überprüft die Ergebnisse.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet sichere und skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten. Dieses Muster verwendet Session Manager, eine Funktion von Systems Manager.

Andere Tools

- Prowler ist ein Open-Source-Befehlszeilentool, mit dem Sie Ihre Konten bewerten, prüfen und überwachen können, um sicherzustellen, dass sie bewährte AWS Sicherheitsmethoden und andere Sicherheitsrahmen und -standards einhalten.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Multi-Account Security Assessment via Prowler verfügbar. Das Code-Repository enthält die folgenden Dateien:

- prowler_scan.sh — Dieses Bash-Skript wird verwendet, um eine Prowler-Sicherheitsbewertung von mehreren gleichzeitig AWS-Konten zu parallel. Wie in der Datei Prowler-Resources.yaml definiert CloudFormationtemplate, wird dieses Skript automatisch im Ordner auf der EC2-Instance bereitgestellt. `usr/local/prowler`
- prowler-resources.YAML — Sie verwenden diese CloudFormation Vorlage, um einen Stack im Sicherheitskonto der Organisation zu erstellen. Diese Vorlage stellt alle erforderlichen Ressourcen für dieses Konto bereit, um die Lösung zu unterstützen. Dieser Stack muss vor der Vorlage IAM-ProwlerExec Role.yaml bereitgestellt werden. Es wird nicht empfohlen, diese Ressourcen in einem Konto bereitzustellen, das kritische Produktionsworkloads hostet.

Hinweis: Wenn dieser Stack gelöscht und erneut bereitgestellt wird, müssen Sie den `ProwlerExecRole` Stacksatz neu erstellen, um die kontenübergreifenden Abhängigkeiten zwischen den IAM-Rollen wiederherzustellen.

- IAM- ProwlerExec Role.yaml — Sie verwenden diese CloudFormation Vorlage, um ein Stack-Set zu erstellen, das die `ProwlerExecRole` IAM-Rolle in allen Konten der Organisation, einschließlich des Verwaltungskontos, bereitstellt.
- generateVisualizations.py — Das Skript prowler_scan.sh ruft dieses Python-Skript automatisch auf, um Visualisierungen auf der Grundlage der aggregierten Ergebnisse zu generieren, und fügt sie in die im S3-Bucket gespeicherte ZIP-Datei ein. Dieses Skript erstellt die folgenden Dateien:
  - `FailuresByAccount-<date>.png`— Balkendiagramm, das die fehlgeschlagenen Prowler-Prüfungen für jedes Konto veranschaulicht
  - `FailuresByService-<date>.png`— Balkendiagramm, das die fehlgeschlagenen Prowler-Prüfungen für jedes einzelne zeigt AWS-Service
  - `ProcessedResultsByFailureSeverityCount-<date>.png`— Balkendiagramm, das die Verteilung der fehlgeschlagenen Prowler-Prüfungen für jeden Schweregrad (kritisch, hoch, mittel, niedrig und informativ) veranschaulicht
  - `ResultsByFail-<date>.png`— Kreisdiagramm der fehlgeschlagenen Prowler-Prüfungen nach Schweregrad
  - `ResultsBySeverity-<date>.png`— Kreisdiagramm aller Prowler-Prüfungen (bestanden und fehlgeschlagen) nach Schweregrad
  - `ProwlerReport.html`— Einzelne HTML-Datei, in der alle Bilder enthalten sind
- prowler3-report-template.xlsm — Sie verwenden diese Excel-Vorlage, um die Ergebnisse von Prowler zu verarbeiten. Die Pivot-Tabellen im Bericht bieten Suchfunktionen, Diagramme und konsolidierte Ergebnisse.

Epen

Bereite dich auf den Einsatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Ändern Sie in einer Befehlszeilenschnittstelle	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten. 2. Geben Sie den folgenden Befehl ein: `git clone https://github.com/aws-samples/multi-account-security-assessment-via-prowler.git`	
Überprüfen Sie die Vorlagen.	1. Öffnen Sie im geklonten Repository die Dateien Prowler-Resources.yaml und IAM-Role.yaml. ProwlerExec 2. Überprüfen Sie die mit diesen Vorlagen erstellten Ressourcen und passen Sie die Vorlagen nach Bedarf an Ihre Umgebung an. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Arbeiten mit Vorlagen. 3. Speichern und schließen Sie die Dateien Prowler-Resources.yaml und IAM-Role.yaml. ProwlerExec	AWS DevOps

Erstellen Sie die CloudFormation Stapel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Sicherheitskonto bereit.	Mithilfe der Vorlage prowler-resources.yaml erstellen Sie einen CloudFormation Stack, der alle erforderlichen Ressourcen im Sicherheitskonto bereitstellt. Anweisungen finden Sie in der Dokumentation unter Einen Stack erstellen. CloudFormation Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage ist bereit aus und laden Sie dann die Datei prowler-resources.yaml hoch. 2. Geben Sie auf der Seite „Stack-Details angeben“ im Feld Stack-Name den folgenden Text ein. `Prowler-Resources` 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `VPCId`— Wählen Sie eine VPC im Konto aus. • `SubnetId`— Wählen Sie ein privates Subnetz mit Internetzugang aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Hinweis: Wenn Sie ein öffentliches Subnetz auswählen, wird der EC2-Instance keine öffentlic he IP-Adresse zugewiese n, da die CloudFormation Vorlage standardmäßig keine Elastic IP-Adresse bereitstellt und anfügt.
	• `InstanceType` — Wählen Sie eine Instanzgröße basierend auf der Anzahl der parallel Bewertungen aus:
	  • Für 10 wählen Sie `r6i.large` .
	  • Für 12 wählen Sie `r6i.xlarge` .
	  • Wählen Sie für 14—18. `r6i.2xlarge`
	• `InstanceImageId` — Behalten Sie die Standardeinstellung für Amazon Linux bei.
	• `KeyPairName` — Wenn Sie SSH für den Zugriff verwenden, geben Sie den Namen eines vorhandenen key pair an.
	• `PermittedSSHInboun d` — Wenn Sie SSH für den Zugriff verwenden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, geben Sie einen zulässigen CIDR-Block an. Wenn Sie SSH nicht verwenden, behalten Sie den Standardwert von bei. `127.0.0.1` • `BucketName` — Der Standardwert ist`prowler-output-<accountID>-<region>` . Sie können dies nach Bedarf ändern. Wenn Sie einen benutzerdefinierten Wert angeben, werden die Konto-ID und die Region automatisch an den angegebenen Wert angehängt. • `EmailAddress` — Geben Sie eine E-Mail-Adresse für eine Amazon SNS SNS-Benachrichtigung an, wenn Prowler die Bewertung abgeschlossen und die ZIP-Datei in den S3-Bucket hochlädt. Hinweis: Die Konfiguration des SNS-Abonnements muss bestätigt werden, bevor Prowler die Bewertung abschließt. Andernfalls wird	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	keine Benachrichtigung gesendet. • `IAMProwler rEC2Role` — Behalten Sie die Standarde instellung bei, es sei denn, Ihre Benennung skonventionen erfordern einen anderen Namen für diese IAM-Rolle. • `IAMProwlerExecRole` — Behalten Sie die Standardeinstellung bei, es sei denn, bei der Bereitstellung der Datei IAM- ProwlerEx ec Role.yaml wird ein anderer Name verwendet . • `Parallelism` — Geben Sie die Anzahl der parallel Prüfungen an, die durchgeführt werden sollen. Stellen Sie sicher, dass der Wert im `InstanceType` Parameter diese Anzahl parallel Bewertungen unterstützt. • `FindingOutput` — Wenn Sie bestandene Ergebnisse ausschlie ßen möchten, wählen Sie`FailOnly`. Dadurch	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird die Ausgabegr öße erheblich reduziert und der Schwerpunkt liegt auf den Prüfungen , die möglicherweise behoben werden müssen. Wenn Sie bestandene Ergebnisse einbezieh en möchten, wählen Sie`FailAndPass` . 4. Wählen Sie auf der Seite Überprüfen die Option Die folgenden Ressource n erfordern Fähigkeiten: [AWS::IAM::Role] und wählen Sie dann Stack erstellen aus. 5. Nachdem der Stack erfolgreich erstellt wurde, kopieren Sie in der CloudFormation Konsole auf der Registerkarte Outputs den `ProwlerEC 2Role` Amazon-Re ssourcennamen (ARN). Sie verwenden diesen ARN später, wenn Sie die Datei ProwlerExecIAM-Role.yaml bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle in den Mitgliedskonten bereit.	Verwenden Sie im AWS Organizations Verwaltungskonto oder einem Konto mit delegierten Administratorrechten für die Vorlage ProwlerExecIAM-Role.yaml CloudFormation, um ein Stack-Set zu erstellen. CloudFormation Das Stack-Set stellt die `ProwlerExecRole` IAM-Rolle in allen Mitgliedskonten der Organisation bereit. Anweisungen finden Sie in der Dokumentation unter Erstellen eines Stack-Sets mit vom Service verwalteten Berechtigungen. CloudFormation Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie unter Vorlage vorbereiten die Option Vorlage ist bereit aus und laden Sie dann die Datei ProwlerExecIAM-Role.yaml hoch. 2. Geben Sie auf der Seite „StackSet Details angeben“ dem Stack-Set einen Namen. `IAM-ProwlerExecRole` 3. Geben Sie im Abschnitt Parameter Folgendes ein:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `AuthorizedARN` — Geben Sie den `ProwlerEC2Role` ARN ein, den Sie bei der Erstellung des `Prowler-Resources` Stacks kopiert haben. • `ProwlerExecRoleNam e` — Behalten Sie den Standardwert von bei, `ProwlerExecRole` sofern bei der Bereitste llung der Datei Prowler-Resources.yaml kein anderer Name verwendet wurde. 4. Wählen Sie unter Permissio ns (Berechtigungen) die Option Service-managed permissions (Servicev erwaltete Berechtigungen) aus. 5. Wählen Sie auf der Seite Bereitstellungsoptionen festlegen unter Bereitste llungsziele die Option Für die Organisation bereitste llen aus und akzeptieren Sie alle Standardeinstellun gen. Hinweis: Wenn Sie möchten, dass die Stacks für alle Mitgliedskonten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gleichzeitig bereitgestellt werden, legen Sie „Maximale Anzahl gleichzeitiger Konten“ und „Fehlertoleranz“ auf einen hohen Wert fest, z. B. `100` 6. Wählen Sie unter Bereitstellungsregionen die Region aus, AWS-Region in der die EC2-Instance für Prowler bereitgestellt wird. Da es sich bei den IAM-Ressourcen um globale und nicht um regionale Ressourcen handelt, wird dadurch die IAM-Rolle in allen aktiven Regionen bereitgestellt. 7. Wählen Sie auf der Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden, und wählen Sie dann Erstellen aus. StackSet 8. Überwachen Sie die Registerkarte Stack-Instances (für den Status einzelner Konten) und die Registerkarte Operationen (für den Gesamtstatus), um festzustellen, wann die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung abgeschlossen ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle im Verwaltungskonto bereit.	Mithilfe der Vorlage IAM-ProwlerExec Role.YAML erstellen Sie einen CloudFormation Stack, der die `ProwlerExecRole` IAM-Rolle im Verwaltungskonto der Organisation bereitstellt. Das Stack-Set, das Sie zuvor erstellt haben, stellt die IAM-Rolle nicht im Verwaltungskonto bereit. Anweisungen finden Sie in der CloudFormation Dokumentation unter Einen Stack erstellen. Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage ist bereit aus und laden Sie dann die Datei ProwlerExecIAM-Role.yaml hoch. 2. Geben Sie auf der Seite „Stack-Details angeben“ im Feld Stack-Name den folgenden Text ein. `IAM-ProwlerExecRole` 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `AuthorizedARN` — Geben Sie den `ProwlerEC2Role`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ARN ein, den Sie bei der Erstellung des `Prowler-Resources` Stacks kopiert haben. • `ProwlerExecRoleName` — Behalten Sie den Standardwert von bei, `ProwlerExecRole` sofern bei der Bereitstellung der Datei Prowler-Resources.yaml kein anderer Name verwendet wurde. 4. Wählen Sie auf der Seite „Überprüfen“ die Option Die folgenden Ressourcen erfordern Fähigkeiten: [AWS::IAM::Role] und wählen Sie dann Stapel erstellen aus.	

Führen Sie die Prowler-Sicherheitsbewertung durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Scan aus.	1. Melden Sie sich mit dem Sicherheitskonto in der Organisation an. 2. Stellen Sie mithilfe von Session Manager eine Verbindung zu der EC2-Instance für Prowler her, die Sie zuvor bereitgestellt haben. Anweisungen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager. Wenn Sie keine Verbindung herstellen können, lesen Sie den Abschnitt zur Fehlerbehebung in diesem Muster. 3. Navigieren Sie zu der Datei prowler_scan.sh **`usr/local/prowler`** , und öffnen Sie sie. 4. Überprüfen und ändern Sie die einstellbaren Parameter und Variablen in diesem Skript nach Bedarf für Ihre Umgebung. Weitere Informationen zu Anpassungsoptionen finden Sie in den Kommentaren am Anfang des Skripts. Anstatt beispielsweise eine Liste aller Mitgliedskonten in der Organisation aus dem Verwaltungskonto abzurufen, können Sie das Skript so ändern, AWS-Regionen dass es die AWS-Konto IDs angibt oder die Sie scannen möchten, oder Sie können auf eine externe Datei verweisen, die diese Parameter enthält.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Speichern und schließen Sie die Datei prowler_scan.sh.
	6. Geben Sie die folgenden Befehle ein. Dadurch wird das Skript prowler_scan.sh ausgeführt.
	`sudo -i`
	`screen`
	`cd /usr/local/prowler`
	`./prowler_scan.sh`
	Beachten Sie Folgendes:
	• Der Befehl screen ermöglicht die weitere Ausführung des Skripts für den Fall, dass die Verbindung unterbrochen wird oder Sie den Konsolenzugriff verlieren.
	• Nach dem Start des Scans können Sie das Trennen des Bildschirms erzwingen, indem Sie Strg+A D drücken. Der Bildschirm wird getrennt, und Sie können die Instanzverbindung schließen und die Bewertung fortsetzen.
	• Um eine getrennte Sitzung wieder aufzunehmen, stellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie eine Verbindung zur Instanz her, geben Sie ein und geben Sie `sudo -i` dann die Eingabetaste ein`screen -r`. • Um den Fortschritt der einzelnen Kontoprüf ungen zu überwachen, können Sie zum `usr/local/prowler` Verzeichnis navigiere n und den Befehl eingeben`tail -f output/stdout-<account-id>` . 7. Warten Sie, bis Prowler die Scans aller Konten abgeschlossen hat. Das Skript bewertet mehrere Konten gleichzeitig. Wenn die Bewertung für alle Konten abgeschlossen ist, erhalten Sie eine Benachrichtigung, falls Sie bei der Bereitstellung der Datei Prowler-Resources. yaml eine E-Mail-Adresse angegeben haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Ergebnisse von Prowler ab.	1. Laden Sie die `prowler-output-<assessDate>.zip` Datei aus dem Bucket herunter. `prowler-output-<accountID>-<region>` Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekt herunterladen. 2. Löschen Sie alle Objekte im Bucket, einschließlich der Datei, die Sie heruntergeladen haben. Dies ist eine bewährte Methode zur Kostenoptimierung und um sicherzustellen, dass Sie den `Prowler-Resources` CloudFormation Stapel jederzeit löschen können. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekte löschen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die EC2-Instance an.	Um zu verhindern, dass die Instance abgerechnet wird, während sich die Instance im Leerlauf befindet, beenden Sie die EC2-Instance, auf der Prowler ausgeführt wird. Anweisungen finden Sie unter Stoppen und Starten Ihrer Instances in der Amazon EC2 EC2-Dokumentation.	AWS DevOps

Erstellen Sie einen Bericht über die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie die Ergebnisse.	1. Öffnen Sie in Excel die Datei prowler-report-template.xlsx und wählen Sie dann das Prowler CSV-Arbeitsblatt aus. 2. Löschen Sie alle Beispieldaten, einschließlich der Kopfzeile. Wenn Sie gefragt werden, ob Sie die Abfrage löschen möchten, die mit den zu entfernenden Daten verknüpft ist, wählen Sie Nein. Das Löschen der Abfrage kann sich auf die Funktionalität der Pivot-Tabellen in der Excel-Vorlage auswirken. 3. Extrahieren Sie den Inhalt der Zip-Datei, die Sie aus	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem S3-Bucket heruntergeladen haben. 4. Öffnen Sie in Excel die Datei prowler-fullorgresults-accessdeniedfiltered.txt. Es wird empfohlen, diese Datei zu verwenden, da die häufigsten Fehler, die nicht behoben werden können, bereits behoben wurden, z. B. `Access Denied` Fehler im Zusammenhang mit versuchten Scans von AWS Control Tower Ressourcen. Wenn Sie die ungefilterten Ergebnisse erhalten möchten, öffnen Sie stattdessen die Datei prowler-fullorgresults.txt. 5. Wählen Sie Spalte A aus. 6. Wenn Sie Windows verwenden, geben Sie Strg+C ein, oder wenn Sie macOS verwenden, geben Sie Cmd+C ein. Dadurch werden alle Daten in die Zwischenablage kopiert. 7. Wählen Sie in der Excel-Berichtsvorlage im CSV-Arbeitsblatt Prowler die Zelle A1 aus. 8. Wenn Sie Windows verwenden, geben Sie Strg+V ein, oder wenn Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	macOS verwenden, geben Sie Cmd+V ein. Dadurch werden die Ergebnisse in den Bericht eingefügt. 9. Vergewissern Sie sich, dass alle Zellen mit eingefügten Daten ausgewählt sind. Wenn nicht, wählen Sie Spalte A aus. 10. Wählen Sie auf der Registerkarte Daten die Option Text in Spalten aus. 11. Gehen Sie im Assistenten wie folgt vor: • Wählen Sie für Schritt 1 die Option Delimited aus. • Wählen Sie für Schritt 2 für Trennzeichen die Option Semikolon aus. Vergewissern Sie sich im Bereich Datenvorschau, dass die Daten in Spalten aufgeteilt sind. • Wählen Sie für Schritt 3 die Option Fertig stellen aus. 12. Vergewissern Sie sich, dass die Textdaten über mehrere Spalten getrennt sind. 13. Speichern Sie den Excel-Bericht unter einem neuen Namen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	14. Suchen und löschen Sie alle `Access Denied` Fehler in den Ergebnissen. Anweisungen zum programmgesteuerten Entfernen von Fehlern finden Sie unter Programmgesteuertes Entfernen von Fehlern im Abschnitt Zusätzliche Informationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Finalisieren Sie den Bericht.	1. Wählen Sie das Arbeitsblatt Ergebnisse und dann Zelle A17 aus. Diese Zelle ist die Kopfzeile der Pivot-Tabelle. 2. Wählen Sie in der Multifunktionsleiste unter PivotTable Tools die Option Analysieren und anschließend unter Aktualisieren die Option Alle aktualisieren aus. Dadurch werden die Pivot-Tabellen mit dem neuen Datensatz aktualisiert. 3. Standardmäßig zeigt Excel AWS-Konto Zahlen nicht richtig an. Gehen Sie wie folgt vor, um die Zahlenformatierung zu korrigieren: • Öffnen Sie im Arbeitsblatt Ergebnisse das Kontextmenü (Rechtsklick) für Spalte A, und wählen Sie dann Zellen formatieren aus. • Wählen Sie Zahl und geben Sie im Feld Dezimalstellen den Wert ein`0`. • Wählen Sie OK aus. Hinweis: Wenn eine AWS-Konto Zahl mit einer oder mehreren Nullen beginnt, entfernt Excel die Nullen	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	automatisch. Wenn Sie im Bericht eine Kontonummer mit weniger als 12 Ziffern sehen, sind die fehlenden Ziffern Nullen am Anfang der Zahl. 4. (Optional) Sie können Felder reduzieren, um die Ergebnisse leichter lesbar zu machen. Gehen Sie wie folgt vor: • Wenn Sie auf dem Arbeitsblatt Ergebnisse den Cursor auf die Zeile zwischen den Zeilen 18 und 19 bewegen (den Raum zwischen der kritischen Überschrift und dem ersten Ergebnis), ändert sich das Cursorsymbol in einen kleinen Pfeil, der nach unten zeigt. • Klicken Sie hier, um alle Suchfelder auszuwählen. • Öffnen Sie das Kontextmenü (Rechtsklick), suchen Sie nach Erweiteren/Reduzieren und wählen Sie dann Reduzieren. 5. Einzelheiten zur Bewertung finden Sie in den Arbeitsblättern „Ergebnisse“,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	„Schweregrad“ und „Nicht bestanden“. 6. Sehen Sie sich in der ZIP-Datei im `Results-Visualizaton-<date-of-scan>` Ordner die automatisch generierten Grafiken und Diagramme an, mit denen Sie Ihre Berichte mit Visualisierungen erweitern können.	

(Optional) Aktualisieren Sie Prowler oder die Ressourcen im Code-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisiere Prowler.	Wenn Sie Prowler auf die neueste Version aktualisieren möchten, gehen Sie wie folgt vor: 1. Stellen Sie mithilfe von Session Manager eine Connect zur EC2-Instance für Prowler her. Anweisungen finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager. 2. Geben Sie den folgenden Befehl ein. `sudo -i`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pip3 install --upgrade prowler`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie das Skript prowler_scan.sh.	Wenn Sie das Skript prowler_scan.sh auf die neueste Version im Repository aktualisieren möchten, gehen Sie wie folgt vor:
	1. Stellen Sie mithilfe von Session Manager eine Connect zur EC2-Instance für Prowler her. Anweisungen finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager.
	2. Geben Sie den folgenden Befehl ein.
	`sudo -i`
	3. Navigieren Sie zum Prowler-Skriptverzeichnis.
	`cd /usr/local/prowler`
	4. Geben Sie den folgenden Befehl ein, um das lokale Skript zu speichern, sodass Sie benutzerdefinierte Änderungen in der neuesten Version zusammenführen können.
	`git stash`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Geben Sie den folgenden Befehl ein, um die neueste Version des Skripts abzurufen.
	`git pull`
	6. Geben Sie den folgenden Befehl ein, um das benutzerdefinierte Skript mit der neuesten Version des Skripts zusammenzuführen.
	`git stash pop`
	Hinweis: Möglicherweise erhalten Sie Warnungen im Zusammenhang mit lokal generierten Dateien, die sich nicht im GitHub Repository befinden, z. B. beim Suchen nach Berichten. Sie können diese ignorieren, solange in der Datei prowler_scan.sh angezeigt wird, dass die lokal gespeicherten Änderunge n wieder zusammengeführt wurden.	

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle bereitgestellten Ressourcen.	Sie können die bereitgestellten Ressourcen in den Konten belassen. Wenn Sie die EC2-Instance herunterfahren, wenn sie nicht verwendet wird, und den S3-Bucket leer lassen, reduziert dies die Kosten für die Wartung der Ressourcen für future Scans. Wenn Sie die Bereitstellung aller Ressourcen aufheben möchten, gehen Sie wie folgt vor: 1. Löschen Sie den `IAM-ProwlerExecRole` Stack, der im Verwaltungskonto bereitgestellt wurde. Anweisungen finden Sie in der CloudFormation Dokumentation unter Löschen eines Stacks. 2. Löschen Sie das `IAM-ProwlerExecRole` Stack-Set, das im Verwaltungskonto der Organisation oder im delegierten Administratorkonto bereitgestellt wurde. Anweisungen finden Sie in der Dokumentation	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Löschen eines Stack-Sets. CloudFormation 3. Löschen Sie alle Objekte im `prowler-output` S3-Bucket. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekte löschen. 4. Löschen Sie den im Sicherheitskonto bereitgestellten `Prowler-Resources` Stack. Anweisungen finden Sie in der CloudFormation Dokumentation unter Löschen eines Stacks.	

Fehlerbehebung

Problem	Lösung
Es konnte keine Verbindung zur EC2-Instance mithilfe von Session Manager hergestellt werden.	Der SSM-Agent muss in der Lage sein, mit dem Systems Manager Manager-Endpunkt zu kommunizieren. Gehen Sie wie folgt vor: 1. Stellen Sie sicher, dass das Subnetz, in dem die EC2-Instance bereitgestellt wird, über Internetzugang verfügt. 2. Starten Sie die EC2-Instance neu.
Bei der Bereitstellung des Stack-Sets werden Sie von der CloudFormation Konsole dazu aufgefordert. `Enable trusted access`	Dies weist darauf hin, dass der vertrauen swürdige Zugriff zwischen AWS Organizations und CloudFormation nicht aktiviert wurde. Für die Bereitstellung des vom Service verwaltet

Problem	Lösung
`with AWS Organizations to use service-managed permissions`	en Stack-Sets ist ein vertrauenswürdiger Zugriff erforderlich. Wählen Sie die Schaltfläche, um den vertrauenswürdigen Zugriff zu aktivieren. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Vertrauenswürdigen Zugriff aktivieren.

Zugehörige Ressourcen

AWS Dokumentation

- Implementierung von Sicherheitskontrollen am AWS (AWS Prescriptive Guidance)

Sonstige Ressourcen

- Prowler () GitHub

Zusätzliche Informationen

Programmgesteuertes Entfernen von Fehlern

Wenn die Ergebnisse `Access Denied` Fehler enthalten, sollten Sie diese aus den Ergebnissen entfernen. Diese Fehler sind in der Regel auf externe Einflussberechtigungen zurückzuführen, die Prowler daran hindern, eine bestimmte Ressource zu bewerten. Beispielsweise schlagen einige Prüfungen fehl, wenn S3-Buckets überprüft werden, die über bereitgestellt wurden. AWS Control Tower Sie können diese Ergebnisse programmgesteuert extrahieren und die gefilterten Ergebnisse als neue Datei speichern.

Mit den folgenden Befehlen werden Zeilen entfernt, die eine einzelne Textzeichenfolge (ein Muster) enthalten, und die Ergebnisse werden dann in einer neuen Datei ausgegeben.

- Für Linux oder macOS (Grep)

```
grep -v -i "Access Denied getting bucket" myoutput.csv > myoutput_modified.csv
```

- Für Windows () PowerShell

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket' -NotMatch >
 myoutput_modified.csv
```

Die folgenden Befehle entfernen Zeilen, die mehr als einer Textzeichenfolge entsprechen, und geben die Ergebnisse dann in einer neuen Datei aus.

- Für Linux oder macOS (verwendet eine Escape-Pipe zwischen Zeichenketten)

```
grep -v -i 'Access Denied getting bucket\|Access Denied Trying to Get' myoutput.csv >
 myoutput_modified.csv
```

- Für Windows (verwendet ein Komma zwischen Zeichenketten)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket', 'Access
 Denied Trying to Get' -NotMatch > myoutput_modified.csv
```

Beispiele melden

Die folgende Abbildung zeigt ein Beispiel für das Arbeitsblatt „Ergebnisse“ im Bericht über die konsolidierten Ergebnisse von Prowler.

Die folgende Abbildung zeigt ein Beispiel für das Arbeitsblatt „Pass Fail“ im Bericht über die konsolidierten Ergebnisse von Prowler. (Standardmäßig werden erfolgreiche Ergebnisse von der Ausgabe ausgeschlossen.)

Die folgende Abbildung zeigt ein Beispiel für das Arbeitsblatt „Schweregrad“ im Bericht über die konsolidierten Ergebnisse von Prowler.

Löschen ungenutzter Amazon Elastic Block Store (Amazon EBS)-Volumes mithilfe von AWS Config und AWS Systems Manager

Erstellt von Sankar Sangubotla (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Management und Governance; Kostenmanagement	AWS-Services: AWS Config ;AWS Systems Manager

Übersicht

Der Lebenszyklus eines Amazon Elastic Block Store (Amazon EBS)-Volumes ist in der Regel unabhängig vom Lebenszyklus der Amazon Elastic Compute Cloud (Amazon EC2)-Instance, an die es angehängt ist. Sofern Sie beim Start nicht die Option Bei Beendigung löschen auswählen, wird das EBS-Volume durch das Beenden der EC2-Instance getrennt, aber nicht gelöscht. Insbesondere in Entwicklungs- und Testumgebungen, in denen es üblich ist, EC2-Instances zu starten und zu beenden, kann dies zu einer großen Anzahl nicht genutzter EBS-Volumes führen. Für EBS-Volumes fallen Gebühren in Ihrem Amazon Web Services (AWS)-Konto an, unabhängig davon, ob sie verwendet werden. Durch das Löschen dieser Volumes können Sie die Kosten für Ihre AWS-Konten optimieren. Darüber hinaus ist das Löschen ungenutzter EBS-Volumes eine bewährte Sicherheitsmethode, um den Zugriff auf ungenutzte, potenziell sensible Daten in diesen Volumes zu verhindern.

AWS Config kann Ihnen helfen, nicht konforme Ressourcen manuell oder automatisch zu beheben. Dieses Muster beschreibt, wie Sie eine AWS Config-Regel und eine automatische Korrekturmaßnahme konfigurieren, die ungenutzte Amazon EBS-Volumes im Konto löscht. Die Abhilfemaßnahme ist ein vordefiniertes Runbook für Automation, eine Funktion von AWS Systems Manager . Sie können das Runbook so konfigurieren, dass vor dem Löschen ein Snapshot des Volumes erstellt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- AWS Identity and Access Management (IAM)-Berechtigungen zum Ausführen des `AWSConfigRemediation-DeleteUnusedEBSVolume` Runbooks für Automation, eine Funktion von AWS Systems Manager . Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen in AWSConfigRemediation-DeleteUnusedEBSVolume.
- Ein oder mehrere ungenutzte Amazon EBS-Volumes.

Einschränkungen

- Die nicht verwendeten Amazon-EBS-Volumes müssen sich im `available` Status befinden.

Architektur

Technologie-Stack

- AWS Config
- Amazon EBS
- Systems Manager
- Systems Manager Automation

Zielarchitektur

1. Die AWS Config-Regel wertet die EBS-Volumes aus.
2. Die Regel gibt eine Liste von konformen und nicht konformen Ressourcen zurück. EBS-Volumes, die sich im `available` Status befinden, bei denen es sich um ungenutzte Volumes handelt, werden als nicht konform eingestuft.
3. AWS Config startet das Automation-Runbook automatisch.
4. Falls konfiguriert, erstellt Systems Manager Snapshots der nicht verwendeten Volumes, bevor sie gelöscht werden.
5. Systems Manager löscht die nicht verwendeten EBS-Volumes.

Automatisierung und Skalierung

Sie können diese Lösung auf alle Konten in Ihrer Organisation anwenden. Weitere Informationen finden Sie unter Verwalten von Regeln für alle Konten in Ihrer Organisation in der AWS Config-Dokumentation.

Tools

- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und wie sie konfiguriert sind. Auf diese Weise können Sie feststellen, wie Ressourcen miteinander in Beziehung stehen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht die Anwendungs- und Ressourcenverwaltung, verkürzt die Zeit zum Erkennen und Beheben betrieblicher Probleme und erleichtert Ihnen die sichere Verwaltung Ihrer AWS-Ressourcen in großem Umfang.
- AWS Systems Manager Automation vereinfacht allgemeine Wartungs-, Bereitstellungs- und Korrekturaufgaben für viele AWS-Services.

Polen

Konfigurieren der AWS Config-Regel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle für das Automation-Runbook.	Erstellen Sie eine Rolle mit dem Namen `AssumeRole` . Systems Manager Automation verwendet diese Rolle, um das Runbook auszuführen. Anweisungen finden Sie unter Konfigurieren des Zugriffs einer Servicerolle (Rolle übernehmen) für Automatisierungen in der Systems Manager-Dokumentation.	AWS-Systemadministrator
Aktivieren Sie den AWS Config Recorder.	Folgen Sie den Anweisungen unter Einrichten von AWS Config mit der Konsole in der	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Config-Dokumentation, um sicherzustellen, dass AWS Config ausgeführt wird und für die Aufzeichnung von Amazon EBS-Volumes konfiguriert ist.	
Führen Sie die Regel aus.	1. Folgen Sie den Anweisungen unter Auswerten Ihrer Ressourcen in der AWS Config-Dokumentation, um die `ec2-volume-inuse-check` Regel auszuführen. Warten Sie, bis die Auswertung abgeschlossen ist. 2. Wählen Sie auf der Seite Regeln die `ec2-volume-inuse-check` Regel aus und wählen Sie dann für Ressourcen im Bereich die Option Nicht konform aus. 3. Vergewissern Sie sich, dass die Auswertungsergebnisse ein oder mehrere ungenutzte Amazon-EBS-Volumes enthalten.	AWS-Systemadministrator

Konfigurieren der automatischen Behebung von ungenutzten Amazon EBS-Volumes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die automatische Abhilfemaßnahme hinzu.	1. Wählen Sie auf der Seite Regeln die `ec2-volume-inuse-check` Regel aus.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Folgen Sie den Anweisungen unter Automatische Behebung einrichten in der AWS Config-Dokumentation. Beachten Sie Folgendes: 3. Wählen Sie im Abschnitt Details zur Abhilfemaßnahme die Option aus `AWSConfigRemediation-DeleteUnusedEBSVolume` . • Wählen Sie den Ressourcen-ID-Parameter und dann in der Liste aus VolumeId. Zur Laufzeit wird dieser Parameter durch die ID des nicht konformen EBS-Volumes ersetzt. • Geben Sie im Abschnitt Parameter Werte für die folgenden Parameter an: • `CreateSnapshot` – (Optional) Wenn diese Option auf festgelegt ist `true`, erstellt die Automatisierung einen Snapshot des EBS-Volumes, bevor es gelöscht wird. • `AutomationAssumeRole` – Geben Sie den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-Ressourcennamen (ARN) der `AssumeRole` Servicerolle ein, die Sie zuvor erstellt haben.	
Testen Sie die automatische Behebung für die AWS Config-Regel.	1. Wählen Sie in der AWS Config-Konsole auf der Seite Regeln die `ec2-volume-inuse-check` Regel aus. 2. Wählen Sie im Menü Aktionen die Option Auswerten aus. 3. Erlauben Sie der Regel, die nicht konformen Ressourcen auszuwerten, und bestätigen Sie dann, dass die nicht verwendeten Amazon EBS-Volumes gelöscht werden.	AWS-Systemadministrator

Fehlerbehebung

Problem	Lösung
AWS Config spiegelt den Ressourcenstatus nicht genau wider.	Manchmal aktualisiert AWS Config den Status der Ressourcen nicht. Schalten Sie den Recorder aus und schalten Sie ihn dann auf der Seite AWS Config-Einstellungen wieder ein. Der Recorder erfasst den Status der Ressourcen. Bei neu erstellten oder gelöschten Ressourcen kann es einige Zeit dauern, bis der Recorder den aktuellen Status widerspiegelt. Weitere Informationen zu EBS-Volume-Status

Problem	Lösung
	finden Sie unter Volume-Status in der Amazon EC2-Dokumentation.

Zugehörige Ressourcen

- AWSConfigRemediation-DeleteUnusedEBSVolume-Runbook
- EC2-volume-inuse-check Regel
- Behebung nicht konformer AWS-Ressourcen mit AWS Config-Regeln

Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation

Erstellt von Iker Reina Fuente (AWS) und I Bol GSpeedrdi (AWS)

Code-Repository: aws-control-tower-controls-cdk	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Cloudnativ; Infrastruktur; Management und Governance
AWS-Services: AWS CloudFormation; AWS Control Tower; AWS Organizations ; AWS-CDK		

Übersicht

Dieses Muster beschreibt, wie AWS CloudFormation und AWS Cloud Development Kit (AWS CDK) verwendet werden, um präventive, detektivische und proaktive Kontrollen von AWS Control Tower als Infrastructure as Code (IaC) zu implementieren und zu verwalten. Eine Kontrolle (auch bekannt als Integritätsschutz) ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung für Ihre gesamte AWS Control Tower-Umgebung ermöglicht. Sie können beispielsweise Steuerelemente verwenden, um die Protokollierung für Ihre AWS-Konten zu erzwingen und dann automatische Benachrichtigungen zu konfigurieren, wenn bestimmte sicherheitsrelevante Ereignisse auftreten.

AWS Control Tower unterstützt Sie bei der Implementierung präventiver, detektivischer und proaktiver Kontrollen, die Ihre AWS-Ressourcen regeln und die Compliance über mehrere AWS-Konten hinweg überwachen. Jede Kontrolle erzwingt eine einzelne Regel. In diesem Muster verwenden Sie eine bereitgestellte IaC-Vorlage, um anzugeben, welche Kontrollen Sie in Ihrer Umgebung bereitstellen möchten.

AWS Control Tower-Steuerelemente gelten für eine gesamte Organisationseinheit (OU), und die Kontrolle wirkt sich auf jedes AWS-Konto innerhalb der OU aus. Wenn Benutzer also Aktionen in einem Konto in Ihrer Landing Zone ausführen, unterliegt die Aktion den Kontrollen, die für die Organisationseinheit gelten.

Die Implementierung von AWS Control Tower-Kontrollen trägt dazu bei, eine starke Sicherheitsgrundlage für Ihre AWS-Landing Zone zu schaffen. Durch die Verwendung dieses Musters zur Bereitstellung der Kontrollen als IaC über CloudFormation und AWS CDK können Sie die Kontrollen in Ihrer Landing Zone standardisieren und effizienter bereitstellen und verwalten. Diese Lösung verwendet cdk_nag, um die AWS-CDK-Anwendung während der Bereitstellung zu scannen. Dieses Tool prüft, ob die Anwendung die bewährten Methoden von AWS einhält.

Um AWS Control Tower-Steuerelemente als IaC bereitzustellen, können Sie auch HashiCorp Terraform anstelle von AWS-CDK verwenden. Weitere Informationen finden Sie unter Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform.

Zielgruppe

Dieses Muster wird für Benutzer empfohlen, die Erfahrung mit AWS Control Tower, CloudFormationAWS CDK und AWS Organizations haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktive AWS-Konten, die als Organisation in AWS Organizations und einer Landing Zone von AWS Control Tower verwaltet werden. Anweisungen finden Sie unter Erstellen einer Kontostruktur (AWS Well-Architected Labs).
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.
- Knotenpaketmanager (npm), installiert und für das AWS-CDK konfiguriert.
- Voraussetzungen für AWS CDK.
- Berechtigungen zum Annehmen einer vorhandenen AWS Identity and Access Management (IAM)-Rolle in einem Bereitstellungskonto.
- Berechtigungen zum Annehmen einer IAM-Rolle im Verwaltungskonto der Organisation, die zum Bootstrappen von AWS-CDK verwendet werden kann. Die Rolle muss über Berechtigungen zum Ändern und Bereitstellen von CloudFormation Ressourcen verfügen. Weitere Informationen finden Sie unter Bootstrapping in der AWS-CDK-Dokumentation.
- Berechtigungen zum Erstellen von IAM-Rollen und -Richtlinien im Verwaltungskonto der Organisation. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für den Zugriff auf IAM-Ressourcen in der IAM-Dokumentation.
- Wenden Sie die auf der Service-Kontrollrichtlinie (SCP) basierende Kontrolle mit der ID CT.CLOUDFORMATION.PR.1 an. Diese SCP muss aktiviert sein, um proaktive Kontrollen

bereitzustellen. Anweisungen finden Sie unter Verweigern der Verwaltung von Ressourcentypen, Modulen und Hooks innerhalb der AWS- CloudFormation Registrierung .

Einschränkungen

- Dieses Muster enthält Anweisungen für die Bereitstellung dieser Lösung über AWS-Konten hinweg, von einem Bereitstellungskonto bis zum Verwaltungskonto der Organisation. Zu Testzwecken können Sie diese Lösung direkt im Verwaltungskonto bereitstellen, Anweisungen für diese Konfiguration werden jedoch nicht explizit bereitgestellt.

Produktversionen

- Python Version 3.9 oder höher
- npm Version 8.9.0 oder höher

Architektur

Zielarchitektur

Dieser Abschnitt bietet einen allgemeinen Überblick über diese Lösung und die Architektur, die durch den Beispielcode eingerichtet wird. Das folgende Diagramm zeigt Steuerelemente, die über die verschiedenen Konten in der Organisationseinheit bereitgestellt werden.

AWS Control Tower-Steuerelemente werden entsprechend ihrem Verhalten und ihrer Anleitung kategorisiert.

Es gibt drei Haupttypen von Kontrollverhalten:

1. Präventive Kontrollen sollen verhindern, dass Aktionen ausgeführt werden. Diese werden mit Service-Kontrollrichtlinien (SCPs) in AWS Organizations implementiert. Der Status einer präventiven Kontrolle wird entweder erzwungen oder nicht aktiviert. Präventive Kontrollen werden in allen AWS-Regionen unterstützt.
2. Detektivische Kontrollen sind darauf ausgelegt, bestimmte Ereignisse zu erkennen, wenn sie auftreten, und die Aktion in zu protokollieren CloudTrail. Diese werden mit AWS Config-Regeln implementiert. Der Status einer detektivischen Kontrolle ist entweder leer, verletzt oder nicht

aktiviert. Detektivische Kontrollen gelten nur in den AWS-Regionen, die von AWS Control Tower unterstützt werden.

3. Proaktive Kontrollen scannen Ressourcen, die von AWS bereitgestellt werden würden, CloudFormation und überprüfen, ob sie Ihren Unternehmensrichtlinien und -zielen entsprechen. Ressourcen, die nicht konform sind, werden nicht bereitgestellt. Diese werden mit AWS-CloudFormation Hooks implementiert. Der Status einer proaktiven Kontrolle lautet PASS , FAIL oder SKIP .

Die Anleitung zur Kontrolle bezieht sich auf die empfohlene Praxis, wie jede Kontrolle auf Ihre OUs. AWS Control Tower bietet drei Kategorien von Leitlinien: obligatorische , dringend empfohlene und gewählte . Die Anleitung einer Kontrolle ist unabhängig von ihrem Verhalten. Weitere Informationen finden Sie unter Kontrollverhalten und Anleitung.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können. Das AWS CDK Toolkit ist das primäre Tool für die Interaktion mit Ihrer AWS CDK-App.
- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und wie sie konfiguriert sind. Auf diese Weise können Sie feststellen, wie Ressourcen miteinander in Beziehung stehen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Control Tower unterstützt Sie bei der Einrichtung und Verwaltung einer AWS-Umgebung mit mehreren Konten gemäß den bewährten Methoden.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

Andere Tools

- cdk_nag ist ein Open-Source-Tool, das eine Kombination von Regelpaketen verwendet, um AWS Cloud Development Kit (AWS CDK)-Anwendungen auf die Einhaltung bewährter Methoden zu überprüfen.

- npm ist eine Softwareregistrierung, die in einer Node.js-Umgebung ausgeführt wird und verwendet wird, um Pakete freizugeben oder zu leihen und die Bereitstellung privater Pakete zu verwalten.
- Python ist eine universelle Computer-Programmiersprache.

Code-Repository

Der Code für dieses Muster ist in den GitHub Steuerelementen Bereitstellen von AWS Control Tower mit AWS-CDK-Repository verfügbar. Sie verwenden die Datei cdk.json, um mit der AWS-CDK-App zu interagieren, und Sie verwenden die Datei package.json, um die npm-Pakete zu installieren.

Bewährte Methoden

- Folgen Sie dem Prinzip der geringsten Berechtigung (IAM-Dokumentation). Die in diesem Muster bereitgestellte IAM-Beispielrichtlinie und Vertrauensrichtlinie enthalten die erforderlichen Mindestberechtigungen, und die im Verwaltungskonto erstellten AWS-CDK-Stacks sind durch diese Berechtigungen eingeschränkt.
- Folgen Sie den bewährten Methoden für AWS Control Tower-Administratoren (Dokumentation zu AWS Control Tower).
- Folgen Sie den bewährten Methoden für die Entwicklung und Bereitstellung der Cloud-Infrastruktur mit dem AWS-CDK (AWS-CDK-Dokumentation).
- Passen Sie beim Bootstrapping des AWS-CDK die Bootstrap-Vorlage an, um Richtlinien und die vertrauenswürdigen Konten zu definieren, die über die Möglichkeit verfügen sollten, jede Ressource im Verwaltungskonto zu lesen und zu schreiben. Weitere Informationen finden Sie unter Bootstrapping anpassen.
- Verwenden Sie Codeanalyse-Tools wie cfn_nag, um die generierten CloudFormation Vorlagen zu scannen. Das Tool cfn-nag sucht in CloudFormation Vorlagen nach Mustern, die darauf hinweisen könnten, dass die Infrastruktur nicht sicher ist. Sie können cdk-nag auch verwenden, um Ihre CloudFormation Vorlagen mithilfe des cloudformation-include-Moduls zu überprüfen.

Sekunden

Vorbereiten der Aktivierung der Kontrollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle im Verwaltungskonto.	1. Erstellen Sie eine IAM-Richtlinie im Verwaltungskonto mit den Berechtigungen, die in der IAM-Richtlinie im Abschnitt Zusätzliche Informationen definiert sind. Anweisungen finden Sie unter Erstellen von IAM-Richtlinien in der IAM-Dokumentation. Notieren Sie sich den Amazon-Ressourcennamen (ARN) der Richtlinie. Im Folgenden finden Sie ein Beispiel für einen ARN. `arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>` 2. Erstellen Sie eine IAM-Rolle im Verwaltungskonto, fügen Sie die IAM-Berechtigungsrichtlinie an, die Sie im vorherigen Schritt erstellt haben, und fügen Sie die benutzerdefinierte Vertrauensrichtlinie in Vertrauensrichtlinie im Abschnitt Zusätzliche Informationen an.	DevOps -Techniker, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien in der IAM-Dokumentation. Im Folgenden finden Sie ein Beispiel für einen ARN für die neue Rolle. `arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:role/<ROLE-NAME>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrappen Sie AWS-CDK.	1. Übernehmen Sie im Verwaltungskonto eine Rolle, die über Berechtigungen zum Bootstrappen von AWS-CDK verfügt. 2. Geben Sie den folgenden Befehl ein und ersetzen Sie Folgendes: • `<MANAGEMENT-ACCOUNT-ID>` ist die ID des Verwaltungskontos der Organisation. • `<AWS-CONTROL-TOWER-REGION>` ist die AWS-Region, in der Control Tower bereitgestellt wird. Eine vollständige Liste der Regionscodes finden Sie unter Regionale Endpunkte in der Allgemeinen AWS-Referenz. • `<DEPLOYMENT-ACCOUNT-ID>` ist die ID des Bereitstellungskontos. • `<DEPLOYMENT-ROLE-NAME>` ist der Name der IAM-Rolle, die Sie für das Bereitstellungskonto verwenden. • `<POLICY-NAME>` ist der Name der Richtlinie, die	DevOps Ingenieur, Allgemeines AWS, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie im Verwaltungskonto erstellt haben. `$ npx cdk bootstrap aws://<MANAGEMENT-ACCOUNT-ID>/<AWS-CONTROL-TOWER-REGION> \ --trust arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-NAME> \ --cloudformation-execution-policies arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`	
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dadurch werden die Steuerelemente von AWS Control Tower mithilfe des AWS-CDK-Repositorys von geklont GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-cdk.git`	DevOps -Techniker, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die AWS-CDK-Konfigurationsdatei.	1. Öffnen Sie im geklonten Repository die Datei constants.py. 2. Geben Sie im `ACCOUNT_ID` Parameter die ID Ihres Verwaltungskontos ein. 3. Geben Sie im `<AWS-CONTROL-TOWER-REGION>` Parameter die AWS-Region ein, in der AWS Control Tower bereitgestellt wird. 4. Geben Sie im `ROLE_ARN` Parameter den ARN der Rolle ein, die Sie im Verwaltungskonto erstellt haben. 5. Geben Sie im `GUARDRAILS_CONFIGURATION` Abschnitt im `Enable-Control` Parameter die Steuerelement-API-Kennungen ein. Geben Sie die Kennung in doppelte Anführungszeichen ein und trennen Sie mehrere Kennungen durch Kommas. Jede Kontrolle hat eine eindeutige API-ID für jede Region, in der AWS Control Tower verfügbar ist. Gehen Sie wie folgt vor, um die Kontrollkennung zu finden:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	a. Suchen Sie in Tabellen mit Kontrollmetadaten das Steuerelement, das Sie aktivieren möchten. b. Suchen Sie in der Spalte Kontroll-API-Kennungen nach Region die API-Kennung für die Region, in der Sie den API-Aufruf ausführen, z. B. `arn:aws:controltower:us-east-1::control/AWS-GR_ENCRYPTED_VOLUMES` . c. Extrahieren Sie die Kontrollkennung aus der regionalen Kennung, z. B. `AWS-GR_ENCRYPTED_VOLUMES` . 6. Geben Sie im `GUARDRAILS_CONFIGURATION` Abschnitt im `OrganizationalUnitIds` Parameter die ID der Organisationseinheit ein, in der Sie die Kontrolle aktivieren möchten, z. B. `ou-1111-11111111` . Geben Sie die ID in doppelte Anführungszeichen ein und trennen Sie mehrere IDs durch Kommas. Weitere Informati	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen zum Abrufen von OU-IDs finden Sie unter Anzeigen der Details einer OU. 7. Speichern und schließen Sie die Datei constants .py. Ein Beispiel für eine aktualisierte constants .py-Datei finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	

Aktivieren von Kontrollen im Verwaltungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übernehmen Sie die IAM-Rolle im Bereitstellungskonto.	Übernehmen Sie im Bereitstellungskonto die IAM-Rolle, die über Berechtigungen zum Bereitstellen der AWS-CDK-Stacks im Verwaltungskonto verfügt. Weitere Informationen zum Annehmen einer IAM-Rolle in der AWS CLI finden Sie unter Verwenden einer IAM-Rolle in der AWS CLI.	DevOps -Techniker, Allgemeines AWS
Aktivieren Sie die Umgebung.	Wenn Sie Linux oder MacOS verwenden: 1. Geben Sie den folgenden Befehl ein, um eine virtuelle Umgebung zu erstellen.	DevOps -Techniker, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	$ python3 -m
	 venv .venv
	``
	2. Nachdem die virtuelle Umgebung erstellt wurde, geben Sie den folgenden Befehl ein, um sie zu aktivieren.
	``
	$ source .venv/bin/
	activate
	``
	Wenn Sie Windows verwenden:
	1. Geben Sie den folgenden Befehl ein, um eine virtuelle Umgebung zu aktivieren.
	``
	% .venv\Scripts\acti
	vate.bat
	``	

Installieren Sie die Abhängigkeiten.	Nachdem die virtuelle Umgebung aktiviert wurde, geben Sie den folgenden Befehl ein, um das Skript install_deps.sh auszuführen. Dieses Skript installiert die erforderlichen Abhängigkeiten. ``` $ ./scripts/install_ deps.sh ```	DevOps Ingenieur, Allgemeines AWS, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Stack bereit.	Geben Sie die folgenden Befehle ein, um den CloudFormation Stack zu synthetisieren und bereitzustellen.
	`$ npx cdk synth`
	`$ npx cdk deploy`
		DevOps Ingenieur, Allgemeines AWS, Python

Zugehörige Ressourcen

AWS-Dokumentation

- Informationen zu Kontrollen (Dokumentation zu AWS Control Tower)
- Steuerbibliothek (Dokumentation zu AWS Control Tower)
- AWS-CDK-Toolkit-Befehle (AWS-CDK-Dokumentation)
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform (AWS Prescriptive Guidance)

Sonstige Ressourcen

- Python

Zusätzliche Informationen

Beispieldatei constants.py

Im Folgenden finden Sie ein Beispiel für eine aktualisierte constants.py-Datei.

```
ACCOUNT_ID = 111122223333
AWS_CONTROL_TOWER_REGION = us-east-2
ROLE_ARN = "arn:aws:iam::111122223333:role/CT-Controls-Role"
GUARDRAILS_CONFIGURATION = [
    {
        "Enable-Control": {
```

```
            "AWS-GR_ENCRYPTED_VOLUMES",
            ...
        },
        "OrganizationalUnitIds": ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        "Enable-Control": {
            "AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED",
            ...
        },
        "OrganizationalUnitIds": ["ou-2222-22222222"...],
    },
]
```

IAM-Richtlinie

Die folgende Beispielrichtlinie erlaubt die Mindestaktionen, die erforderlich sind, um AWS Control Tower-Steuerelemente zu aktivieren oder zu deaktivieren, wenn AWS CDK-Stacks von einem Bereitstellungskonto für das Verwaltungskonto bereitgestellt werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
```

```
                "organizations:UpdatePolicy",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
    ]
}
```

Vertrauensrichtlinie

Die folgende benutzerdefinierte Vertrauensrichtlinie ermöglicht es einer bestimmten IAM-Rolle im Bereitstellungskonto, die IAM-Rolle im Verwaltungskonto zu übernehmen. Ersetzen Sie Folgendes:

- <DEPLOYMENT-ACCOUNT-ID> ist die ID des Bereitstellungskontos
- <DEPLOYMENT-ROLE-NAME> ist der Name der Rolle im Bereitstellungskonto, die die Rolle im Verwaltungskonto übernehmen darf

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Effect”: “Allow”,
            “Principal”: {
                “AWS”: “arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-
NAME>”
            },
            “Action”: “sts:AssumeRole”,
            “Condition”: {}
        }
    ]
}
```

Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform

Erstellt von Iker Reina Fuente (AWS) und I Bol GSpeedrdi (AWS)

Code-Repository: Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von Terraform	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Cloudnativ; Infrastruktur; Management und Governance
Workload: Open-Source	AWS-Services: AWS Control Tower; AWS Organizations	

Übersicht

Dieses Muster beschreibt, wie Sie Steuerelemente von AWS Control Tower, HashiCorp Terraform und Infrastructure as Code (IaC) verwenden, um präventive, detektivische und proaktive Sicherheitskontrollen zu implementieren und zu verwalten. Eine Kontrolle (auch bekannt als Integritätsschutz) ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung für Ihre gesamte AWS Control Tower-Umgebung bietet. Sie können beispielsweise Steuerelemente verwenden, um die Protokollierung für Ihre AWS-Konten zu erzwingen und dann automatische Benachrichtigungen zu konfigurieren, wenn bestimmte sicherheitsrelevante Ereignisse auftreten.

AWS Control Tower unterstützt Sie bei der Implementierung präventiver, detektivischer und proaktiver Kontrollen, die Ihre AWS-Ressourcen regeln und die Compliance über mehrere AWS-Konten hinweg überwachen. Jede Kontrolle erzwingt eine einzelne Regel. In diesem Muster verwenden Sie eine bereitgestellte IaC-Vorlage, um anzugeben, welche Kontrollen Sie in Ihrer Umgebung bereitstellen möchten.

AWS Control Tower-Steuerelemente gelten für eine gesamte Organisationseinheit (OU), und die Kontrolle wirkt sich auf jedes AWS-Konto innerhalb der OU aus. Wenn Benutzer also Aktionen in einem Konto in Ihrer Landing Zone ausführen, unterliegt die Aktion den Kontrollen, die für die Organisationseinheit gelten.

Die Implementierung von AWS Control Tower-Kontrollen trägt dazu bei, eine starke Sicherheitsgrundlage für Ihre AWS-Landing Zone zu schaffen. Durch die Verwendung dieses Musters

zur Bereitstellung der Kontrollen als IaC über Terraform können Sie die Kontrollen in Ihrer Landing Zone standardisieren und effizienter bereitstellen und verwalten.

Um AWS Control Tower-Steuerelemente als IaC bereitzustellen, können Sie auch AWS Cloud Development Kit (AWS CDK) anstelle von Terraform verwenden. Weitere Informationen finden Sie unter Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation.

Zielgruppe

Dieses Muster wird für Benutzer empfohlen, die Erfahrung mit AWS Control Tower, Terraform und AWS Organizations haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktive AWS-Konten, die als Organisation in AWS Organizations und einer Landing Zone von AWS Control Tower verwaltet werden. Anweisungen finden Sie unter Erstellen einer Kontostruktur (AWS Well-Architected Labs).
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.
- Eine AWS Identity and Access Management (IAM)-Rolle im Verwaltungskonto, die über Berechtigungen zum Bereitstellen dieses Musters verfügt. Weitere Informationen zu den erforderlichen Berechtigungen und eine Beispielrichtlinie finden Sie unter Geringste Berechtigungen für die IAM-Rolle im Abschnitt Zusätzliche Informationen dieses Musters.
- Berechtigungen zum Annehmen der IAM-Rolle im Verwaltungskonto.
- Wenden Sie die auf der Service-Kontrollrichtlinie (SCP) basierende Kontrolle mit der ID CT.CLOUDFORMATION.PR.1 an. Diese SCP muss aktiviert sein, um proaktive Kontrollen bereitzustellen. Anweisungen finden Sie unter Verweigern der Verwaltung von Ressourcentypen, Modulen und Hooks innerhalb der AWS- CloudFormation Registrierung .
- Terraform-CLI, installiert (Terraform-Dokumentation).
- Terraform-AWS-Anbieter, konfiguriert (Terraform-Dokumentation).
- Terraform-Backend, konfiguriert (Terraform-Dokumentation).

Produktversionen

- AWS Control Tower Version 3.0 oder höher

- Terraform Version 1.5 oder höher
- Terraform AWS Provider Version 4.67 oder höher

Architektur

Zielarchitektur

Dieser Abschnitt bietet einen allgemeinen Überblick über diese Lösung und die Architektur, die durch den Beispielcode eingerichtet wird. Das folgende Diagramm zeigt Steuerelemente, die über die verschiedenen Konten in der Organisationseinheit bereitgestellt werden.

AWS Control Tower-Steuerelemente werden entsprechend ihrem Verhalten und ihrer Anleitung kategorisiert.

Es gibt drei Haupttypen von Kontrollverhalten:

1. Präventive Kontrollen sollen verhindern, dass Aktionen ausgeführt werden. Diese werden mit Service-Kontrollrichtlinien (SCPs) in AWS Organizations implementiert. Der Status einer präventiven Kontrolle wird entweder erzwungen oder nicht aktiviert. Präventive Kontrollen werden in allen AWS-Regionen unterstützt.
2. Detektivische Kontrollen sind darauf ausgelegt, bestimmte Ereignisse zu erkennen, wenn sie auftreten, und die Aktion in zu protokollieren CloudTrail. Diese werden mit AWS Config-Regeln implementiert. Der Status einer detektivischen Kontrolle ist entweder leer, verletzt oder nicht aktiviert. Detektivische Kontrollen gelten nur in den AWS-Regionen, die von AWS Control Tower unterstützt werden.
3. Proaktive Kontrollen scannen Ressourcen, die von AWS bereitgestellt werden würden, CloudFormation und überprüfen, ob sie Ihren Unternehmensrichtlinien und -zielen entsprechen. Ressourcen, die nicht konform sind, werden nicht bereitgestellt. Diese werden mit AWS-CloudFormation Hooks implementiert. Der Status einer proaktiven Kontrolle lautet PASS , FAIL oder SKIP .

Die Anleitung zur Kontrolle ist die empfohlene Methode, um jede Kontrolle auf Ihre OUs anzuwenden. AWS Control Tower bietet drei Kategorien von Leitlinien: obligatorische , dringend empfohlene und gewählte . Die Anleitung einer Kontrolle ist unabhängig von ihrem Verhalten. Weitere Informationen finden Sie unter Kontrollverhalten und Anleitung.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und wie sie konfiguriert sind. Auf diese Weise können Sie feststellen, wie Ressourcen miteinander in Beziehung stehen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Control Tower unterstützt Sie bei der Einrichtung und Verwaltung einer AWS-Umgebung mit mehreren Konten gemäß den bewährten Methoden.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie zentral erstellen und verwalten.

Andere Tools

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastructure as Code (IaC), mit dem Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.

Code-Repository

Der Code für dieses Muster ist im GitHub Steuerelement Bereitstellen und Verwalten von AWS Control Tower mithilfe des Terraform-Repositorys verfügbar.

Bewährte Methoden

- Die IAM-Rolle, die zur Bereitstellung dieser Lösung verwendet wird, sollte dem Prinzip der geringsten Berechtigung entsprechen (IAM-Dokumentation).
- Folgen Sie den bewährten Methoden für AWS Control Tower-Administratoren (Dokumentation zu AWS Control Tower).

Sekunden

Aktivieren von Kontrollen im Verwaltungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dadurch werden die Kontrollen von AWS Control Tower mithilfe des Terraform-Repositorys von geklont und verwaltet GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-terraform.git`	DevOps Techniker
Bearbeiten Sie die Terraform-Backend-Konfigurationsdatei.	1. Öffnen Sie im geklonten Repository die Datei backend.tf. 2. Bearbeiten Sie die -Datei, um die Terraform-Backend-Konfiguration festzulegen. Die Konfiguration, die Sie in dieser Datei definieren, hängt von Ihrer Umgebung ab. Weitere Informationen finden Sie unter Backend-Konfiguration (Terraform-Dokumentation). 3. Speichern und schließen Sie die Datei backend.tf.	DevOps Techniker, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Konfigurationsdatei des Terraform-Anbieters.	1. Öffnen Sie im geklonten Repository die Datei provider.tf. 2. Bearbeiten Sie die -Datei, um die Konfiguration des Terraform-Anbieters festzulegen. Weitere Informationen finden Sie unter Anbieterkonfiguration (Terraform-Dokumentation). Legen Sie die AWS-Region als Region fest, in der die AWS Control Tower-API verfügbar ist. 3. Speichern und schließen Sie die Datei provider.tf.	DevOps Techniker, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Konfigurationsdatei.	1. Öffnen Sie im geklonten Repository die Datei Variablen.tfvars. 2. Geben Sie im `controls` Abschnitt im `control_names` Parameter die ID der Steuerelement-API ein. Jede Kontrolle hat eine eindeutige API-ID für jede Region, in der AWS Control Tower verfügbar ist. Gehen Sie wie folgt vor, um die Kontrollkennung zu finden: a. Suchen Sie in Tabellen mit Kontrollmetadaten nach der Kontrolle, die Sie aktivieren möchten. b. Suchen Sie in der Spalte Steuer-API-Kennungen nach Region die API-Kennung für die Region, in der Sie den API-Aufruf ausführen, z. B. `arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED` . c. Extrahieren Sie die Kontrollkennung aus der regionalen Kennung, z. B. `AWS-GR_AUDIT_BUCKE`	DevOps Ingenieur, Allgemeines AWS, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`T_ENCRYPT ION_ENABLED` . 3. Geben Sie im `controls` Abschnitt im `organizat ional_unit_ids` Parameter die ID der Organisationseinheit ein, in der Sie die Kontrolle aktivieren möchten, z. B. `ou-1111-11111111` . Geben Sie die ID in doppelte Anführung szeichen ein und trennen Sie mehrere IDs durch Kommas. Weitere Informati onen zum Abrufen von OU-IDs finden Sie unter Anzeigen der Details einer OU. 4. Speichern und schließen Sie die Datei Variablen .tfvars. Ein Beispiel für eine aktualisierte Datei Variablen.tfvars finden Sie im Abschnitt Zusätzlic he Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übernehmen Sie die IAM-Rolle im Verwaltungskonto.	Übernehmen Sie im Verwaltungskonto die IAM-Rolle, die über Berechtigungen zum Bereitstellen der Terraform-Konfigurationsdatei verfügt. Weitere Informationen zu den erforderlichen Berechtigungen und eine Beispielrichtlinie finden Sie unter Geringste Berechtigungen für die IAM-Rolle im Abschnitt Zusätzliche Informationen. Weitere Informationen zum Übernehmen einer IAM-Rolle in der AWS CLI finden Sie unter Verwenden einer IAM-Rolle in der AWS CLI.	DevOps -Techniker, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Konfigurationsdatei bereit.	1. Geben Sie den folgenden Befehl ein, um Terraform zu initialisieren.
	`$ terraform init -upgrade`
	2. Geben Sie den folgenden Befehl ein, um eine Vorschau der Änderungen im Vergleich zum aktuellen Status anzuzeigen.
	`$ terraform plan -var-file="variables.tfvars"`
	3. Überprüfen Sie die Konfigurationsänderungen im Terraform-Plan und bestätigen Sie, dass Sie diese Änderungen in der Organisation implementieren möchten.
	4. Geben Sie den folgenden Befehl ein, um die Ressourcen bereitzustellen.
	`$ terraform apply -var-file="variables.tfvars"`
		DevOps Ingenieur, Allgemeines AWS, Terraform

(Optional) Deaktivieren von Kontrollen im AWS Control Tower-Verwaltungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Befehl Destroy aus.	Geben Sie den folgenden Befehl ein, um die durch dieses Muster bereitgestellten Ressourcen zu entfernen. `$ terraform destroy -var-file="variables.tfvars"`	DevOps Ingenieur, Allgemeines AWS, Terraform

Fehlerbehebung

Problem	Lösung
`Error: creating ControlTower Control ValidationException: Guardrail <control ID> is already enabled on organizational unit <OU ID>`-Fehler	Das Steuerelement, das Sie aktivieren möchten, ist bereits in der Ziel-OU aktiviert . Dieser Fehler kann auftreten, wenn ein Benutzer die Kontrolle manuell über die AWS-Managementkonsole, über AWS Control Tower oder über AWS Organizations aktiviert hat. Um die Terraform-Konfigurationsdatei bereitzustellen, können Sie eine der folgenden Optionen verwenden. Option 1: Aktualisieren der aktuellen Terraform-Zustandsdatei Sie können die Ressource in die aktuelle Statusdatei von Terraform importieren. Wenn Sie den `apply` Befehl erneut ausführen, überspringt Terraform diese Ressource. Gehen Sie wie folgt vor, um die Ressource in den aktuellen Terraform-Status zu importieren:

Problem	Lösung

	1. Geben Sie im AWS Control Tower-Verwaltungskonto den folgenden Befehl ein, um eine Liste der Amazon-Ressourcennamen (ARNs) für die OUs abzurufen, wobei der Organisationsstamm `<root-ID>` ist. Weitere Informationen zum Abrufen dieser ID finden Sie unter Anzeigen der Details des Stamm-.
	`aws organizations list-organizational-units-for-parent --parent-id <root-ID>`
	2. Geben Sie für jede im vorherigen Schritt zurückgegebene Organisationseinheit den folgenden Befehl ein, wobei der ARN der Organisationseinheit `<OU-ARN>` ist.
	`aws controltower list-enabled-controls --target-identifier <OU-ARN>`
	3. Kopieren Sie die ARNs und führen Sie den Terraform-Import im erforderlichen Modul durch, damit er im Terraform-Status enthalten ist. Anweisungen finden Sie unter Import ieren(Terraform-Dokumentation).
	4. Wiederholen Sie die Schritte unter Bereitstellen der Konfiguration im Abschnitt Telefonie.
	
	Option 2: Deaktivieren der Kontrolle
	
	Wenn Sie in einer Nicht-Produktionsumgebung arbeiten, können Sie die Kontrolle in der Konsole deaktivieren. Aktivieren Sie sie erneut, indem Sie die Schritte unter Bereitstellen der Konfiguration im Abschnitt „Pics“ wiederholen.

Problem	Lösung
	Dieser Ansatz wird für Produktionsumgebungen nicht empfohlen, da es einen Zeitraum gibt, in dem die Kontrolle deaktiviert wird. Wenn Sie diese Option in einer Produktionsumgebung verwenden möchten, können Sie temporäre Kontrollen implementieren, z. B. die vorübergehende Anwendung eines SCP in AWS Organizations.

Zugehörige Ressourcen

AWS-Dokumentation

- Informationen zu Kontrollen (Dokumentation zu AWS Control Tower)
- Steuerbibliothek (Dokumentation zu AWS Control Tower)
- Bereitstellen und Verwalten von AWS Control Tower-Steuerelementen mithilfe von AWS CDK und AWS CloudFormation (AWS Prescriptive Guidance)

Sonstige Ressourcen

- Terraform
- Terraform-CLI-Dokumentation

Zusätzliche Informationen

Beispieldatei Variablen.tfvars

Im Folgenden finden Sie ein Beispiel für eine aktualisierte Datei Variablen.tfvars.

```
controls = [
    {
        control_names = [
            "AWS-GR_ENCRYPTED_VOLUMES",
            ...
        ],
```

```
        organizational_unit_ids = ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        control_names = [
            "AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED",
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111"...],
    },
]
```

Geringste Berechtigungen für die IAM-Rolle

Dieses APG-Muster erfordert, dass Sie eine IAM-Rolle im Verwaltungskonto übernehmen. Die bewährte Methode besteht darin, eine Rolle mit temporären Berechtigungen zu übernehmen und die Berechtigungen gemäß dem Prinzip der geringsten Berechtigung einzuschränken. Die folgende Beispielrichtlinie erlaubt die Mindestaktionen, die zum Aktivieren oder Deaktivieren von AWS Control Tower-Steuerelementen erforderlich sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme in mehreren Codeergebnissen gleichzeitig erkennt

Code-Repository: Einfache Pipeline zum Scannen von Code	Umgebung: PoC oder Pilot	Technologien: Sicherheit, Identität, Einhaltung von Vorschriften; DevOps
AWS-Dienste: AWS CloudFormation CodeBuild; AWS CodeCommit; AWS CodePipeline		

Übersicht

Die Simple Code Scanning Pipeline (SCSP) ermöglicht die Erstellung einer Codeanalysepipeline mit zwei Klicks, in der branchenübliche Open-Source-Sicherheitstools parallel ausgeführt werden. Auf diese Weise können Entwickler die Qualität und Sicherheit ihres Codes überprüfen, ohne Tools installieren oder auch nur verstehen zu müssen, wie sie ausgeführt werden. Auf diese Weise können Sie Sicherheitslücken und Fehlkonfigurationen in den Code-Ergebnissen reduzieren. Es reduziert auch den Zeitaufwand, den Ihr Unternehmen mit der Installation, Recherche und Konfiguration von Sicherheitstools verbringt.

Vor SCSP mussten Entwickler beim Scannen von Code mithilfe dieser speziellen Toolsuite die Softwareanalysetools ausfindig machen, manuell installieren und konfigurieren. Selbst lokal installierte all-in-one Tools wie Automated Security Helper (ASH) erfordern die Konfiguration eines Docker-Containers, damit sie ausgeführt werden können. Mit SCSP wird jedoch eine Suite von branchenüblichen Codeanalyse-Tools automatisch im ausgeführt. AWS Cloud Bei dieser Lösung verwenden Sie Git, um Ihre Codeergebnisse zu pushen. Anschließend erhalten Sie eine visuelle Ausgabe mit at-a-glance Informationen darüber, welche Sicherheitsüberprüfungen fehlgeschlagen sind.

Voraussetzungen und Einschränkungen

- Ein aktiver AWS-Konto
- Ein oder mehrere Codeergebnisse, die Sie auf Sicherheitsprobleme überprüfen möchten

- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Python Version 3.0 oder höher und Pip-Version 9.0.3 oder höher, installiert
- Git, installiert
- Installieren Sie git-remote-codecommit auf Ihrer lokalen Workstation

Architektur

Zieltechnologie-Stack

- AWS CodeCommit Repositorium
- AWS CodeBuild Projekt
- AWS CodePipeline Pipeline
- Amazon Simple Storage Service (Amazon S3)-Bucket
- AWS CloudFormation Vorlage

Zielarchitektur

Das SCSP für die statische Codeanalyse ist ein DevOps Projekt, das darauf abzielt, Sicherheitsfeedback zu lieferbarem Code zu geben.

1. Melden Sie AWS Management Console sich in der beim Ziel AWS-Konto an. Vergewissern Sie sich, dass Sie sich an dem AWS-Region Ort befinden, an dem Sie die Pipeline bereitstellen möchten.
2. Verwenden Sie die CloudFormation Vorlage im Code-Repository, um den SCSP-Stack bereitzustellen. Dadurch werden ein neues CodeCommit Repository und ein neues CodeBuild Projekt erstellt.

   Hinweis: Als alternative Bereitstellungsoption können Sie eine vorhandene verwenden, CodeCommit indem Sie bei der Stack-Bereitstellung den Amazon-Ressourcennamen (ARN) des Repositorys als Parameter angeben.

3. Klonen Sie das Repository auf Ihre lokale Workstation und fügen Sie dann alle Dateien zu den entsprechenden Ordnern im geklonten Repository hinzu.

4. Verwende Git, um die Dateien hinzuzufügen, zu übertragen und in das CodeCommit Repository zu übertragen.
5. Durch das Pushen in das CodeCommit Repository wird ein CodeBuild Job initiiert. Das CodeBuild Projekt verwendet die Sicherheitstools, um die im Code enthaltenen Ergebnisse zu scannen.
6. Überprüfen Sie die Ausgabe der Pipeline. Sicherheitstools, die Probleme auf Fehlerebene gefunden haben, führen zu fehlgeschlagenen Aktionen in der Pipeline. Korrigieren Sie diese Fehler oder unterdrücken Sie sie als Fehlalarme. Überprüfen Sie die Details der Tool-Ausgabe in den Aktionsdetails im CodePipeline oder im S3-Bucket der Pipeline.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.

Andere Tools

Eine vollständige Liste der Tools, die SCSP zum Scannen von Codeergebnissen verwendet, finden Sie in der SCSP-Readme-Datei unter. GitHub

Code-Repository

Der Code für dieses Muster ist im Simple Code Scanning Pipeline (SCSP) -Repository unter verfügbar. GitHub

Epen

Stellen Sie das SCSP bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CloudFormation Stapel.	1. Melden Sie sich an der AWS Management Console an. 2. Vergewissern Sie sich in der Konsole, dass Sie sich in der Zielregion befinden, in der Sie die Lösung bereitstellen möchten. Weitere Informationen finden Sie unter Region auswählen. 3. Wählen Sie den folgenden Link. Dadurch wird der Assistent zum schnellen Erstellen von Stacks in geöffnet CloudFormation. https://console.aws.amazon.com/cloudformation/home?#/stacks/create/review?templateURL=https://proservetools.s3.amazonaws.com/cft/scsp-pipeline-stack.template.json&stackName = SimpleCode ScanPipeline 4. Überprüfen Sie im Assistenten zum Quick Create Stack die Parametereinstellungen für Ihren Stack und	AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nehmen Sie die für Ihren Anwendungsfall erforderl ichen Änderungen vor. 5. Wählen Sie Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Resso urcen erstellt, und wählen Sie dann Stack erstellen aus. Dadurch werden ein CodeCommit Repository, eine CodePipeline Pipeline, mehrere CodeBuild Jobdefini tionen und ein S3-Bucket erstellt. Build-Läufe und Scan-Ergebnisse werden in diesen Bucket kopiert. Nachdem der CloudFormation Stack vollständig bereitgestellt wurde, ist SCSP einsatzbereit.	

Verwenden Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen Sie die Ergebnisse des Scans.	1. Wählen Sie in der Amazon S3 S3-Konsole unter Buckets den Bucket simplecodescanpipeline-deleteresourcespipelineeso aus. 2. Wählen Sie das Verzeichn is scan_results und dann	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Ordner mit dem letzten Scandatumsstempel. 3. Überprüfen Sie die Protokoll dateien in diesem Ordner, um alle Probleme zu überprüfen, die von den in der Pipeline verwendeten Sicherheitstools entdeckt wurden. Sicherheitstools, die Probleme auf Fehlerebe ne gefunden haben, führen zu `failed` laufenden Aktionen. Diese müssen behoben oder unterdrückt werden, wenn es sich um Fehlalarme handelt. Hinweis: Sie können sich auch Details der Tool-Ausg abe (sowohl für erfolgrei che als auch für fehlgesch lagene Scans) in der CodePipeline Konsole im Abschnitt Aktionsdetails ansehen.	

Fehlerbehebung

Problem	Lösung
HashiCorp Terraform oder AWS CloudForm ation Dateien werden nicht gescannt.	Stellen Sie sicher, dass Terraform-Dateien (.tf) und CloudFormation (.yml, .yaml oder .json) in den entsprechenden Ordnern im geklonten Repository abgelegt werden. CodeCommit

Problem	Lösung
Der `git clone` Befehl schlägt fehl.	Stellen Sie sicher, dass Sie die Installation installiert haben `git-remote-codecommit` und dass Ihre CLI Zugriff auf AWS Anmeldeinformationen hat, die zum Lesen des CodeCommit Repositorys berechtigt sind.
Ein Parallelitätsfehler, wie z. B. `Project-level concurrent build limit cannot exceed the account-level concurrent build limit of 1`	Führen Sie die Pipeline erneut aus, indem Sie in der Konsole auf die CodePipeline Schaltfläche Release Change klicken. Dies ist ein bekanntes Problem, das bei den ersten Versuchen, in denen die Pipeline ausgeführt wird, offenbar am häufigsten auftritt.

Zugehörige Ressourcen

Geben Sie Feedback zum SCSP-Projekt.

Zusätzliche Informationen

HÄUFIG GESTELLTE FRAGEN

Ist das SCSP-Projekt dasselbe wie Automated Security Helper (ASH)?

Nein. Verwenden Sie ASH, wenn Sie ein CLI-Tool benötigen, das Code-Scan-Tools mithilfe von Containern ausführt. Automated Security Helper (ASH) ist ein Tool, mit dem die Wahrscheinlichkeit einer Sicherheitsverletzung in einer neuen Code-, Infrastruktur- oder IAM-Ressourcenkonfiguration verringert werden soll. ASH ist ein Befehlszeilenprogramm, das lokal ausgeführt werden kann. Für die lokale Verwendung muss eine Container-Umgebung auf dem System installiert und betriebsbereit sein.

Verwenden Sie SCSP, wenn Sie eine einfachere Setup-Pipeline als ASH benötigen. SCSP erfordert keine lokalen Installationen. SCSP ist so konzipiert, dass Prüfungen einzeln in einer Pipeline ausgeführt und die Ergebnisse nach Tools angezeigt werden. SCSP vermeidet außerdem einen Großteil des Aufwands bei der Einrichtung von Docker und ist betriebssystemunabhängig (OS).

Ist SCSP nur für Sicherheitsteams gedacht?

Nein, jeder kann die Pipeline einsetzen, um festzustellen, welche Teile seines Codes die Sicherheitsüberprüfungen nicht bestehen. Benutzer, die keine Sicherheitsprobleme haben, können beispielsweise SCSP verwenden, um ihren Code zu überprüfen, bevor sie ihn mit ihren Sicherheitsteams überprüfen.

Kann ich SCSP verwenden, wenn ich mit einem anderen Repository-Typ wie GitLab GitHub, oder Bitbucket arbeite?

Du kannst ein lokales Git-Repository so konfigurieren, dass es auf zwei verschiedene Remote-Repositorys verweist. Sie könnten beispielsweise ein vorhandenes GitLab Repository klonen, eine SCSP-Instanz erstellen (mit Angabe CloudFormation von Terraform- und AWS RDK-Ordnern (AWS Config Rules Development Kit), falls erforderlich) und dann das lokale Repository auch auf das SCSP-Repository verweisen. `git remote add upstream <SCSPGitLink>` CodeCommit Auf diese Weise können Codeänderungen zuerst an SCSP gesendet, validiert und dann, nachdem weitere Aktualisierungen vorgenommen wurden, um die Ergebnisse zu korrigieren, in das, ,- oder Bitbucket-Repository übertragen werden. GitLab GitHub Weitere Informationen zu mehreren Remotes finden Sie unter Push Commits to an ein zusätzliches Git-Repository (AWS Blogbeitrag).

> Hinweis: Achten Sie auf Abweichungen, z. B. vermeiden Sie es, Änderungen über Weboberfl ächen vorzunehmen.

Tragen Sie Ihre eigenen Aktionen bei und fügen Sie sie hinzu

Das SCSP-Setup wird als GitHub Projekt verwaltet, das den Quellcode für die AWS Cloud Development Kit (AWS CDK) SCSP-Anwendung enthält. Um der Pipeline zusätzliche Prüfungen hinzuzufügen, muss die AWS CDK Anwendung aktualisiert und anschließend synthetisiert oder in AWS-Konto dem Ziel bereitgestellt werden, auf dem die Pipeline ausgeführt werden soll. Klonen Sie dazu zunächst das GitHub SCSP-Projekt und suchen Sie dann die Stack-Definitionsdatei im Ordner. `lib`

Wenn Sie eine zusätzliche Prüfung hinzufügen möchten, macht es die `StandardizedCodeBuildProject` Klasse im AWS CDK Code sehr einfach, Aktionen hinzuzufügen. Geben Sie den Namen, die Beschreibung und/oder `install` die `build` Befehle ein. AWS CDK erstellt das CodeBuild Projekt unter Verwendung sinnvoller Standardwerte. Sie müssen das Build-Projekt nicht nur erstellen, sondern es auch zu den CodePipeline Aktionen in der Build-Phase hinzufügen. Beim Entwerfen einer neuen Prüfung sollte die Aktion erfolgen, `FAIL` wenn das Scan-Tool Probleme feststellt oder nicht ausgeführt werden kann. Die Aktion sollte `PASS` erfolgen,

wenn das Scan-Tool keine Probleme erkennt. Ein Beispiel für die Konfiguration eines Tools finden Sie im Code für die `Bandit` Aktion.

Weitere Informationen zu den erwarteten Eingaben und Ausgaben finden Sie in der Repository-Dokumentation.

Wenn Sie benutzerdefinierte Aktionen hinzufügen, müssen Sie SCSP mithilfe von `cdk deploy` oder `cdk synth + CloudFormation deploy` bereitstellen. Das liegt daran, dass die Quick CloudFormation Create-Stack-Vorlage von den Repo-Besitzern verwaltet wird.

Stellen Sie mithilfe von AWS Config detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit

Erstellt von Alberto Menendez (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Netzwerke	AWS-Dienste: AWS Config; Amazon SNS

Übersicht

Distributed-Edge-Netzwerkarchitekturen verlassen sich auf die Sicherheit am Netzwerkrand, die parallel zu den Workloads in ihren virtuellen privaten Clouds (VPCs) ausgeführt wird. Dies bietet eine beispiellose Skalierbarkeit im Vergleich zum üblicheren, zentralisierten Ansatz. Die Bereitstellung öffentlicher Subnetze in Workload-Konten kann zwar Vorteile bieten, bringt aber auch neue Sicherheitsrisiken mit sich, da dadurch die Angriffsfläche vergrößert wird. Wir empfehlen, nur Elastic Load Balancing (ELB) -Ressourcen wie Application Load Balancer oder NAT-Gateways in den öffentlichen Subnetzen dieser VPCs bereitzustellen. Durch die Verwendung von Load Balancern und NAT-Gateways in dedizierten öffentlichen Subnetzen können Sie eine differenzierte Steuerung für eingehenden und ausgehenden Datenverkehr implementieren.

Wir empfehlen, sowohl präventive als auch detektive Kontrollen zu implementieren, um die Arten von Ressourcen zu begrenzen, die in öffentlichen Subnetzen eingesetzt werden können. Weitere Informationen zur Verwendung der attributebasierten Zugriffskontrolle (ABAC) zur Bereitstellung präventiver Kontrollen für öffentliche Subnetze finden Sie unter Bereitstellen präventiver attributebasierter Zugriffskontrollen für öffentliche Subnetze. Diese präventiven Kontrollen sind zwar in den meisten Situationen wirksam, decken aber möglicherweise nicht alle möglichen Anwendungsfälle ab. Daher baut dieses Muster auf dem ABAC-Ansatz auf und hilft Ihnen bei der Konfiguration von Warnmeldungen über nicht konforme Ressourcen, die in öffentlichen Subnetzen bereitgestellt werden. Die Lösung prüft, ob Elastic Network-Schnittstellen zu einer Ressource gehören, die in öffentlichen Subnetzen nicht zulässig ist.

Um dies zu erreichen, verwendet dieses Muster benutzerdefinierte AWS Config-Regeln und ABAC. Die benutzerdefinierte Regel verarbeitet die Konfiguration einer elastic network interface, wann immer sie erstellt oder geändert wird. Auf einer höheren Ebene führt diese Regel zwei Aktionen durch, um festzustellen, ob die Netzwerkschnittstelle konform ist:

1. Um festzustellen, ob die Netzwerkschnittstelle in den Geltungsbereich der Regel fällt, prüft die Regel, ob das Subnetz über bestimmte AWS-Tags verfügt, die darauf hinweisen, dass es sich um ein öffentliches Subnetz handelt. Dieses Tag könnte beispielsweise sein. `IsPublicFacing=True`
2. Wenn die Netzwerkschnittstelle in einem öffentlichen Subnetz bereitgestellt wird, prüft die Regel, welcher AWS-Service diese Ressource erstellt hat. Wenn es sich bei der Ressource nicht um eine ELB-Ressource oder ein NAT-Gateway handelt, wird die Ressource als nicht konform gekennzeichnet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Config, im Workload-Konto eingerichtet
- Berechtigungen zur Bereitstellung der erforderlichen Ressourcen im Workload-Konto
- Eine VPC mit öffentlichen Subnetzen
- Ordnungsgemäß angewendete Tags zur Identifizierung der öffentlichen Zielsubnetze
- (Optional) Eine Organisation in AWS Organizations
- (Optional) Ein zentrales Sicherheitskonto, das der delegierte Administrator für AWS Config und AWS Security Hub ist

Architektur

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Wenn eine elastic network interface Interface-Ressource (`AWS::EC2::NetworkInterface`) bereitgestellt oder geändert wird, erfasst AWS Config das Ereignis und die Konfiguration.
2. AWS Config vergleicht dieses Ereignis mit der benutzerdefinierten Regel, die zur Bewertung der Konfiguration verwendet wurde.
3. Die mit dieser benutzerdefinierten Regel verknüpfte AWS Lambda Lambda-Funktion wird aufgerufen. Die Funktion wertet die Ressource aus und wendet die angegebene Logik an,

um festzustellen, ob die Ressourcenkonfiguration oder ist`COMPLIANT`. `NON_COMPLIANT` `NOT_APPLICABLE`

4. Wenn festgestellt wird, dass es sich bei einer Ressource um eine solche handelt`NON_COMPLIANT`, sendet AWS Config eine Warnung über Amazon Simple Notification Service (Amazon SNS).

> Hinweis: Wenn es sich bei diesem Konto um ein Mitgliedskonto bei AWS Organizations handelt, können Sie Compliance-Daten über AWS Config oder AWS Security Hub an ein zentrales Sicherheitskonto senden.

Bewertungslogik für Lambda-Funktionen

Das folgende Diagramm zeigt die Logik, die von der Lambda-Funktion angewendet wird, um die Konformität der elastic network interface zu bewerten.

Automatisierung und Skalierung

Dieses Muster ist eine detektivische Lösung. Sie können es auch durch eine Behebungsregel ergänzen, um automatisch alle Ressourcen zu beheben, die den Anforderungen nicht entsprechen. Weitere Informationen finden Sie unter Korrigieren nicht konformer Ressourcen mit AWS Config-Regeln.

Sie können diese Lösung wie folgt skalieren:

- Erzwingung der Anwendung der entsprechenden AWS-Tags, die Sie einrichten, um öffentlich zugängliche Subnetze zu identifizieren. Weitere Informationen finden Sie unter Tag-Richtlinien in der Dokumentation zu AWS Organizations.
- Konfiguration eines zentralen Sicherheitskontos, das die benutzerdefinierte AWS Config-Regel auf jedes Workload-Konto in der Organisation anwendet. Weitere Informationen finden Sie unter Automatisieren der Einhaltung skalierbarer Konfigurationen in AWS (AWS-Blogbeitrag).
- Integration von AWS Config mit AWS Security Hub zur Erfassung, Zentralisierung und Benachrichtigung in großem Umfang Weitere Informationen finden Sie unter Konfiguration von AWS Config in der AWS Security Hub Hub-Dokumentation.

Tools

- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Bewährte Methoden

Weitere Beispiele und bewährte Methoden für die Entwicklung benutzerdefinierter AWS Config-Regeln finden Sie im offiziellen AWS Config Rules Repository unter GitHub.

Epen

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Lambda-Konsole.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Klicken Sie auf der Seite Functions (Funktionen) auf Create function (Funktion erstellen). 3. Wählen Sie Verfassen von Grund auf aus. 4. Geben Sie im Bereich Grundinformationen für Funktionsname einen Namen ein. 5. Wählen Sie für Runtime Python 3.12. 6. Lassen Sie die Architektur auf x86_64 eingestellt. 7. Wählen Sie Funktion erstellen. 8. Wählen Sie die Registerkarte Code. 9. Wählen Sie im Datei-Explorer lambda_function.py. 10. Fügen Sie den Beispielcode aus dem Abschnitt Zusätzliche Informationen dieses Musters in die Registerkarte lambda_function.py ein. Passen Sie den Beispielcode an, um jede benutzerdefinierte Bewertungslogik in der `evaluate_change_notification_compliance` Funktion zu identifizieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie Bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Ausführungsrolle der Lambda-Funktion Berechtigungen hinzu.	1. Wählen Sie im Navigationsbereich Funktionen aus. 2. Wählen Sie die Funktion aus, die Sie gerade erstellt haben. 3. Wählen Sie Configuration (Konfiguration) und anschließend Permissions (Berechtigungen) aus. 4. Wählen Sie den Rollennamen, um die Rolle in der AWS Identity and Access Management (IAM) -Konsole zu öffnen. 5. Wählen Sie unter Berechtigungsrichtlinien die Option Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus. 6. Wählen Sie JSON. 7. Fügen Sie die folgende Richtlinie in den Richtlinien-Editor ein. Dadurch kann die Lambda-Funktion: • Rufen Sie die Details der Subnetz-Tags ab. • Senden Sie das Konformitätsergebnis zurück an AWS Config. `{`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Action": [
	"config:PutEvaluations",
	"ec2:DescribeSubnets"
	],
	"Resource": "*",
	"Effect": "Allow"
	}
	]
	}</pre>
	8. Wählen Sie Weiter aus.
	9. Geben Sie einen Namen für die Richtlinie ein und wählen Sie dann Create policy (Richtlinie erstellen) aus.	

Rufen Sie die Lambda-Funktion Amazon Resource Name (ARN) ab.	1. Öffnen Sie die Lambda-Konsole. 2. Wählen Sie im Navigationsbereich Funktionen aus. 3. Wählen Sie die Funktion aus, die Sie gerade erstellt haben. 4. Kopieren Sie im Abschnitt Funktionsübersicht unter Function ARN den Wert.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die benutzerdefinierte AWS Config-Regel.	1. Öffnen Sie die AWS Config-Konsole unter https://console.aws.amazon.com/config/. 2. Wählen Sie auf der Seite Rules (Regeln) die Option Add Rule (Regel hinzufügen) aus. 3. Wählen Sie auf der Seite Regeltyp angeben die Option Benutzerdefinierte Lambda-Regel erstellen und dann Weiter aus. 4. Gehen Sie auf der Seite Regel konfigurieren wie folgt vor: a. Geben Sie einen Namen und eine Beschreibung ein. b. Fügen Sie für den ARN der AWS-Lambda-Funktion den ARN ein, den Sie zuvor kopiert haben. c. Als Triggertyp wählen Sie Wenn sich die Konfiguration ändert aus. d. Wählen Sie unter Umfang der Änderungen die Option Ressourcen aus. e. Wählen Sie als Ressourcentyp AWS	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2 NetworkInterface aus. f. Wählen Sie Weiter aus. 5. Überprüfen Sie auf der Seite Überprüfen und erstellen Ihre Regel und wählen Sie dann Speichern aus.	
Benachrichtigungen konfigurieren.	1. Folgen Sie den Anweisungen unter Ein Amazon SNS SNS-Thema erstellen, um ein Amazon SNS SNS-Thema zu erstellen. 2. Folgen Sie den Anweisungen unter Amazon SNS SNS-Thema abonnieren, um einen Endpunkt zu konfigurieren, der Benachrichtigungen für das Amazon SNS SNS-Thema empfängt. 3. Folgen Sie den Anweisungen unter Wie kann ich benachrichtigt werden, wenn eine AWS-Ressource nicht konform ist? Verwenden Sie AWS Config, um eine benutzerdefinierte EventBridge Amazon-Regel für Ihre nicht konformen Ressourcen zu konfigurieren.	Allgemeines AWS

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine konforme Ressource.	1. Verwenden Sie die folgenden Anweisungen, um eine der unterstützten Ressourcen in einem öffentlichen Subnetz zu erstellen: • Erstellen Sie ein NAT-Gateway • Erste Schritte mit Network Load Balancers • Erstellen Sie einen Application Load Balancer 2. Nachdem die Ressource erstellt wurde, bewertet die benutzerdefinierte AWS Config-Regel die Elastic Network-Schnittstellen, die der Ressource zugeordnet sind. Sie kennzeichnet diese Netzwerkschnittstellen als `COMPLIANT`. Sie können die Ressourcen in AWS Config anzeigen, indem Sie die folgenden Schritte ausführen: a. Öffnen Sie die AWS Config-Konsole unter https://console.aws.amazon.com/config/.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	b. Wählen Sie auf der Seite Regeln Ihre Regel aus. c. Gehen Sie auf der Seite mit den Regeldetails zum Ende der Seite. d. Wählen Sie unter Ressourcen im Geltungsbereich die Option Konformität aus. Vergewissern Sie sich, dass Sie die IDs der Netzwerkschnittstellen sehen, die erstellt wurden. e. Wählen Sie die Ressourcen-ID aus, um weitere Informationen zur Konfiguration der Netzwerkschnittstelle zu erhalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine nicht konforme Ressource.	1. Verwenden Sie die folgenden Anweisungen, um eine nicht konforme Ressource in einem öffentlichen Subnetz zu erstellen: • Starten Sie eine Amazon EC2 EC2-Instance • Erstellen einer Amazon Relational Database Service (Amazon RDS) - Datenbank-Instance • Erstellen Sie einen VPC-Endpunkt 2. Nachdem die Ressource erstellt wurde, bewertet die benutzerdefinierte AWS Config-Regel die Elastic Network-Schnittstellen, die der Ressource zugeordnet sind. Sie kennzeichnet diese Netzwerkschnittstellen als `NON_COMPLIANT`. Sie können die Ressourcen in AWS Config anzeigen, indem Sie die folgenden Schritte ausführen: a. Öffnen Sie die AWS Config-Konsole unter https://console.aws.amazon.com/config/. b. Wählen Sie auf der Seite Regeln Ihre Regel aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Gehen Sie auf der Seite mit den Regeldetails zum Ende der Seite. d. Wählen Sie unter Ressourcen im Geltungsbereich die Option aus NonCompli ant. Vergewissern Sie sich, dass Sie die IDs der Netzwerkschnittste llen sehen, die erstellt wurden. e. Wählen Sie die Ressourcen-ID aus, um weitere Informationen zur Konfiguration der Netzwerkschnittstelle zu erhalten. 3. Vergewissern Sie sich, dass Sie die Benachrichtigung an dem Endpunkt erhalten, den Sie in Amazon SNS konfiguriert haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ressource, die nicht zutrifft.	1. Erstellen Sie in einem privaten Subnetz jede Ressource, die eine elastic network interface benötigt. 2. Nachdem die Ressource erstellt wurde, bewertet die benutzerdefinierte AWS Config-Regel die Elastic Network-Schnittstellen, die der Ressource zugeordnet sind. Sie kennzeichnet diese Netzwerkschnittstellen als `NOT_APPLICABLE`. Diese Ressourcen werden in der AWS Config-Konsole nicht angezeigt.	Allgemeines AWS

Zugehörige Ressourcen

AWS-Dokumentation

- Einrichtung von AWS Config
- Benutzerdefinierte AWS Config-Regeln
- ABAC für AWS
- Implementieren Sie präventive, auf Attributen basierende Zugriffskontrollen für öffentliche Subnetze

Andere AWS-Ressourcen

- Automatisieren Sie die Einhaltung von Konfigurationen in großem Umfang in AWS
- Verteilte Inspektionsarchitekturen mit Gateway Load Balancer

Zusätzliche Informationen

Im Folgenden finden Sie ein Beispiel für eine Lambda-Funktion, die zu Demonstrationszwecken bereitgestellt wird.

```
import boto3
import json
import os

# Init clients
config_client = boto3.client('config')
ec2_client = boto3.client('ec2')

def lambda_handler(event, context):

    # Init values
    compliance_value = 'NOT_APPLICABLE'
    invoking_event = json.loads(event['invokingEvent'])
    configuration_item = invoking_event['configurationItem']

    status = configuration_item['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']

    # First check if the event configuration applies. Ex. resource event is not delete
    if (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope:
        compliance_value = evaluate_change_notification_compliance(configuration_item)


    config_client.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])

# Function with the logs to evaluate the resource
```

```
def evaluate_change_notification_compliance(configuration_item):
    is_in_scope = is_in_scope_subnet(configuration_item['configuration']['subnetId'])

    if (configuration_item['resourceType'] != 'AWS::EC2::NetworkInterface') or not
 is_in_scope:
        return 'NOT_APPLICABLE'

    else:
        alb_condition = configuration_item['configuration']['requesterId'] in ['amazon-
elb']
        nlb_condition = configuration_item['configuration']['interfaceType'] in
 ['network_load_balancer']
        nat_gateway_condition = configuration_item['configuration']['interfaceType'] in
 ['nat_gateway']

        if alb_condition or nlb_condition or nat_gateway_condition:
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

# Function to check if elastic network interface is in public subnet
def is_in_scope_subnet(eni_subnet):

    subnet_description = ec2_client.describe_subnets(
        SubnetIds=[eni_subnet]
    )

    for subnet in subnet_description['Subnets']:
        for tag in subnet['Tags']:
            if tag['Key'] == os.environ.get('TAG_KEY') and tag['Value'] ==
 os.environ.get('TAG_VALUE'):
                return True

    return False
```

Stellen Sie präventive attributebasierte Zugriffskontrollen für öffentliche Subnetze bereit

Erstellt von Joel Alfredo Nunez Gonzalez (AWS) und Samuel Ortega Sancho (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Netzwerke; Bereitstellung von Inhalten	AWS-Services: AWS Organizations; AWS Identity and Access Management

Übersicht

In zentralisierten Netzwerkarchitekturen konzentrieren Inspection und Edge Virtual Private Clouds (VPCs) den gesamten eingehenden und ausgehenden Verkehr, z. B. den Verkehr zum und vom Internet. Dies kann jedoch zu Engpässen führen oder dazu führen, dass die Grenzen der AWS-Servicekontingenten erreicht werden. Die Bereitstellung von Network-Edge-Sicherheit zusammen mit den Workloads in ihren VPCs bietet eine beispiellose Skalierbarkeit im Vergleich zum üblicheren, zentralisierten Ansatz. Dies wird als Distributed-Edge-Architektur bezeichnet.

Die Bereitstellung öffentlicher Subnetze in Workload-Konten kann zwar Vorteile bieten, bringt aber auch neue Sicherheitsrisiken mit sich, da dadurch die Angriffsfläche vergrößert wird. Wir empfehlen, nur Elastic Load Balancing (ELB) -Ressourcen wie Application Load Balancer oder NAT-Gateways in den öffentlichen Subnetzen dieser VPCs bereitzustellen. Durch die Verwendung von Load Balancern und NAT-Gateways in dedizierten öffentlichen Subnetzen können Sie eine differenzierte Steuerung für eingehenden und ausgehenden Datenverkehr implementieren.

Bei der attributebasierten Zugriffskontrolle (ABAC) werden detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname erstellt. Weitere Informationen finden Sie unter ABAC for AWS. ABAC kann Leitplanken für öffentliche Subnetze in Workload-Konten bereitstellen. Dies hilft Anwendungsteams, agil zu sein, ohne die Sicherheit der Infrastruktur zu gefährden.

Dieses Muster beschreibt, wie Sie öffentliche Subnetze schützen können, indem Sie ABAC mithilfe einer Service Control Policy (SCP) in AWS Organizations und Richtlinien in AWS Identity and Access Management (IAM) implementieren. Sie wenden das SCP entweder auf ein Mitgliedskonto einer Organisation oder auf eine Organisationseinheit (OU) an. Diese ABAC-Richtlinien ermöglichen es

Benutzern, NAT-Gateways in den Zielsubnetzen bereitzustellen und sie daran zu hindern, andere Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen wie EC2-Instances und elastische Netzwerkschnittstellen bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Organisation in AWS Organizations
- Administratorzugriff auf das Root-Konto von AWS Organizations
- In der Organisation ein aktives Mitgliedskonto oder eine Organisationseinheit zum Testen des SCP

Einschränkungen

- Das SCP in dieser Lösung verhindert nicht, dass AWS-Services, die eine serviceverknüpfte Rolle verwenden, Ressourcen in den Zielsubnetzen bereitstellen. Beispiele für diese Dienste sind Elastic Load Balancing (ELB), Amazon Elastic Container Service (Amazon ECS) und Amazon Relational Database Service (Amazon RDS). Weitere Informationen finden Sie unter SCP-Auswirkungen auf Berechtigungen in der Dokumentation zu AWS Organizations. Implementieren Sie Sicherheitskontrollen, um diese Ausnahmen zu erkennen.

Architektur

Zieltechnologie-Stack

- SCP wurde auf ein AWS-Konto oder eine Organisationseinheit in AWS Organizations angewendet
- Die folgenden IAM-Rollen:
  - `AutomationAdminRole`— Wird verwendet, um Subnetz-Tags zu ändern und VPC-Ressourcen nach der Implementierung des SCP zu erstellen
  - `TestAdminRole`— Wird verwendet, um zu testen, ob der SCP andere IAM-Prinzipale, einschließlich derer mit Administratorzugriff, daran hindert, die Aktionen auszuführen, die für `AutomationAdminRole`

Zielarchitektur

1. Sie erstellen die `AutomationAdminRole` IAM-Rolle im Zielkonto. Diese Rolle verfügt über Berechtigungen zur Verwaltung von Netzwerkressourcen. Beachten Sie die folgenden Berechtigungen, die ausschließlich für diese Rolle gelten:
   - Diese Rolle kann VPCs und öffentliche Subnetze erstellen.
   - Diese Rolle kann die Tag-Zuweisungen für die Zielsubnetze ändern.
   - Diese Rolle kann ihre eigenen Berechtigungen verwalten.
2. In AWS Organizations wenden Sie den SCP auf das AWS-Zielkonto oder die Organisationseinheit an. Eine Beispielrichtlinie finden Sie unter Zusätzliche Informationen in diesem Muster.
3. Ein Benutzer oder ein Tool in der CI/CD-Pipeline kann die `AutomationAdminRole` Rolle übernehmen, das `SubnetType` Tag auf die Zielsubnetze anzuwenden.
4. Durch die Übernahme anderer IAM-Rollen können autorisierte IAM-Prinzipale in Ihrer Organisation NAT-Gateways in den Zielsubnetzen und andere zulässige Netzwerkressourcen im AWS-Konto verwalten, z. B. Routing-Tabellen. Verwenden Sie IAM-Richtlinien, um diese Berechtigungen zu gewähren. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon VPC.

Automatisierung und Skalierung

Um öffentliche Subnetze zu schützen, müssen die entsprechenden AWS-Tags angewendet werden. Nach der Anwendung des SCP sind NAT-Gateways die einzige Art von Amazon EC2 EC2-Ressource, die autorisierte Benutzer in Subnetzen mit diesem Tag erstellen können. `SubnetType:IFA` (*IFA*bedeutet Ressourcen, die mit dem Internet verbunden sind.) Das SCP verhindert die Erstellung anderer Amazon EC2 EC2-Ressourcen wie Instances und Elastic Network Interfaces. Es wird empfohlen, eine CI/CD-Pipeline zu verwenden, die die `AutomationAdminRole` Rolle beim Erstellen von VPC-Ressourcen übernimmt, sodass diese Tags ordnungsgemäß auf öffentliche Subnetze angewendet werden.

Tools

AWS-Services

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten. In AWS Organizations

können Sie Service Control Policies (SCPs) implementieren. Dabei handelt es sich um eine Art von Richtlinie, mit der Sie Berechtigungen in Ihrer Organisation verwalten können.

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Wenden Sie das SCP an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Test-Admin-Rolle.	Erstellen Sie eine IAM-Rolle mit dem Namen `TestAdminRole` des AWS-Zielkontos. Hängen Sie die von AdministratorAccessAWS verwaltete IAM-Richtlinie an die neue Rolle an. Anweisungen finden Sie in der IAM-Dokumentation unter Eine Rolle erstellen, um Berechtigungen an einen IAM-Benutzer zu delegieren.	AWS-Administrator
Erstellen Sie die Automatisierungs-Admin-Rolle.	1. Erstellen Sie eine IAM-Rolle mit dem Namen `AutomationAdminRole` des AWS-Zielkontos. 2. Hängen Sie die von AdministratorAccessAWS verwaltete IAM-Richtlinie an die neue Rolle an. Im Folgenden finden Sie ein Beispiel für eine Vertrauen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	srichtlinie, mit der Sie die Rolle vom `000000000000` Konto aus testen können. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::000000000000:root" ] }, "Action": "sts:AssumeRole", "Condition": {} } ] }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SCP und hängen Sie es an.	1. Erstellen Sie mithilfe des Beispielcodes im Abschnitt Zusätzliche Informationen eine Richtlinie zur Sicherheitskontrolle. Anweisungen finden Sie in der Dokumentation zu AWS Organizations unter Creating an SCP. 2. Ordnen Sie den SCP dem AWS-Zielkonto oder der Organisationseinheit zu. Anweisungen finden Sie in der Dokumentation zu AWS Organizations unter Servicesteuerungsrichtlinien anhängen und trennen.	AWS-Administrator

Testen Sie das SCP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC oder ein Subnetz.	1. Nehmen Sie die `TestAdminRole` Rolle im AWS-Zielkonto an. 2. Versuchen Sie, eine VPC oder ein neues öffentliches Subnetz in einer vorhandenen VPC zu erstellen. Anweisungen finden Sie unter Erstellen einer VPC, Subnetze und anderer VPC-Ressourcen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der Amazon VPC-Dokumentation. Sie sollten nicht in der Lage sein, diese Ressourcen zu erstellen. 3. Nehmen Sie die `AutomationAdminRole` Rolle an und wiederholen Sie den vorherigen Schritt. Jetzt sollten Sie in der Lage sein, die Netzwerkressourcen zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Tags verwalten.	1. Nehmen Sie die `TestAdminRole` Rolle im AWS-Zielkonto an. 2. Fügen Sie einem verfügbaren öffentlichen Subnetz ein `SubnetType:IFA` Tag hinzu. Sie sollten in der Lage sein, dieses Tag hinzuzufügen. Anweisungen zum Hinzufügen von Tags über die AWS-Befehlszeilenschnittstelle (AWS CLI) finden Sie unter create-tags in der AWS CLI Command Reference. 3. Versuchen Sie, das diesem Subnetz zugewiesene `SubnetType:IFA` Tag zu ändern, ohne Ihre Anmeldeinformationen zu ändern. Sie sollten dieses Tag nicht ändern können. 4. Nehmen Sie die `AutomationAdminRole` Rolle an und wiederholen Sie die vorherigen Schritte. Diese Rolle sollte in der Lage sein, dieses Tag hinzuzufügen und zu ändern.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen in den Zielsubnetzen bereit.	1. Übernimm die `TestAdmin Role` Rolle. 2. Versuchen Sie für ein öffentliches Subnetz mit dem `SubnetType:IFA` Tag, eine EC2-Instance zu erstellen. Anweisungen finden Sie in der Amazon EC2 EC2-Dokumentation unter Eine Instance starten. In diesem Subnetz sollten Sie keine Amazon EC2 EC2-Ressourcen außer NAT-Gateways erstellen , ändern oder löschen können. 3. Erstellen Sie im selben Subnetz ein NAT-Gatew ay. Anweisungen finden Sie unter Erstellen eines NAT-Gateways in der Amazon VPC-Dokumentation. Sie sollten in der Lage sein, NAT-Gateways in diesem Subnetz zu erstellen, zu ändern oder zu löschen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwalte die AutomationAdminRole Rolle.	1. Übernimm die `TestAdminRole` Rolle. 2. Versuchen Sie, die `AutomationAdminRole` Rolle zu ändern. Anweisungen finden Sie in der IAM-Dokumentation unter Eine Rolle ändern. Sie sollten diese Rolle nicht ändern können. 3. Nehmen Sie die `AutomationAdminRole` Rolle an und wiederholen Sie den vorherigen Schritt. Jetzt sollten Sie in der Lage sein, die Rolle zu ändern.	AWS-Administrator

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubern Sie die eingesetzten Ressourcen.	1. Trennen Sie das SCP vom AWS-Konto oder der Organisationseinheit. Anweisungen finden Sie unter Trennen eines SCP in der Dokumentation zu AWS Organizations. 2. Löschen Sie die SCP. Anweisungen finden Sie unter Löschen eines SCP	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Dokumentation zu AWS Organizations). 3. Löschen Sie die `AutomationAdminRole` Rolle und die `TestAdminRole` Rolle. Anweisungen finden Sie in der IAM-Dokumentation unter Rollen löschen. 4. Löschen Sie alle Netzwerkressourcen wie VPCs und Subnetze, die Sie für diese Lösung erstellt haben.	

Zugehörige Ressourcen

AWS-Dokumentation

- SCPs anhängen und trennen
- SCPs erstellen, aktualisieren und löschen
- Stellen Sie mithilfe von AWS Config detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit
- Detektivkontrollen
- Referenz zur Serviceautorisierung
- Tagging von AWS-Ressourcen
- Was ist ABAC für AWS?

Zusätzliche AWS-Referenzen

- Sicherung von Ressourcen-Tags, die für die Autorisierung verwendet werden, mithilfe einer Service Control-Richtlinie in AWS Organizations (AWS-Blogbeitrag)

Zusätzliche Informationen

Die folgende Service Control-Richtlinie ist ein Beispiel, mit dem Sie diesen Ansatz in Ihrer Organisation testen können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyVPCActions",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateVPC",
        "ec2:CreateRoute",
        "ec2:CreateSubnet",
        "ec2:CreateInternetGateway",
        "ec2:DeleteVPC",
        "ec2:DeleteRoute",
        "ec2:DeleteSubnet",
        "ec2:DeleteInternetGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "AllowNATGWOnIFASubnet",
      "Effect": "Deny",
      "NotAction": [
        "ec2:CreateNatGateway",
        "ec2:DeleteNatGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition": {
        "ForAnyValue:StringEqualsIfExists": {
          "aws:ResourceTag/SubnetType": "IFA"
```

```
        },
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "DenyChangesToAdminRole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AutomationAdminRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "allowbydefault",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Stellen Sie die Lösung Security Automations für AWS WAF mithilfe von Terraform bereit

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) undilsel Bol P (AWS)

Code-Repository: aws-waf-automation-terraform-samples	Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Infrastruktur; Bereitstellung von Inhalten; DevOps
Workload: Alle anderen Workloads	AWS-Services: AWS WAF	

Übersicht

AWS WAF ist eine Firewall für Webanwendungen, die Anwendungen vor häufigen Exploits schützt, indem anpassbare Regeln verwendet werden, die Sie definieren und in Web-Zugriffskontrolllisten (ACLs) bereitstellen. Die Konfiguration von AWS WAF-Regeln kann schwierig sein, insbesondere für Organisationen, die keine dedizierten Sicherheitsteams haben. Um diesen Prozess zu vereinfachen, bietet Amazon Web Services (AWS) die Lösung Security Automations for AWS WAF, die automatisch eine einzelne Web-ACL mit einem Satz von AWS WAF-Regeln bereitstellt, die webbasierte Angriffe filtern. Während der Terraform-Bereitstellung können Sie angeben, welche Schutzfunktionen berücksichtigt werden sollen. Nach der Bereitstellung dieser Lösung überprüft AWS WAF Webanforderungen an vorhandene Amazon- CloudFront Verteilungen oder Application Load Balancer und blockiert alle Anforderungen, die nicht den Regeln entsprechen.

Die Lösung Security Automations for AWS WAF kann mithilfe von AWS CloudFormation gemäß den Anweisungen im Implementierungshandbuch für Security Automations for AWS WAF bereitgestellt werden. Dieses Muster bietet eine alternative Bereitstellungsoption für Organisationen, die HashiCorp Terraform als bevorzugtes Infrastructure as Code (IaC)-Tool zur Bereitstellung und Verwaltung ihrer Cloud-Infrastruktur verwenden. Wenn Sie diese Lösung bereitstellen, wendet Terraform die Änderungen automatisch in der Cloud an und stellt die AWS WAF-Einstellungen und Schutzfunktionen bereit und konfiguriert sie.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI) installiert und mit den erforderlichen Berechtigungen konfiguriert. Weitere Informationen finden Sie unter Erste Schritte (AWS-CLI-Dokumentation).
- Terraform installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren von Terraform (Terraform-Dokumentation).

Produktversionen

- AWS CLI Version 2.4.25 oder höher
- Terraform Version 1.1.9 oder höher

Architektur

Zielarchitektur

Dieses Muster stellt die Lösung Security Automations für AWS WAF bereit. Weitere Informationen zur Zielarchitektur finden Sie unter Architekturübersicht im Handbuch zur Implementierung von Sicherheitsautomatisierungen für AWS WAF. Weitere Informationen zu den AWS Lambda-Automatisierungen in dieser Bereitstellung, zum Anwendungsprotokoll-Parser, zum AWS WAF-Protokoll-Parser, zum IP-Listen-Parser und zum Zugriffshandler finden Sie unter Komponentendetails im Handbuch zur Implementierung von Sicherheitsautomatisierungen für AWS WAF.

Terraform-Bereitstellung

Wenn Sie ausführen`terraform apply`, geht Terraform wie folgt vor:

1. Terraform erstellt IAM-Rollen und Lambda-Funktionen basierend auf den Eingaben aus der Datei test.tfvars.
2. Terraform erstellt AWS WAF-ACL-Regeln und IP-Sets basierend auf den Eingaben aus der Datei test.tfvars.
3. Terraform erstellt die Amazon Simple Storage Service (Amazon S3)-Buckets, Amazon-EventBridge Regeln, AWS Glue-Datenbanktabellen und Amazon Athena-Arbeitsgruppen basierend auf den Eingaben aus der Datei test.tfvars.

4. Terraform stellt den AWS- CloudFormation Stack bereit, um die benutzerdefinierten Ressourcen bereitzustellen.
5. Terraform erstellt die Amazon API Gateway-Ressourcen basierend auf den angegebenen Eingaben aus der Datei test.tfvars.

Automatisierung und Skalierung

Sie können dieses Muster verwenden, um AWS WAF-Regeln für mehrere AWS-Konten und AWS-Regionen zu erstellen, um die Lösung Security Automations for AWS WAF in Ihrer gesamten AWS Cloud-Umgebung bereitzustellen.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS WAF ist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anforderungen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere -Services

- Git ist ein verteiltes Open-Source-Versionsverwaltungssystem.
- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.

Code-Repository

Der Code für dieses Muster ist im GitHub AWS WAF Automation Using Terraform-Repository verfügbar.

Bewährte Methoden

- Platzieren Sie statische Dateien in separaten S3-Buckets.
- Vermeiden Sie die Hartkodierung von Variablen.
- Beschränken Sie die Verwendung von benutzerdefinierten Skripts.
- Übernehmen Sie eine Namenskonvention.

Sekunden

Einrichten Ihrer lokalen Workstation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Git.	Folgen Sie den Anweisungen unter Erste Schritte (Git-Website), um Git auf Ihrer lokalen Workstation zu installieren.	DevOps Techniker
Klonen Sie das Repository	Geben Sie auf Ihrer lokalen Workstation den folgenden Befehl ein, um das Code-Repository zu klonen. Informationen zum Kopieren des vollständigen Befehls, einschließlich der Repo-URL, finden Sie im Abschnitt Zusätzliche Informationen dieses Musters. `git clone <repo-URL>.git`	DevOps Techniker
Aktualisieren Sie die Variablen.	1. Navigieren Sie in das geklonte Verzeichnis, indem Sie den folgenden Befehl eingeben. `cd terraform-aws-waf-automation` 2. Öffnen Sie in einem beliebigen Texteditor die Datei test.tfvars. 3. Aktualisieren Sie die Werte der Variablen in der Datei test.tfvars.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Speichern und schließen Sie die Datei.	

Bereitstellen der Zielarchitektur mit Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie die Terraform-Konfiguration.	Geben Sie den folgenden Befehl ein, um Ihr Arbeitsverzeichnis zu initialisieren, das die Terraform-Konfigurationsdateien enthält. `terraform init`	DevOps Techniker
Zeigen Sie eine Vorschau des Terraform-Plans an.	Geben Sie den folgenden Befehl ein. Terraform wertet die Konfigurationsdateien aus, um den Zielstatus für die deklarierten Ressourcen zu bestimmen. Anschließend wird der Zielstatus mit dem aktuellen Status verglichen und ein Plan erstellt. `terraform plan -var-file ="testing.tfvars"`	DevOps Techniker
Überprüfen Sie den Plan.	Überprüfen Sie den Plan und bestätigen Sie, dass er die erforderliche Architektur in Ihrem AWS-Zielkonto konfiguriert.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	1. Geben Sie den folgenden Befehl ein, um den Plan anzuwenden. `terraform apply -var-file="testing.tfvars"` 2. Geben Sie `yes` zur Bestätigung ein. Terraform erstellt, aktualisiert oder zerstört Infrastrukturen, um den in den Konfigurationsdateien deklarierten Zielstatus zu erreichen. Weitere Informationen zur Sequenz finden Sie unter Terraform-Bereitstellung im Abschnitt Architektur dieses Musters.	DevOps Techniker

Validieren und Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Änderungen.	1. Überprüfen Sie in der Terraform-Konsole, ob die Ausgaben den erwarteten Ergebnissen entsprechen. 2. Melden Sie sich bei der AWS-Managementkonsole an. 3. Überprüfen Sie, ob die Ausgaben in der Terraform-	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole erfolgreich in Ihrem AWS-Konto bereitgestellt wurden.	
(Optional) Bereinigen Sie die Infrastruktur.	Wenn Sie alle Ressourcen und Konfigurationsänderungen entfernen möchten, die von dieser Lösung vorgenommen wurden, gehen Sie wie folgt vor: 1. Geben Sie in der Terraform -Konsole den folgenden Befehl ein. `terraform destroy -var-file="testing .tfvars”` 2. Geben Sie `yes` zur Bestätigung ein.	DevOps Techniker

Fehlerbehebung

Problem	Lösung
`WAFV2 IPSet: WAFOptimisticLockException` -Fehler	Wenn Sie diesen Fehler erhalten, wenn Sie den `terraform destroy` Befehl ausführen , müssen Sie die IP-Sets manuell löschen. Anweisungen finden Sie unter Löschen eines IP-Sets (AWS WAF-Dokumentation).

Zugehörige Ressourcen

AWS-Referenzen

- Leitfaden zur Implementierung von Sicherheitsautomatisierungen für AWS WAF
- Sicherheitsautomatisierungen für AWS WAF (AWS Solutions Library)
- Häufig gestellte Fragen zu Sicherheitsautomatisierungen für AWS WAF

Terraform-Referenzen

- Terraform-Backend-Konfiguration
- Terraform-AWS-Anbieter – Dokumentation und Verwendung
- Terraform-AWS-Anbieter (Repository)GitHub

Zusätzliche Informationen

Der folgende Befehl klont das GitHub Repository für dieses Muster.

```
git clone https://github.com/aws-samples/aws-waf-automation-terraform-samples.git
```

Generieren Sie dynamisch eine IAM-Richtlinie mit IAM Access Analyzer mithilfe von Step Functions

Erstellt von BolSpeed (AWS), A El Kanabi (AWS), Koen Van Blijderveen (AWS) und Rafal Pawlaszek (AWS)

Code-Repository: Rollenrichtliniengenerator für automatisierten IAM Access Analyzer	Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Serverless
AWS-Services: AWS IAM Access Analyzer; AWS Lambda ;AWS Step Functions ;AWS Identity and Access Management		

Übersicht

Geringste Berechtigung ist die bewährte Sicherheitsmethode, die Mindestberechtigungen zu erteilen, die für die Ausführung einer Aufgabe erforderlich sind. Die Implementierung des Zugriffs mit den geringsten Berechtigungen in einem bereits aktiven Amazon Web Services (AWS)-Konto kann schwierig sein, da Sie Benutzer nicht versehentlich daran hindern möchten, ihre Aufgaben zu erledigen, indem Sie ihre Berechtigungen ändern. Bevor Sie AWS Identity and Access Management (IAM)-Richtlinienänderungen implementieren können, müssen Sie die Aktionen und Ressourcen verstehen, die die Kontobenutzer ausführen.

Dieses Muster soll Ihnen helfen, das Prinzip des Zugriffs mit den geringsten Rechten anzuwenden, ohne die Produktivität des Teams zu blockieren oder zu verlangsamen. Es beschreibt, wie Sie IAM Access Analyzer und AWS Step Functions verwenden, um dynamisch eine up-to-date IAM-Richtlinie für Ihre Rolle zu generieren, basierend auf den Aktionen, die derzeit im Konto ausgeführt werden. Die neue Richtlinie ist so konzipiert, dass sie die aktuelle Aktivität zulässt, jedoch alle unnötigen, erhöhten Rechte entfernt. Sie können die generierte Richtlinie anpassen, indem Sie Regeln zum Zulassen und Verweigern definieren, und die Lösung integriert Ihre benutzerdefinierten Regeln.

Dieses Muster enthält Optionen für die Implementierung der Lösung mit AWS Cloud Development Kit (AWS CDK) oder HashiCorp CDK for Terraform (CDKTF). Anschließend können Sie die neue

Richtlinie mithilfe einer Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) der Rolle zuordnen. Wenn Sie über eine Architektur mit mehreren Konten verfügen, können Sie diese Lösung in jedem Konto bereitstellen, in dem Sie aktualisierte IAM-Richtlinien für die Rollen generieren möchten, wodurch die Sicherheit Ihrer gesamten AWS Cloud-Umgebung erhöht wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit aktiviertem CloudTrail Trail.
- IAM-Berechtigungen für Folgendes:
  - Erstellen und Bereitstellen von Step Functions-Workflows. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Step Functions (Dokumentation zu Step Functions).
  - Erstellen Sie AWS Lambda-Funktionen. Weitere Informationen finden Sie unter Ausführungsrolle und Benutzerberechtigungen (Lambda-Dokumentation).
  - Erstellen Sie IAM-Rollen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer (IAM-Dokumentation).
- npm installiert. Weitere Informationen finden Sie unter Herunterladen und Installieren von Node.js und npm (npm-Dokumentation).
- Wenn Sie diese Lösung mit AWS CDK bereitstellen (Option 1):
  - AWS CDK Toolkit, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren des AWS-CDK (AWS-CDK-Dokumentation).
- Wenn Sie diese Lösung mit CDKTF bereitstellen (Option 2):
  - CDKTF, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren von CDK für Terraform (CDKTF-Dokumentation).
  - Terraform, installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte (Terraform-Dokumentation).
- AWS Command Line Interface (AWS CLI) lokal installiert und für Ihr AWS-Konto konfiguriert. Weitere Informationen finden Sie unter Installieren oder Aktualisieren der neuesten Version der AWS CLI (AWS CLI-Dokumentation).

Einschränkungen

- Dieses Muster wendet die neue IAM-Richtlinie nicht auf die Rolle an. Am Ende dieser Lösung wird die neue IAM-Richtlinie in einem CodeCommit Repository gespeichert. Sie können eine CI/CD-Pipeline verwenden, um Richtlinien auf die Rollen in Ihrem Konto anzuwenden.

Architektur

Zielarchitektur

1. Eine regelmäßig geplante Amazon- EventBridge Ereignisregel startet einen Step Functions-Workflow. Sie definieren diesen Zeitplan für die Neugenerierung im Rahmen der Einrichtung dieser Lösung.
2. Im Step Functions-Workflow generiert eine Lambda-Funktion die Datumsbereiche, die bei der Analyse der Kontoaktivitäten in den CloudTrail Protokollen verwendet werden sollen.
3. Der nächste Workflow-Schritt ruft die API von IAM Access Analyzer auf, um mit der Generierung der Richtlinie zu beginnen.
4. Mithilfe des Amazon-Ressourcennamens (ARN) der Rolle, die Sie bei der Einrichtung angeben, analysiert IAM Access Analyzer die CloudTrail Protokolle auf Aktivitäten innerhalb der angegebenen Datumsrate. Basierend auf der Aktivität generiert IAM Access Analyzer eine IAM-Richtlinie, die nur die Aktionen und Services zulässt, die von der Rolle während des angegebenen Datumsbereichs verwendet werden. Wenn dieser Schritt abgeschlossen ist, generiert dieser Schritt eine Auftrags-ID.
5. Im nächsten Workflow-Schritt wird alle 30 Sekunden nach der Auftrags-ID gesucht. Wenn die Auftrags-ID erkannt wird, verwendet dieser Schritt die Auftrags-ID, um die API von IAM Access Analyzer aufzurufen und die neue IAM-Richtlinie abzurufen. IAM Access Analyzer gibt die Richtlinie als JSON-Datei zurück.
6. Im nächsten Workflow-Schritt wird die Datei **<**IAM role name**>**/policy.json in einem Amazon Simple Storage Service (Amazon S3)-Bucket abgelegt. Sie definieren diesen S3-Bucket im Rahmen der Einrichtung dieser Lösung.
7. Eine Amazon S3-Ereignisbenachrichtigung startet eine Lambda-Funktion.
8. Die Lambda-Funktion ruft die Richtlinie aus dem S3-Bucket ab, integriert die benutzerdefinierten Regeln, die Sie in den Dateien allow.json und deny.json definieren, und überträgt dann die aktualisierte Richtlinie an CodeCommit. Im Rahmen der Einrichtung dieser Lösung definieren Sie das CodeCommit Repository, den Zweig und den Ordnerpfad.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, mit dem Sie AWS Cloud-Infrastruktur im Code definieren und bereitstellen können.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, mit dem Sie mit Ihrer AWS Cloud Development Kit (AWS CDK)-App interagieren können.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Governance, Compliance und des Betriebsrisikos Ihres AWS-Kontos.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist. Dieses Muster verwendet IAM Access Analyzer, eine Funktion von IAM, um Ihre CloudTrail Protokolle zu analysieren, um Aktionen und Services zu identifizieren, die von einer IAM-Entität (Benutzer oder Rolle) verwendet wurden, und dann eine IAM-Richtlinie zu generieren, die auf dieser Aktivität basiert.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. In diesem Muster verwenden Sie AWS SDK-Serviceintegrationen in Step Functions, um Service-API-Aktionen aus Ihrem Workflow aufzurufen.

Andere Tools

- CDK for Terraform (CDKTF) hilft Ihnen, Infrastructure as Code (IaC) mithilfe gängiger Programmiersprachen wie Python und Typescript zu definieren.

- Lerna ist ein Build-System zum Verwalten und Veröffentlichen mehrerer - JavaScript oder - TypeScript Pakete aus demselben Repository.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js-Umgebung ausgeführt wird und verwendet wird, um Pakete freizugeben oder zu leihen und die Bereitstellung privater Pakete zu verwalten.

Code-Repository

Der Code für dieses Muster ist im Repository für den GitHub automatisierten IAM Access Analyzer Role Policy Generator verfügbar.

Polen

Vorbereiten der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo.	Der folgende Befehl klont das GitHubRepository für den automatisierten IAM Access Analyze Role Policy Generator (). `git clone https://github.com/aws-samples/automated-iam-access-analyzer.git`	App-Developer
Installieren Sie Lerna.	Mit dem folgenden Befehl wird Lerna installiert. `npm i -g lerna`	App-Developer
Richten Sie die Abhängigkeiten ein.	Mit dem folgenden Befehl werden die Abhängigkeiten für das Repository installiert.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd automated-iam-acce ss-advisor/ npm install && npm run bootstrap`	
Erstellen Sie den Code.	Der folgende Befehl testet, erstellt und bereitet die ZIP-Pakete der Lambda-Fu nktionen vor. `npm run test:code npm run build:code npm run pack:code`	App-Developer
Erstellen Sie die Konstrukte.	Der folgende Befehl erstellt die Infrastruktur zur Synthetis ierung von Anwendungen sowohl für AWS CDK als auch für CDKTF. `npm run build:infra`	
Konfigurieren Sie alle benutzerdefinierten Berechtig ungen.	Bearbeiten Sie im Repo-Ordner des geklonten Repositorys die Dateien allow.json und deny.json, um benutzerdefinierte Berechtig ungen für die Rolle zu definieren. Wenn die Dateien allow.json und deny.json dieselbe Berechtigung enthalten, wird die Zugriffsv erweigerungsberechtigung angewendet.	AWS-Administrator, App-Entwi ckler

Option 1 – Bereitstellen der Lösung mit AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den AWS-CDK-Stack bereit.	Der folgende Befehl stellt die Infrastruktur über AWS CloudFormation bereit. Legen Sie die folgenden Parameter fest:
	• `<NAME_OF_ROLE>` – Der ARN der IAM-Rolle, für die Sie eine neue Richtlinie erstellen.
	• `<TRAIL_ARN>` – Der ARN des CloudTrail Trails, in dem die Rollenaktivität gespeichert ist.
	• `<CRON_EXPRESSION_TO_RUN_SOLUTION>` – Der Cron-Ausdruck, der den Zeitplan für die Neugenerierung der Richtlinie definiert. Der Step-Functions-Workflow wird nach diesem Zeitplan ausgeführt.
	• `<TRAIL_LOOKBACK>` – Der Zeitraum in Tagen, der bei der Auswertung der Rollenberechtigungen im Trail zurückgeschaut werden soll.
	`cd infra/cdk`
	`cdk deploy –-parameters roleArn=<NAME_OF_ROLE> \`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`—-parameters trailArn=<TRAIL_ARN> \ --parameters schedule=<CRON_EXPRESSION_TO_RUN_SOLUTION> \ [ --parameters trailLookBack=<TRAIL_LOOKBACK> ]` Hinweis – Die eckigen Klammern bezeichnen optionale Parameter.	
(Optional) Warten Sie auf die neue Richtlinie.	Wenn der Trail keine angemessene Menge an historischen Aktivitäten für die Rolle enthält, warten Sie, bis Sie sicher sind, dass genügend protokollierte Aktivitäten vorhanden sind, damit IAM Access Analyzer eine genaue Richtlinie generiert. Wenn die Rolle über einen ausreichenden Zeitraum im Konto aktiv war, ist diese Wartezeit möglicher weise nicht erforderlich.	AWS-Administrator
Überprüfen Sie die generierte Richtlinie manuell.	Überprüfen Sie in Ihrem CodeCommit Repository die generierte Datei <ROLE_ARN>.json, um zu bestätigen, dass die Berechtigungen zum Zulassen und Verweigern für die Rolle angemessen sind.	AWS-Administrator

Option 2 – Bereitstellen der Lösung mit CDKTF

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synthetisieren Sie die Terraform-Vorlage.	Der folgende Befehl synthetisiert die Terraform-Vorlage. `lerna exec cdktf synth --scope @aiaa/tfm`	App-Developer
Stellen Sie die Terraform-Vorlage bereit.	Der folgende Befehl navigiert zu dem Verzeichnis, das die CDKTF-definierte Infrastruktur enthält. `cd infra/cdktf` Der folgende Befehl stellt die Infrastruktur im AWS-Zielkonto bereit. Legen Sie die folgenden Parameter fest: • `<account_ID>` – Die ID des Zielkontos. • `<region>` – Die AWS-Zielregion. • `<selected_role_ARN>` – Der ARN der IAM-Rolle, für die Sie eine neue Richtlinie erstellen. • `<trail_ARN>` – Der ARN des CloudTrail Trails, in dem die Rollenaktivität gespeichert ist. • `<schedule_expression>` – Der Cron-Ausdruck,	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der den Zeitplan für die Neugenerierung der Richtlinie definiert. Der Step-Functions-Workflow wird nach diesem Zeitplan ausgeführt. • `<trail_look_back>` – Der Zeitraum in Tagen, der bei der Auswertung der Rollenberechtigungen im Trail zurückgeschaut werden soll. `TF_VAR_accountId=<account_ID> \ TF_VAR_region=<region> \ TF_VAR_roleArns=<selected_role_ARN> \ TF_VAR_trailArn=<trail_ARN> \ TF_VAR_schedule=<schedule_expression> \ [ TF_VAR_trailLookBack=<trail_look_back> ] \ cdktf deploy` Hinweis – Die eckigen Klammern bezeichnen optionale Parameter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Warten Sie auf die neue Richtlinie.	Wenn der Trail keine angemessene Menge an historischen Aktivitäten für die Rolle enthält, warten Sie, bis Sie sicher sind, dass genügend protokoll ierte Aktivitäten vorhanden sind, damit IAM Access Analyzer eine genaue Richtlini e generiert. Wenn die Rolle über einen ausreichenden Zeitraum im Konto aktiv war, ist diese Wartezeit möglicher weise nicht erforderlich.	AWS-Administrator
Überprüfen Sie die generierte Richtlinie manuell.	Überprüfen Sie in Ihrem CodeCommit Repository die generierte Datei <ROLE_ARN >.json, um zu bestätigen, dass die Berechtigungen zum Zulassen und Verweigern für die Rolle angemessen sind.	AWS-Administrator

Zugehörige Ressourcen

AWS-Ressourcen

- Endpunkte und Kontingente von IAM Access Analyzer
- Konfigurieren der AWS CLI
- Erste Schritte mit dem AWS-CDK
- Berechtigungen mit den geringsten Berechtigungen

Sonstige Ressourcen

- CDK für Terraform (Terraform-Website)

Aktivieren Sie Amazon GuardDuty unter bestimmten Bedingungen mithilfe von AWS-Vorlagen CloudFormation

Erstellt von Ram Kandaswamy (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance DevOps; Betrieb	AWS-Services: AWS CloudFormation; Amazon GuardDuty; AWS Lambda; AWS Identity and Access Management

Übersicht

Sie können Amazon GuardDuty auf einem Amazon Web Services (AWS) -Konto aktivieren, indem Sie eine CloudFormation AWS-Vorlage verwenden. Standardmäßig schlägt die Stack-Bereitstellung fehl, wenn es bereits aktiviert GuardDuty ist, wenn Sie versuchen, es CloudFormation zu aktivieren. Sie können jedoch Bedingungen in Ihrer CloudFormation Vorlage verwenden, um zu überprüfen, ob sie bereits aktiviert GuardDuty ist. CloudFormation unterstützt die Verwendung von Bedingungen, die statische Werte vergleichen; die Verwendung der Ausgabe einer anderen Ressourceneigenschaft innerhalb derselben Vorlage wird nicht unterstützt. Weitere Informationen finden Sie im CloudFormation Benutzerhandbuch unter Bedingungen.

In diesem Muster verwenden Sie eine CloudFormation benutzerdefinierte Ressource, die von einer AWS-Lambda-Funktion unterstützt wird, um sie bedingt zu aktivieren, GuardDuty falls sie nicht bereits aktiviert ist. Wenn GuardDuty aktiviert, erfasst der Stack den Status und zeichnet ihn im Ausgabebereich des Stacks auf. Wenn nicht GuardDuty aktiviert, aktiviert der Stack es.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM) -Rolle mit Berechtigungen zum Erstellen, Aktualisieren und Löschen CloudFormation von Stacks

Einschränkungen

- Wenn dieses Muster für ein AWS-Konto oder eine AWS-Region manuell deaktiviert GuardDuty wurde, wird es GuardDuty für dieses Zielkonto oder diese Region nicht aktiviert.

Architektur

Zieltechnologie-Stack

Das Muster wird CloudFormation für Infrastructure as Code (IaC) verwendet. Sie verwenden eine CloudFormation benutzerdefinierte Ressource, die von einer Lambda-Funktion unterstützt wird, um die dynamische Service-Enablement-Funktion zu erreichen.

Zielarchitektur

Das folgende Architekturdiagramm auf hoher Ebene zeigt den Prozess der Aktivierung GuardDuty durch die Bereitstellung einer CloudFormation Vorlage:

1. Sie stellen eine CloudFormation Vorlage bereit, um einen CloudFormation Stack zu erstellen.
2. Der Stack erstellt eine IAM-Rolle und eine Lambda-Funktion.
3. Die Lambda-Funktion übernimmt die IAM-Rolle.
4. Wenn GuardDuty es auf dem AWS-Zielkonto noch nicht aktiviert ist, aktiviert es die Lambda-Funktion.

Automatisierung und Skalierung

Sie können die CloudFormation StackSet AWS-Funktion verwenden, um diese Lösung auf mehrere AWS-Konten und AWS-Regionen auszudehnen. Weitere Informationen finden Sie CloudFormation StackSets im CloudFormation Benutzerhandbuch unter Arbeiten mit AWS.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.

- Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS-Umgebung zu identifizieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Epen

Erstellen Sie die CloudFormation Vorlage und stellen Sie den Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CloudFormation Vorlage.	1. Kopieren Sie den Code in der CloudFormation Vorlage im Abschnitt Zusätzliche Informationen. 2. Fügen Sie den Code in einen Texteditor ein. 3. Speichern Sie die Datei wie `sample.yaml` auf Ihrer Workstation.	AWS DevOps
Erstellen Sie den CloudFormation Stack.	1. Geben Sie in AWS CLI den folgenden Befehl ein. Dadurch wird mithilfe der `sample.yaml` Datei ein neuer CloudFormation Stack erstellt. Weitere Informationen finden Sie im CloudFormation Benutzerhandbuch unter Einen Stapel erstellen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws cloudformation create-stack \ --stack-name guardduty-cf-stack \ --template-body file://sample.yaml`
	2. Vergewissern Sie sich, dass der folgende Wert in der AWS-CLI angezeigt wird, was darauf hinweist, dass der Stack erfolgreich erstellt wurde. Der Zeitaufwand für die Erstellung des Stacks kann variieren.
	`"StackStatus": "CREATE_COMPLETE",`	

Stellen Sie sicher, GuardDuty dass dies für das AWS-Konto aktiviert ist.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 2. Stellen Sie sicher, dass der GuardDuty Service aktiviert ist.	Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie zusätzliche Konten oder AWS-Regionen.	Verwenden Sie je nach Bedarf die CloudFormation StackSet AWS-Funktion, um diese Lösung auf mehrere AWS-Konten und AWS-Regio nen auszudehnen. Weitere Informationen finden Sie CloudFormation StackSets im CloudFormation Benutzerh andbuch unter Arbeiten mit AWS.	Cloud-Administrator, AWS-Administrator

Zugehörige Ressourcen

Referenzen

- CloudFormation AWS-Dokumentation
- Referenz zum AWS-Lambda-Ressourcentyp
- CloudFormation Ressourcentyp: AWS::IAM::Role
- CloudFormation Ressourcentyp: AWS::GuardDuty::Detector
- Vier Möglichkeiten, AWS-Serviceimmobilien mithilfe von AWS abzurufen CloudFormation (Blog)

Tutorials und Videos

- Vereinfachen Sie Ihr Infrastrukturmanagement mit AWS CloudFormation (Tutorial)
- Verwenden Sie Amazon GuardDuty und AWS Security Hub, um mehrere Konten zu sichern (AWS re:Invent 2020)
- Bewährte Methoden für die Erstellung von AWS CloudFormation (AWS re:Invent 2019)
- Bedrohungserkennung auf AWS: Eine Einführung in Amazon GuardDuty (AWS re:InForce 2019)

Zusätzliche Informationen

CloudFormation Vorlage

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  rLambdaLogGroup:
    Type: 'AWS::Logs::LogGroup'
    DeletionPolicy: Delete
    Properties:
      RetentionInDays: 7
      LogGroupName: /aws/lambda/resource-checker
  rLambdaCheckerLambdaRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Sub 'resource-checker-lambda-role-${AWS::Region}'
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: /
      Policies:
        - PolicyName: !Sub 'resource-checker-lambda-policy-${AWS::Region}'
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Sid: CreateLogGroup
                Effect: Allow
                Action:
                  - 'logs:CreateLogGroup'
                  - 'logs:CreateLogStream'
                  - 'logs:PutLogEvents'
                  - 'iam:CreateServiceLinkedRole'
                  - 'cloudformation:CreateStack'
                  - 'cloudformation:DeleteStack'
                  - 'cloudformation:Desc*'
                  - 'guardduty:CreateDetector'
                  - 'guardduty:ListDetectors'
                  - 'guardduty:DeleteDetector'
                Resource: '*'
  resourceCheckerLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Description: Checks for resource type enabled and possibly name to exist
```

```
      FunctionName: resource-checker
      Handler: index.lambda_handler
      Role: !GetAtt
        - rLambdaCheckerLambdaRole
        - Arn
      Runtime: python3.8
      MemorySize: 128
      Timeout: 180
      Code:
        ZipFile: |
          import boto3
          import os
          import json
          from botocore.exceptions import ClientError
          import cfnresponse


          guardduty=boto3.client('guardduty')
          cfn=boto3.client('cloudformation')


          def lambda_handler(event, context):
              print('Event: ', event)
              if 'RequestType' in event:
                if event['RequestType'] in ["Create","Update"]:
                    enabled=False
                    try:
                      response=guardduty.list_detectors()
                      if "DetectorIds" in response and len(response["DetectorIds"])>0:
                        enabled="AlreadyEnabled"
                      elif "DetectorIds" in response and
len(response["DetectorIds"])==0:
                        cfn_response=cfn.create_stack(
                          StackName='guardduty-cfn-stack',
                          TemplateBody='{ "AWSTemplateFormatVersion": "2010-09-09",
"Description": "A sample template",    "Resources": { "IRWorkshopGuardDutyDetector": {
 "Type": "AWS::GuardDuty::Detector",    "Properties": {   "Enable": true  }   } } }'
                          )
                        enabled="True"
                    except Exception as e:
                        print("Exception: ",e)
                    responseData = {}
                    responseData['status'] = enabled
```

```
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
 "CustomResourcePhysicalID" )
                elif event['RequestType'] == "Delete":
                    cfn_response=cfn.delete_stack(
                            StackName='guardduty-cfn-stack')
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, {})
  CheckResourceExist:
    Type: 'Custom::LambdaCustomResource'
    Properties:
      ServiceToken: !GetAtt
        - resourceCheckerLambda
        - Arn
Outputs:
  status:
    Value: !GetAtt
      - CheckResourceExist
      - status
```

Alternative Codeoption für die Lambda-Ressource

Die bereitgestellte CloudFormation Vorlage verwendet Inline-Code, um auf die Lambda-Ressource zu verweisen, um die Referenz und Anleitung zu erleichtern. Alternativ können Sie den Lambda-Code in einem Amazon Simple Storage Service (Amazon S3) -Bucket platzieren und in der CloudFormation Vorlage darauf verweisen. Inline-Code unterstützt keine Paketabhängigkeiten oder Bibliotheken. Sie können diese unterstützen, indem Sie den Lambda-Code in einem S3-Bucket platzieren und in der CloudFormation Vorlage darauf verweisen.

Ersetzen Sie die folgenden Codezeilen:

```
Code:
         ZipFile: |
```

durch die folgenden Codezeilen:

```
Code:
      S3Bucket: <bucket name>
      S3Key: <python file name>
      S3ObjectVersion: <version>
```

Die `S3ObjectVersion` Eigenschaft kann weggelassen werden, wenn Sie in Ihrem S3-Bucket keine Versionierung verwenden. Weitere Informationen finden Sie unter Verwenden der Versionierung in S3-Buckets im Amazon S3 S3-Benutzerhandbuch.

Aktivieren der transparenten Datenverschlüsselung in Amazon RDS für SQL Server

Erstellt von Ranga Cherukuri (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Datenbanken	Workload: Microsoft
AWS-Services: Amazon RDS		

Übersicht

Dieses Muster beschreibt, wie Sie die transparente Datenverschlüsselung (Transparent Data Encryption, TDE) in Amazon Relational Database Service (Amazon RDS) für SQL Server implementieren, um Daten im Ruhezustand zu verschlüsseln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine DB-Instance von Amazon RDS für SQL Server

Produktversionen

Amazon RDS unterstützt derzeit TDE für die folgenden SQL Server-Versionen und -Editionen:

- SQL Server 2012 Enterprise Edition
- SQL Server 2014 Enterprise Edition
- SQL Server 2016 Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2019: Standard- und Enterprise Editions

Aktuelle Informationen zu unterstützten Versionen und Editionen finden Sie unter Unterstützung für transparente Datenverschlüsselung in SQL Server in der Amazon-RDS-Dokumentation.

Architektur

Technologie-Stack

- Amazon RDS für SQL Server

Architektur

Tools

Tools

- Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung einer SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Polen

Erstellen einer Optionsgruppe in der Amazon-RDS-Konsole

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie die Amazon RDS-Konsole.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole .	Entwickler, DBA
Erstellen Sie eine Optionsgruppe.	Wählen Sie im Navigationsbereich Optionsgruppen, Gruppe erstellen aus. Wählen Sie sqlserver-ee als DB-Engine und dann die Engine-Version aus.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Option TRANSPARENT_DATA_ENCRYPTION hinzu.	Bearbeiten Sie die von Ihnen erstellte Optionsgruppe und fügen Sie die Option mit dem Namen hinzu`TRANSPARENT_DATA_ENCRYPTION` .	Entwickler, DBA

Zuordnen der Optionsgruppe zu einer DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die DB-Instance aus.	Wählen Sie im Navigationsbereich der Amazon-RDS-Konsole Datenbanken und dann die DB-Instance aus, die Sie der Optionsgruppe zuordnen möchten.	Entwickler, DBA
Ordnen Sie die DB-Instance der Optionsgruppe zu.	Wählen Sie Ändern und verwenden Sie dann die Einstellung Optionsgruppe, um die SQL Server-DB-Instance der zuvor erstellten Optionsgruppe zuzuordnen.	Entwickler, DBA
Wenden Sie die Änderungen an.	Wenden Sie die Änderungen wie gewünscht sofort oder während des nächsten Wartungsfensters an.	Entwickler, DBA
Rufen Sie den Zertifikatnamen ab.	Rufen Sie den Standardzertifikatnamen ab, indem Sie die folgende Abfrage verwenden. `USE [master]`	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	GO SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECe rtificate%' GO	

Erstellen des Datenbankverschlüsselungsschlüssels

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe von SSMS eine Verbindung mit der DB-Instance von Amazon RDS für SQL Server her.	Anweisungen finden Sie unter Verwenden von SSMS in der Microsoft-Dokumentation.	Entwickler, DBA
Erstellen Sie den Datenbank verschlüsselungsschlüssel mit dem Standardzertifikat.	Erstellen Sie einen Datenbank verschlüsselungsschlüssel, indem Sie den Standardz ertifikatnamen verwenden , den Sie zuvor erhalten haben. Verwenden Sie die folgende T-SQL-Abfrage, um einen Datenbankverschlüs selungsschlüssel zu erstellen . Sie können den AES_256-Algorithmus anstelle von AES_128 angeben. USE [Databasename] GO CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_128	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ENCRYPTION BY SERVER CERTIFICATE [certificatename]` `GO`	

Aktivieren Sie die Verschlüsselung für die Datenbank.	Verwenden Sie die folgende T-SQL-Abfrage, um die Datenbankverschlüsselung zu aktivieren.
	`ALTER DATABASE [Database Name]`
	`SET ENCRYPTION ON`
	`GO`
		Entwickler, DBA

Überprüfen Sie den Status der Verschlüsselung.	Verwenden Sie die folgende T-SQL-Abfrage, um den Status der Verschlüsselung zu überprüfen. `SELECT DB_NAME(database_id) AS DatabaseName, encryption_state, percent_complete FROM sys.dm_database_encryption_keys`	Entwickler, DBA

Zugehörige Ressourcen

- Unterstützung für transparente Datenverschlüsselung in SQL Server (Amazon-RDS-Dokumentation)
- Arbeiten mit Optionsgruppen (Amazon-RDS-Dokumentation)
- Ändern einer Amazon RDS-DB-Instance (Amazon RDS-Dokumentation)
- Transparente Datenverschlüsselung für SQL Server (Microsoft-Dokumentation)

- Verwenden von SSMS (Microsoft-Dokumentation)

Stellen Sie sicher, dass CloudFormation AWS-Stacks von autorisierten S3-Buckets aus gestartet werden

Umwelt: Produktion	Technologien: Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon SNS; AWS CloudFormation; Amazon CloudWatch; AWS Lambda; Amazon S3		

Übersicht

Sie können CloudFormation AWS-Vorlagen verwenden, um Amazon Web Services (AWS) -Ressourcen programmgesteuert einzurichten, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden. Dieses Muster bietet eine Möglichkeit zu überprüfen, ob CloudFormation AWS-Stacks nur aus Vorlagen erstellt werden, die in bestimmten Amazon Simple Storage Service (Amazon S3) -Buckets gespeichert sind. Diese Prüfung ist nützlich, wenn Sie eine Sicherheits- oder Compliance-Anforderung haben, die Verwendung von Vorlagen vorschreibt, die in S3-Buckets gespeichert sind, die sich in einer Zulassungsliste befinden.

Diese Sicherheitskontrolle überwacht die AWS CloudFormation CreateStack- und UpdateStackAPI-Aufrufe und ruft eine AWS-Lambda-Funktion auf, die überprüft, ob die im Aufruf verwendete Vorlage aus einem autorisierten S3-Bucket stammt. Wenn die Vorlage aus einem nicht autorisierten Bucket stammt, löst die Lambda-Funktion eine E-Mail-Benachrichtigung des Amazon Simple Notification Service (Amazon SNS) mit den entsprechenden Informationen an den Benutzer aus.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten
- Ein S3-Bucket zum Hochladen des bereitgestellten Lambda-Codes
- Eine Liste autorisierter S3-Bucket-Namen

Einschränkungen

- UpdateStackAPI-Aufrufe, die eine vorhandene Vorlage in einem nicht autorisierten S3-Bucket verwenden, erzeugen keine zusätzlichen Verstöße, da die URL für den S3-Bucket im EventBridge Amazon-Event nicht verfügbar ist. Wir empfehlen, dass Sie vorhandene Vorlagen aus nicht autorisierten S3-Buckets löschen, nachdem Sie die ursprüngliche Benachrichtigung über den CreateStackVerstoß erhalten haben.
- Diese Sicherheitskontrolle überwacht die folgenden CloudFormation AWS-Ereignisse nicht, da sie Updates nach der ersten Bereitstellung der Vorlage verarbeiten: CreateChangeSet, CreateStackSet, UpdateStackSet.
- Sie müssen diese Sicherheitskontrolle in jeder AWS-Region einsetzen, die Sie überwachen möchten.

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon SNS
- EventBridge Amazon-Regel

Zielarchitektur

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS verwenden, CloudFormation StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

- AWS Cloudformation — Unterstützt Sie bei der Modellierung und Einrichtung von AWS-Ressourcen mithilfe eines infrastructure-as-code Modells.
- Amazon EventBridge — Stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, software-as-a-service (SaaS-) Anwendungen und AWS-Services bereit und leitet diese Daten an Ziele wie AWS Lambda weiter.

- AWS Lambda — Ermöglicht die Ausführung von Code, ohne Server bereitzustellen oder zu verwalten.
- Amazon SNS — Ermöglicht die Nachrichtenzustellung von Verlagen an Abonnenten. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.
- Amazon S3 — Ermöglicht das Speichern und Abrufen beliebiger Datenmengen zu jeder Zeit und von überall im Internet.

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code auf Amazon S3 hoch.	Laden Sie die ZIP-Datei, die den Lambda-Code enthält, der im Abschnitt „Anlagen“ bereitgestellt wird, in einen neuen oder vorhandenen S3-Bucket hoch. Dieser Bucket sollte sich in derselben AWS-Region befinden wie die Ressourcen, die Sie bewerten möchten.	Cloud-Architekt
Stellen Sie die CloudForm ation AWS-Vorlage bereit.	Öffnen Sie die CloudForm ation AWS-Konsole in derselben Region wie Ihr S3-Bucket und stellen Sie die im Abschnitt „Anlagen“ bereitges tellte Vorlage bereit. Geben Sie Werte für die Parameter an. Diese werden im Abschnitt „Zusätzliche Informationen“ beschrieben.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement für das Amazon SNS SNS-Thema.	Wenn die CloudFormation AWS-Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegeben e E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachric htigungen zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Bereitstellung von CloudFormation AWS-Vorlagen
- Amazon EventBridge
- AWS Lambda
- Amazon S3

Zusätzliche Informationen

Wenn Sie die mit diesem Muster bereitgestellte CloudFormation AWS-Vorlage bereitstellen, werden Sie zur Eingabe der folgenden Informationen aufgefordert:

- S3-Bucket: Geben Sie den Bucket an, in den Sie den angehängten Lambda-Code (.zip-Datei) hochgeladen haben. Sie können einen neuen Bucket erstellen oder einen vorhandenen Bucket angeben.
- S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B.: Dateiname .zip oder controls/ filename .zip). Verwenden Sie keine führenden Schrägstriche.
- Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, an die Benachrichtigungen über Verstöße gesendet werden sollen.
- Lambda-Protokollierungsebene: Geben Sie die Protokollierungsebene für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen über den Fortschritt, Fehler

für Fehlerereignisse, die die Fortsetzung der Bereitstellung dennoch ermöglichen würden, und Warnmeldungen für potenziell schädliche Situationen zu protokollieren.

- Autorisierte Buckets: Geben Sie eine durch Kommas getrennte Liste autorisierter S3-Buckets an.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Sicherstellen, dass AWS Load Balancer sichere Listener-Protokolle (HTTPS, SSL/TLS) verwenden

Erstellt von Chandini Penmetsa (AWS) und Purushotham G K (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance	Workload: Alle anderen Workloads
AWS-Services: Amazon SNS ; AWS CloudFormation; Amazon CloudWatch; AWS Lambda ; Elastic Load Balancing (ELB)		

Übersicht

In der Amazon Web Services (AWS) Cloud verteilt Elastic Load Balancing eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container, IP-Adressen und AWS Lambda-Funktionen. Die Load Balancer verwenden Listener, um die Ports und Protokolle zu definieren, die der Load Balancer verwendet, um Datenverkehr von Benutzern zu akzeptieren. Application Load Balancer treffen Routing-Entscheidungen auf Anwendungsebene und verwenden die HTTP/HTTPS-Protokolle. Network Load Balancer treffen Routing-Entscheidungen auf der Transportebene und verwenden die Protokolle Transmission Control Protocol (TCP), Transport Layer Security (TLS), User Datagram Protcol (UDP) oder TCP_UDP. Classic Load Balancer treffen Routing-Entscheidungen entweder auf der Transportebene, mithilfe von TCP- oder Secure Sockets Layer (SSL)-Protokollen oder auf der Anwendungsebene mithilfe von HTTP/HTTPS.

Ihre Organisation hat möglicherweise eine Sicherheits- oder Compliance-Anforderung, dass Load Balancer Datenverkehr von Benutzern nur über sichere Protokolle wie HTTPS oder SSL/TLS akzeptieren.

Dieses Muster bietet eine Sicherheitskontrolle, die eine Amazon- EventBridge Regel verwendet, um die - `CreateListener` und `ModifyListener`-API-Aufrufe für Application Load Balancer und Network Load Balancer sowie die - `CreateLoadBalancerListeners` und

`CreateLoadBalancer`-API-Aufrufe für Classic Load Balancer zu überwachen. Wenn HTTP, TCP/UDP oder TCP_UDP für das Listener-Protokoll des Load Balancers verwendet wird, ruft die Steuerung eine Lambda-Funktion auf. Die Lambda-Funktion veröffentlicht eine Nachricht in einem Amazon Simple Notification Service (Amazon SNS)-Thema, um eine Benachrichtigung zu senden, die die Load Balancer-Details enthält.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Benachrichtigung über den Verstoß erhalten möchten
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket zum Speichern der ZIP-Datei des Lambda-Codes

Einschränkungen

- Diese Sicherheitskontrolle prüft nicht auf vorhandene Load Balancer, es sei denn, es wird eine Aktualisierung der Load-Balancer-Listener vorgenommen.
- Diese Sicherheitskontrolle ist regional und muss in den AWS-Regionen bereitgestellt werden, die Sie überwachen möchten.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- Amazon SNS-Thema
- EventBridge Regel

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung von AWS-Ressourcen unterstützt, indem Infrastruktur als Code verwendet wird.
- Amazon EventBridge – Amazon EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software as a Service (SaaS)-Anwendungen und AWS-Services bereit und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambda – Lambda unterstützt das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Bewährte Methoden

Stellen Sie sicher, dass das verwendete SNS-Thema nicht öffentlich zugänglich ist. Weitere Informationen finden Sie in der AWS-Dokumentation.

Polen

Laden Sie den Lambda-Code hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstr iche enthält. Ein S3-Bucket -Name ist global eindeutig und der Namespace wird	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben Region befinden wie der Load Balancer, der ausgewertet wird.	
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die ZIP-Datei des Lambda-Codes, die im Abschnitt „Anfügungen“ bereitgestellt wird, in den definierten S3-Bucket hoch.	Cloud-Architektur
Stellen Sie die AWS-CloudFormation Vorlage bereit.	Stellen Sie in der AWS-CloudFormation Konsole in derselben AWS-Region wie der S3-Bucket die Vorlage bereit, die im Abschnitt „Anfügungen“ bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an.	Cloud-Architektur

CloudFormation -Parameter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Benennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epos erstellt haben.	Cloud-Architektur
Geben Sie das Amazon S3-Präfix an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket ohne voranstehende Schrägstriche	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an (z. B. `<directory>/<file-name>.zip`).	
Geben Sie den ARN des SNS-Themas an.	Geben Sie den Amazon-Ressourcennamen (ARN) des SNS-Themas an, wenn Sie ein vorhandenes SNS-Thema für Benachrichtigungen über Verstöße verwenden möchten. Um ein neues SNS-Thema zu erstellen, behalten Sie den Wert als `None` (Standardwert) bei.	Cloud-Architektur
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS-Benachrichtigungen zu erhalten.	Cloud-Architektur
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und -häufigkeit für Ihre Lambda-Funktion. `Info` bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. `Error` bezeichnet Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. `Warning` bezeichnet potenziell schädliche Situationen.	Cloud-Architektur

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Vorlage für herunter.	Laden Sie die CloudFormation Vorlage herunter, die im Abschnitt Anhänge bereitgestellt wird.	Cloud-Architekt
Erstellen Sie den Stack.	Navigieren Sie in derselben Region wie der S3-Bucket zur CloudFormation Servicekonsole und stellen Sie die heruntergeladene Vorlage bereit. Weitere Parameterdetails finden Sie im vorherigen Epic.	Cloud-Architekt
Überprüfen Sie die Ressourcen.	Nachdem der Stack vollständig erstellt wurde, navigieren Sie zur Registerkarte Ressourcen und überprüfen Sie die Ressourcen. Die Vorlage erstellt die folgenden Ressourcen: • EventBridge Regel • Lambda-Funktion • Lambda-Ausführungsrolle • Lambda-Aufrufberechtigung	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde und ein neues SNS-Thema erstellt wurde, wird eine Abonnement-E-Mail-Nachricht an die in den Parametern angegebene E-Mail-Adresse gesendet. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Die Stack-Erstellung ist fehlgeschlagen. Es ist ein Fehler aufgetreten, während GetObject . S3-Fehlercode: PermanentRedirect. S3-Fehlermeldung: Der Bucket befindet sich in dieser Region: xx-xxxx-1. Bitte verwenden Sie diese Region, um die Anforderung erneut zu versuchen.	Stellen Sie sicher, dass die S3-Bucket-Region und die Region, in der der Stack bereitgestellt wird, identisch sind.
Die Stack-Erstellung ist fehlgeschlagen. Der Laufzeitparameter von python3.6 wird für das Erstellen oder Aktualisieren von AWS Lambda-Funktionen nicht mehr unterstützt.	Aktualisieren Sie die heruntergeladene Vorlage in Zeile 186 von Python Version 3.6 auf 3.9.

Zugehörige Ressourcen

- Erstellen eines Stacks in der AWS- CloudFormation Konsole
- AWS Lambda
- Was ist ein Classic Load Balancer?
- Was ist ein Application Load Balancer?
- Was ist ein Network Load Balancer?
- Bewährte Methoden für die Arbeit mit AWS Lambda-Funktionen
- CloudFormation Bewährte Methoden für AWS

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Sicherstellen, dass die Verschlüsselung für Amazon-EMR-Daten im Ruhezustand beim Start aktiviert ist

Erstellt von Priyanka Chaudhary (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Analytik	Workload: Open-Source
AWS-Services: Amazon EMR; Amazon SNS; AWS KMS; AWS CloudFormation; AWS Lambda ;Amazon S3		

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle zur Überwachung der Verschlüsselung von Amazon-EMR-Clustern auf Amazon Web Services (AWS).

Die Datenverschlüsselung verhindert, dass nicht autorisierte Benutzer Daten auf einem Cluster und in den dazugehörigen Datenspeichersystemen lesen können. Dazu gehören Daten, die abgefangen werden können, während es das Netzwerk durchquert, die als Daten während der Übertragung bezeichnet werden, und Daten, die auf persistenten Medien gespeichert werden, die als Daten im Ruhezustand bezeichnet werden. Daten im Ruhezustand in Amazon Simple Storage Service (Amazon S3) können auf zwei Arten verschlüsselt werden.

- Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3)
- Serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS)-Schlüsseln (SSE-KMS), eingerichtet mit Richtlinien, die für Amazon EMR geeignet sind.

Diese Sicherheitskontrolle überwacht API-Aufrufe und initiiert ein Amazon CloudWatch Events-Ereignis auf RunJobFlow. Der Auslöser ruft AWS Lambda auf, das ein Python-Skript ausführt. Die Funktion ruft die EMR-Cluster-ID aus der Ereignis-JSON-Eingabe ab und bestimmt, ob ein Sicherheitsverstoß vorliegt, indem sie die folgenden Prüfungen durchführt.

1. Überprüfen Sie, ob ein EMR-Cluster einer Amazon-EMR-spezifischen Sicherheitskonfiguration zugeordnet ist.

2. Wenn dem EMR-Cluster eine Amazon-EMR-spezifische Sicherheitskonfiguration zugeordnet ist, überprüfen Sie, ob Verschlüsselung im Ruhezustand aktiviert ist.
3. Wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist, senden Sie eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung, die den Namen des EMR-Clusters, die Details zu Verstößen, die AWS-Region, das AWS-Konto und den Lambda Amazon-Ressourcennamen (ARN) enthält, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket für die ZIP-Datei des Lambda-Codes
- Eine E-Mail-Adresse, an die Sie die Benachrichtigung über einen Verstoß erhalten möchten
- Die Amazon-EMR-Protokollierung ist deaktiviert, sodass alle API-Protokolle abgerufen werden können

Einschränkungen

- Diese detektivische Kontrolle ist regional und muss in den AWS-Regionen bereitgestellt werden, die Sie überwachen möchten.

Produktversionen

- Amazon-EMR-Version 4.8.0 und höher

Architektur

Zieltechnologie-Stack

- Amazon EMR
- Amazon- CloudWatch Events-Ereignis
- Lambda-Funktion
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

Tools

- AWS CloudFormation – AWS CloudFormation ist ein Service, der Ihnen hilft, AWS-Ressourcen mithilfe von Infrastructure as Code zu modellieren und einzurichten.
- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.
- Amazon EMR – Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks vereinfacht.
- AWS Lambda – AWS Lambda unterstützt das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon S3 – Amazon S3 ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon SNS koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

- Die EMR-EncryptionAtRestZIP- und EMR-EncryptionAtRestYML-Dateien für dieses Projekt sind als Anhang verfügbar.

Polen

Definieren des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben Region wie der Amazon-EMR-Cluster befinden, der ausgewertet wird.	Cloud-Architektur

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die ZIP-Datei des Lambda-Codes, die im Abschnitt „Anfügungen“ bereitgestellt wird, in den definierten S3-Bucket hoch.	Cloud-Architektur

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CloudFormation Vorlage bereit.	Stellen Sie in der AWS-CloudFormation Konsole in derselben Region wie Ihr S3-Bucket die AWS- CloudFormation Vorlage bereit, die als Anhang zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an. Weitere Informationen zum Bereitstellen von AWS- CloudFormation Vorlagen finden Sie im Abschnitt „Verwandte Ressourcen“.	Cloud-Architektur

Vervollständigen der Parameter in der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Benennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epos erstellt haben.	Cloud-Architektur
Geben Sie den Amazon S3-Schlüssel an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket an, ohne Schrägstriche voranzustellen (z. B. <directory>/<file-name>.zip).	Cloud-Architektur
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SNS-Benachrichtigungen zu erhalten.	
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. „Informationen“ bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. „Fehler“ bezeichnet Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. „Warnung“ bezeichnet potenziell schädliche Situationen.	Cloud-Architektur

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architektur

Zugehörige Ressourcen

- Erstellen eines Stacks in der AWS- CloudFormation Konsole
- AWS Lambda
- Amazon-EMR-Verschlüsselungsoptionen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Sicherstellen, dass ein IAM-Profil einer EC2-Instance zugeordnet ist

Erstellt von Mansi Suratwala (AWS)

Umgebung: Produktion	Technologien: Infrastruktur; Sicherheit, Identität, Compliance	AWS-Services: Amazon EC2; AWS Identity and Access Management; Amazon CloudWatch; AWS Lambda ;Amazon SNS

Übersicht

Dieses Muster bietet eine AWS- CloudFormation Sicherheitskontrollvorlage, die automatische Benachrichtigungen einrichtet, wenn ein AWS Identity and Access Management (IAM)-Profilverstoß für eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance auftritt.

Ein Instance-Profil ist ein Container für eine IAM-Rolle, mit dem Sie Rolleninformationen an eine EC2-Instance übergeben können, wenn die Instance gestartet wird.

Amazon CloudWatch Events initiiert diese Prüfung, wenn AWS Amazon EC2-API-Aufrufe basierend auf den `ReplaceIamInstanceProfileAssociation` Aktionen `RunInstances`, `AssociateIamInstanceProfile`und CloudTrail protokolliert. Der Auslöser ruft eine AWS Lambda-Funktion auf, die ein Amazon CloudWatch Events-Ereignis verwendet, um nach einem IAM-Profil zu suchen.

Wenn kein IAM-Profil vorhanden ist, initiiert die Lambda-Funktion eine Amazon Simple Notification Service (Amazon SNS)-E-Mail-Benachrichtigung, die die Amazon Web Services (AWS)-Konto-ID und die AWS-Region enthält.

Wenn ein IAM-Profil vorhanden ist, prüft die Lambda-Funktion auf Platzhaltereinträge in den Richtliniendokumenten. Wenn die Platzhaltereinträge vorhanden sind, initiiert eine Amazon SNS-Verstoßbenachrichtigung, mit der Sie die erweiterte Sicherheit implementieren können. Die Benachrichtigung enthält den Namen des IAM-Profils, das Ereignis, die EC2-Instance-ID, den Namen der verwalteten Richtlinie, den Verstoß, die Konto-ID und die Region.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Konto
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket für die ZIP-Datei des Lambda-Codes

Einschränkungen

- Die AWS- CloudFormation Vorlage darf nur für die `ReplaceIamInstanceProfileAssociation` Aktionen `RunInstancesAssociateIamInstanceProfile`, und bereitgestellt werden.
- Die Sicherheitskontrolle überwacht nicht die Trennung von IAM-Profilen.
- Die Sicherheitskontrolle prüft nicht, ob IAM-Richtlinien geändert wurden, die dem EC2-Instance-IAM-Profil angefügt sind.
- Die Sicherheitskontrolle berücksichtigt nicht unterstützte Berechtigungen auf Ressourcenebene, die die Verwendung von erfordern`"Resource":*`.

Architektur

Zieltechnologie-Stack

- Amazon EC2
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die AWS- CloudFormation Vorlage mehrmals für verschiedene AWS-Regionen und -Konten verwenden. Sie müssen die Vorlage nur einmal für jedes Konto oder jede Region starten.

Tools

Tools

- Amazon EC2 – Amazon EC2 bietet skalierbare Rechenkapazität (virtuelle Server) in der AWS Cloud.
- AWS CloudTrail – AWS CloudTrail unterstützt Sie bei der Aktivierung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos. Aktionen eines Benutzers, einer Rolle oder eines AWS-Services werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 – Amazon S3 bietet hoch skalierbaren Objektspeicher, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon SNS ermöglicht es Anwendungen und Geräten, Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Polen

Definieren des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Um die ZIP-Datei des Lambda-Codes zu hosten,	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen oder erstellen Sie einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben Region befinden wie die EC2-Insta nce, die ausgewertet wird.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den Lambda-Co de, der im Abschnitt Anhänge bereitgestellt wird, in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie die EC2-Insta nce, die ausgewertet wird.	Cloud-Architektur

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CloudFormation Vorlage bereit.	Stellen Sie die AWS-CloudFormation Vorlage bereit, die als Anhang zu diesem Muster bereitges tellt wird. Geben Sie im	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nächsten Epic die Werte für die Parameter an.	

Vervollständigen der Parameter in der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Benennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epos erstellt haben.	Cloud-Architektur
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket ohne voranstehende Schrägstriche an (z. B. `<directory>/<file-name>.zip`).	Cloud-Architektur
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS-Benachrichtigungen zu erhalten.	Cloud-Architektur
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info` bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. `Error` bezeichnet Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. `Warning` bezeichnet	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	potenziell schädliche Situation en.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachric htigungen über Verstöße zu erhalten.	Cloud-Architektur

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Hochladen von Dateien in einen S3-Bucket
- Verwenden von Instance-Profilen
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Sicherstellen, dass ein Amazon-Redshift-Cluster bei der Erstellung verschlüsselt wird

Erstellt von Mansi Suratwala (AWS)

Umgebung: Produktion	Technologien: Analytik; Data Lakes; Sicherheit, Identität, Compliance	Workload: Alle anderen Workloads
AWS-Services: Amazon Redshift; Amazon SNS; AWS CloudTrail; Amazon CloudWatch; AWS Lambda ;Amazon S3		

Übersicht

Dieses Muster bietet eine AWS- CloudFormation Vorlage, die Ihnen automatische Benachrichtigungen bereitstellt, wenn ein neuer Amazon-Redshift-Cluster ohne Verschlüsselung erstellt wird.

Die AWS- CloudFormation Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS Lambda-Funktion. Das Ereignis überwacht, ob ein Amazon-Redshift-Cluster über AWS erstellt oder aus einem Snapshot wiederhergestellt wird CloudTrail. Wenn der Cluster ohne AWS Key Management Service (AWS KMS)- oder Cloud Hardware Security Model (HSM)-Verschlüsselung im AWS-Konto erstellt wird, CloudWatch initiiert eine Lambda-Funktion, die Ihnen eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung sendet, die Sie über den Verstoß informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Virtual Private Cloud (VPC) mit einer Cluster-Subnetzgruppe und einer zugehörigen Sicherheitsgruppe.

Einschränkungen

- Die AWS- CloudFormation Vorlage kann nur für die `RestoreFromClusterSnapshot` Aktionen `CreateCluster` und bereitgestellt werden.

Architektur

Zieltechnologie-Stack

- Amazon Redshift
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die AWS- CloudFormation Vorlage mehrmals für verschiedene AWS-Regionen und -Konten verwenden. Sie müssen sie nur einmal in jeder Region oder jedem Konto ausführen.

Tools

Tools

- Amazon Redshift – Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service in Petabytegröße in der Cloud. Amazon Redshift ist in Ihren Data Lake integriert, sodass Sie Ihre Daten verwenden können, um neue Erkenntnisse für Ihr Unternehmen und Ihre Kunden zu gewinnen.
- AWS CloudTrail – AWS CloudTrail ist ein AWS-Service, der Sie bei der Implementierung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos unterstützt. Aktionen eines Benutzers, einer Rolle oder eines AWS-Services werden als Ereignisse in aufgezeichnet CloudTrail.

- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.
- AWS Lambda – AWS Lambda unterstützt das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 – Amazon S3 ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon SNS ist ein Webservice, der die Zustellung oder das Senden von Nachrichten an zwischen Publishern und Clients koordiniert und verwaltet, einschließlich Webservern und E-Mail-Adressen.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Polen

Definieren des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket. Dieser S3-Bucket hostet die ZIP-Datei des Lambda-Codes. Ihr S3-Bucket muss sich in derselben Region befinden wie der Amazon-Redshift-Cluster, der ausgewertet wird. Der Name des S3-Buckets darf keine führenden Schrägstriche enthalten.	Cloud-Architektur

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den im Abschnitt Anhänge bereitgestellten Lambda-Code in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie der Amazon-Redshift-Cluster, der ausgewertet wird.	Cloud-Architektur

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CloudFormation Vorlage bereit.	Stellen Sie die AWS-CloudFormation Vorlage bereit, die als Anhang zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an.	Cloud-Architektur

Vervollständigen der Parameter in der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Benennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epos erstellt haben.	Cloud-Architektur
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket ohne	Cloud-Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	voranstehende Schrägstriche an (z. B. `<directory>/<file-name>.zip`).	
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS-Benachrichtigungen zu erhalten.	Cloud-Architektur
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und -häufigkeit für Ihre Lambda-Funktion. `Info` bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. `Error` bezeichnet Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. `Warning` bezeichnet potenziell schädliche Situationen.	Cloud-Architektur

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architektur

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Hochladen von Dateien in einen S3-Bucket
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail
- Erstellen eines Amazon-Redshift-Clusters

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Exportieren Sie einen Bericht über AWS IAM Identity Center-Identitäten und deren Zuweisungen mithilfe von PowerShell

Erstellt von Jorge Pava (AWS), Chad Bol (AWS), Allotta (AWS) und Manideep Reddy Gla (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Management und Governance	Workload: Microsoft
AWS-Services: IAM Identity Center; AWS-Tools für PowerShell		

Übersicht

Wenn Sie AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) verwenden, um den SSO-Zugriff (Single Sign-On) auf alle Ihre Amazon Web Services (AWS)-Konten und Cloud-Anwendungen zentral zu verwalten, kann die Meldung und Prüfung dieser Zuweisungen über die AWS-Managementkonsole mühsam und zeitaufwändig sein. Dies gilt insbesondere, wenn Sie über Berechtigungen für einen Benutzer oder eine Gruppe über Dutzende oder Hunderte von AWS-Konten hinweg berichten.

Für viele wäre das ideale Tool, diese Informationen anzuzeigen, in einer Tabellenkalkulationsanwendung wie Microsoft Excel. Auf diese Weise können Sie die Daten für Ihre gesamte Organisation filtern, durchsuchen und visualisieren, die von AWS Organizations verwaltet wird.

Dieses Muster beschreibt, wie Sie AWS-Tools für verwenden PowerShell , um einen Bericht über SSO-Identitätskonfigurationen in IAM Identity Center zu erstellen. Der Bericht ist als CSV-Datei formatiert und enthält den Identitätsnamen (Prinzipal), den Identitätstyp (Benutzer oder Gruppe), Konten, auf die die Identität zugreifen kann, und Berechtigungssätze. Nachdem Sie diesen Bericht erstellt haben, können Sie ihn in Ihrer bevorzugten Anwendung öffnen, um die Daten nach Bedarf zu suchen, zu filtern und zu prüfen. Die folgende Abbildung zeigt Beispieldaten in einer Tabellenkalkulationsanwendung.

Wichtig: Da dieser Bericht vertrauliche Informationen enthält, empfehlen wir dringend, sie sicher zu speichern und nur need-to-know auf Basis freizugeben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- IAM Identity Center und AWS Organizations , konfiguriert und aktiviert.
- PowerShell, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren von PowerShell (Microsoft-Dokumentation).
- AWS-Tools für PowerShell, installiert und konfiguriert. Aus Leistungsgründen empfehlen wir dringend, die modularisierte Version von AWS-Tools für zu installieren PowerShell. `AWS.Tools` Jeder AWS-Service wird von einem eigenen individuellen, kleinen Modul unterstützt. Geben Sie in der PowerShell Shell die folgenden Befehle ein, um die für dieses Muster erforderlichen Module zu installieren: `AWS.Tools.Installer`, `OrganizationsSSOAdmin`, und `IdentityStore`.

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore
```

  Weitere Informationen finden Sie unter Installieren von AWS.Tools unter Windows oder Installieren von AWS.Tools unter Linux oder macOS (Dokumentation PowerShell zu AWS-Tools). Wenn Sie bei der Installation der Module eine Fehlermeldung erhalten, lesen Sie den Abschnitt Fehlerbehebung dieses Musters.
- AWS Command Line Interface (AWS CLI) oder das AWS SDK müssen zuvor mit funktionierenden Anmeldeinformationen konfiguriert werden, indem Sie einen der folgenden Schritte ausführen:
  - Verwenden Sie die AWS CLI `aws configure` Weitere Informationen finden Sie unter Schnellkonfiguration (AWS CLI-Dokumentation).
  - Konfigurieren Sie AWS CLI oder AWS Cloud Development Kit (AWS CDK), um temporären Zugriff über eine AWS Identity and Access Management (IAM)-Rolle zu erhalten. Weitere Informationen finden Sie unter Abrufen von IAM-Rollenanmeldeinformationen für den CLI-Zugriff (Dokumentation zu IAM Identity Center).
- Ein benanntes Profil für die AWS CLI, das Anmeldeinformationen für einen IAM-Prinzipal gespeichert hat, der:

- Hat Zugriff auf das AWS Organizations-Verwaltungskonto oder das delegierte Administratorkonto für IAM Identity Center
- Hat die von `AWSSSOReadOnly` und `AWSSSODirectoryReadOnly` AWS verwalteten Richtlinien darauf angewendet

Weitere Informationen finden Sie unter Verwenden benannter Profile (AWS CLI-Dokumentation) und Von AWS verwaltete Richtlinien (IAM-Dokumentation).

Einschränkungen

- Die AWS-Zielkonten müssen als Organisation in AWS Organizations verwaltet werden.

Produktversionen

- Für alle Betriebssysteme wird empfohlen, Version PowerShell 7.0 oder höher zu verwenden.

Architektur

Zielarchitektur

1. Der Benutzer führt das Skript in einer PowerShell Befehlszeile aus.
2. Das Skript geht von dem benannten Profil für AWS CLI aus. Dadurch wird Zugriff auf IAM Identity Center gewährt.
3. Das Skript ruft die SSO-Identitätskonfigurationen vom IAM Identity Center ab.
4. Das Skript generiert eine CSV-Datei im selben Verzeichnis auf der lokalen Workstation, in der das Skript gespeichert ist.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- AWS IAM Identity Center hilft Ihnen dabei, den SSO-Zugriff (Single Sign-On) auf alle Ihre AWS-Konten und Cloud-Anwendungen zentral zu verwalten.
- AWS-Tools für PowerShell sind eine Reihe von PowerShell Modulen, die Ihnen helfen, Skriptoperationen für Ihre AWS-Ressourcen über die PowerShell Befehlszeile zu erstellen.

Andere Tools

- PowerShell ist ein Microsoft-Automatisierungs- und Konfigurationsmanagementprogramm, das unter Windows, Linux und macOS ausgeführt wird.

Polen

Generieren des Berichts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das Skript vor.	1. Kopieren Sie das PowerShell Skript im Abschnitt Zusätzliche Informationen dieses Musters. 2. Definieren Sie im `Param` Abschnitt für Ihre AWS-Umgebung die Werte für die folgenden Variablen: • `OutputFile` – Der Dateiname des Berichts. • `ProfileName` – Das benannte AWS CLI-Profil, das Sie zum Generieren des Berichts verwenden möchten. • `Region` – Die AWS-Region, in der IAM Identity Center bereitges	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tellt wird. Eine vollständige Liste der Regionen und ihrer Codes finden Sie unter Regionale Endpunkte. 3. Speichern Sie das Skript mit dem Dateinamen `SSO-Report.ps1` .	

Führen Sie das Skript aus.	Es wird empfohlen, Ihr benutzerdefiniertes Skript in der PowerShell Shell mit dem folgenden Befehl auszuführen.
	`.\SSO-Report.ps1`
	Alternativ können Sie das Skript von einer anderen Shell ausführen, indem Sie den folgenden Befehl eingeben.
	`pwsh .\SSO-Report.ps1`
	Das Skript generiert eine CSV-Datei im selben Verzeichnis wie die Skriptdatei.
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Berichtsdaten.	Die CSV-Ausgabedatei hat die Header AccountName, , PermissionSet Principal und Typ . Öffnen Sie diese Datei in Ihrer bevorzugten Tabellenkalkulationsanwendung. Sie können eine Datentabelle erstellen, um die Ausgabe zu filtern und zu sortieren.	Cloud-Administrator

Fehlerbehebung

Problem	Lösung

`The term 'Get-<parameter>' is not recognized as the name of a cmdlet, function, script file, or operable program.`-Fehler	AWS-Tools für PowerShell oder ihre Module sind nicht installiert. Geben Sie in der PowerShell Shell die folgenden Befehle ein, um AWS-Tools für PowerShell und die für dieses Muster erforderlichen Module zu installieren: `AWS.Tools.Installer` , `Organizations` `SSOAdmin`, und `IdentityStore` .
	`Install-Module AWS.Tools.Installer`
	`Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore`

`No credentials specified or obtained from persisted/shell defaults`-Fehler	Vergewissern Sie sich im Abschnitt Skript vorbereiten im Abschnitt „Epics“, dass Sie die `Region` Variablen `ProfileName` und korrekt eingegeben haben. Stellen Sie sicher, dass die Einstellungen und Anmeldeinformationen im benannten Profil über ausreichende Berechtig

Problem	Lösung
	ungen zur Verwaltung von IAM Identity Center verfügen.
`Authenticode Issuer …` -Fehler bei der Installation der AWS.Tools-Module	Fügen Sie den `-SkipPublisherCheck` Parameter am Ende des `Install-AWSToolsModule` Befehls hinzu.

`Get-ORGAccountList : Assembly AWSSDK.SSO could not be found or loaded.`-Fehler	Dieser Fehler kann auftreten, wenn benannte AWS CLI-Profile angegeben sind, AWS CLI für die Authentifizierung von Benutzern mit IAM Identity Center konfiguriert ist und AWS CLI für den automatischen Abruf aktualisierter Authentifizierungstoken konfiguriert ist. Gehen Sie wie folgt vor, um diesen Fehler zu beheben:
	1. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die `SSOOIDC` Module `SSO` und installiert sind.
	`Install-AWSToolsModule SSO, SSOOIDC`
	2. Fügen Sie die folgenden Zeilen in das Skript unter dem `-param()`Block ein.
	`Import-Module AWS.Tools.SSO`
	`Import-Module AWS.Tools.SSOOIDC`

Zugehörige Ressourcen

- Wo werden die Konfigurationseinstellungen gespeichert? (AWS-CLI-Dokumentation)
- Konfigurieren der AWS CLI für die Verwendung von AWS IAM Identity Center (AWS CLI-Dokumentation)
- Verwenden benannter Profile (AWS-CLI-Dokumentation)

Zusätzliche Informationen

Stellen Sie im folgenden Skript fest, ob Sie die Werte für die folgenden Parameter aktualisieren müssen:

- Wenn Sie ein benanntes Profil in AWS CLI verwenden, um auf das Konto zuzugreifen, in dem IAM Identity Center konfiguriert ist, aktualisieren Sie den `$ProfileName` Wert.
- Wenn IAM Identity Center in einer anderen AWS-Region als der Standardregion für Ihre AWS CLI- oder AWS SDK-Konfiguration bereitgestellt wird, aktualisieren Sie den `$Region` Wert so, dass er die Region verwendet, in der IAM Identity Center bereitgestellt wird.
- Wenn keine dieser Situationen zutrifft, ist kein Skript-Update erforderlich.

```
param (
    # The name of the output CSV file
    [String] $OutputFile  = "SSO-Assignments.csv",
    # The AWS CLI named profile
    [String] $ProfileName = "",
    # The AWS Region in which IAM Identity Center is configured
    [String] $Region      = ""
)
$Start = Get-Date; $OrgParams = @{}
If ($Region){ $OrgParams.Region = $Region}
if ($ProfileName){$OrgParams.ProfileName = $ProfileName}
$SSOParams   = $OrgParams.Clone(); $IdsParams = $OrgParams.Clone()
$AccountList = Get-ORGAccountList @OrgParams | Select-Object Id, Name
$SSOinstance = Get-SSOADMNInstanceList @OrgParams
$SSOParams['InstanceArn']       = $SSOinstance.InstanceArn
$IdsParams['IdentityStoreId']   = $SSOinstance.IdentityStoreId
$PSsets       = @{}; $Principals   = @{}
$Assignments  = @(); $AccountCount = 1; Write-Host ""
foreach ($Account in $AccountList) {
    $Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
    Write-Host "`r$Duration - Account $AccountCount of $($AccountList.Count)
 (Assignments:$($Assignments.Count))        " -NoNewline
    $AccountCount++
    foreach ($PS in Get-SSOADMNPermissionSetsProvisionedToAccountList -AccountId
 $Account.Id @SSOParams) {
        if (-not $PSsets[$PS]) {$PSsets[$PS] = (Get-SSOADMNPermissionSet @SSOParams -
PermissionSetArn $PS).Name;$APICalls++}
```

```
        $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id
        if ($AssignmentsResponse.NextToken) {$AccountAssignments =
 $AssignmentsResponse.AccountAssignments}
        else {$AccountAssignments = $AssignmentsResponse}
        While ($AssignmentsResponse.NextToken) {
            $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id -NextToken $AssignmentsResponse.NextToken
            $AccountAssignments += $AssignmentsResponse.AccountAssignments}
        foreach ($Assignment in $AccountAssignments) {
            if (-not $Principals[$Assignment.PrincipalId]) {
                $AssignmentType = $Assignment.PrincipalType.Value
                $Expression     = "Get-IDS"+$AssignmentType+" @IdsParams -"+
$AssignmentType+"Id "+$Assignment.PrincipalId
                $Principal      = Invoke-Expression $Expression
                if ($Assignment.PrincipalType.Value -eq "GROUP")
 { $Principals[$Assignment.PrincipalId] = $Principal.DisplayName }
                else { $Principals[$Assignment.PrincipalId] = $Principal.UserName }
            }
            $Assignments += [PSCustomObject]@{
                AccountName     = $Account.Name
                PermissionSet   = $PSsets[$PS]
                Principal       = $Principals[$Assignment.PrincipalId]
                Type            = $Assignment.PrincipalType.Value}
        }
    }
}
$Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
Write-Host "`r$($AccountList.Count) accounts done in $Duration. Outputting result to
 $OutputFile"
$Assignments | Sort-Object Account | Export-CSV -Path $OutputFile -Force
```

Überwachen und Korrigieren des geplanten Löschens von AWS KMS-Schlüsseln

Erstellt von Bolsh Khanal (AWS) und Ramya Pulipaka (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Betrieb	AWS-Services: Amazon SNS; AWS CloudTrail; Amazon CloudWatch

Übersicht

In der Amazon Web Services (AWS) Cloud kann das Löschen eines AWS Key Management Services (AWS KMS)-Schlüssels zu Datenverlust führen. Durch das Löschen werden das Schlüsselmaterial und alle mit dem AWS KMS-Schlüssel verknüpften Metadaten entfernt und es kann nicht rückgängig gemacht werden. Nachdem ein AWS KMS-Schlüssel gelöscht wurde, können Sie die unter diesem AWS KMS-Schlüssel verschlüsselten Daten nicht mehr entschlüsseln, sodass Daten nicht wiederhergestellt werden können.

Dieses Muster richtet die Überwachung mit Benachrichtigungen ein, wenn eine Anwendung oder ein Benutzer einen AWS KMS-Schlüssel zum Löschen plant. Wenn Sie eine Benachrichtigung erhalten, können Sie das Löschen des AWS KMS-Schlüssels abbrechen und Ihre Entscheidung, ihn zu löschen, überdenken. Das Muster verwendet das Automatisierungs-Runbook von AWS Systems Manager AWSConfigRemediation–CancelKeyDeletion , um das Abbrechen des Löschens eines AWS KMS-Schlüssels zu erleichtern.

Hinweis: Die CloudFormation Vorlage des Musters muss in allen AWS-Regionen bereitgestellt werden, in denen Sie das Löschen von AWS KMS-Schlüsseln überwachen möchten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Grundlegendes zu den folgenden AWS-Services:
  - Amazon EventBridge
  - AWS KMS

- Amazon Simple Notification Service (Amazon SNS)
- AWS Systems Manager

Einschränkungen

- Jede Anpassung der Lösung erfordert Kenntnisse über AWS- CloudFormation Vorlagen und die in diesem Muster verwendeten AWS-Services.
- Derzeit verwendet diese Lösung den Standard-Event Bus und kann an die Anforderungen angepasst werden. Weitere Informationen zum benutzerdefinierten Event Bus finden Sie in der AWS-Dokumentation.

Architektur

Zieltechnologie-Stack

- Amazon EventBridge
- AWS KMS
- Amazon SNS
- AWS Systems Manager
- Automatisierung mit Folgendem:
  - AWS Command Line Interface (AWS CLI) oder AWS SDK
  - AWS- CloudFormation Stack

Zielarchitektur

1. Das Löschen eines AWS KMS-Schlüssels ist geplant.
2. Das geplante Löschereignis wird durch eine - EventBridge Regel ausgewertet.
3. Die EventBridge Regel aktiviert das Amazon SNS-Thema.
4. Die EventBridge Regel initiiert die Systems Manager-Automatisierung und Runbooks.
5. Die Runbooks brechen den Löschvorgang ab.

Automatisierung und Skalierung

Der CloudFormation Stack stellt alle erforderlichen Ressourcen und Services bereit, damit diese Lösung funktioniert. Das Muster kann unabhängig in einem einzigen Konto oder mit AWS CloudFormation StackSets für mehrere unabhängige Konten oder eine Organisation ausgeführt werden.

```
aws cloudformation create-stack --stack-name  <stack-name>\
    --template-body file://<Full-Path-of-file> \
    --parameters ParameterKey=,ParameterValue= \
    --capabilities CAPABILITY_NAMED_IAM
```

Tools

Tools

- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer Amazon Web Services-Ressourcen unterstützt, sodass Sie weniger Zeit für die Verwaltung dieser Ressourcen aufwenden müssen und sich stattdessen mehr auf Ihre Anwendungen konzentrieren können, die auf AWS ausgeführt werden. Sie können eine CloudFormation Vorlage verwenden, um Stacks in einem AWS-Konto in einer AWS-Region zu erstellen. Die Vorlage beschreibt alle gewünschten AWS-Ressourcen und stellt diese Ressourcen für Sie CloudFormation bereit und konfiguriert sie.
- AWS CLI – Die AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon EventBridge – Amazon EventBridge ist ein Serverless-Event-Bus-Service, der Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbindet. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen und AWS-Services bereit und leitet diese Daten an Ziele wie AWS Lambda weiter. EventBridge vereinfacht den Prozess der Erstellung ereignisgesteuerter Architekturen.
- AWS KMS – AWS Key Management Service (AWS KMS) ist ein verwalteter Service zum Erstellen und Steuern von AWS KMS-Schlüsseln, die zur Verschlüsselung Ihrer Daten verwendet werden.
- AWS SDKs – AWS-Tools enthalten SDKs, mit denen Sie Anwendungen in AWS in der Programmiersprache Ihrer Wahl entwickeln und verwalten können.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten (auch bekannt als Produzenten und Verbraucher) bereitstellt. Herausgeber kommunizieren asynchron mit Abonnenten, indem sie eine Nachricht erstellen und an ein Thema senden, bei dem es sich um einen logischen Zugriffspunkt und Kommunikationskanal handelt.

- AWS Systems Manager – AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur in AWS anzeigen und steuern können. Mit der Systems Manager-Konsole können Sie operative Aufgaben in Ihren gesamten AWS-Ressourcen automatisieren. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem er Ihre verwalteten Instances scannt und über festgestellte Richtlinienverstöße (oder Abhilfemaßnahmen ergreifen) berichtet.

Code

- Die `alerting_ct_logs.yaml` CloudFormation Vorlage für das Projekt ist angehängt.

Polen

Vorbereiten des AWS-Kontos

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie AWS CLI.	Installieren Sie AWS CLI Version 2. Konfigurieren Sie dann die Einstellungen für Sicherheitsanmeldeinformationen für eine Identität, das Standardausgabeformat und die Standard-AWS-Region, die AWS CLI für die Interaktion mit AWS verwendet. Die Identität muss über die erforderlichen Berechtigungen verfügen, um die Aufgaben auszuführen.	Entwickler, Sicherheitsingenieur

Bereitstellen der AWS- CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie den Anhang zu einem lokalen Pfad auf Ihrem Computer herunter und extrahieren Sie die `alerting_ct_logs.yaml` Vorlagendatei.	Entwickler, Sicherheitsingenieur
Stellen Sie die Vorlage bereit.	Führen Sie im Terminalfenster, in dem das AWS-Kontoprofil konfiguriert wurde, den folgenden Befehl aus. `aws cloudformation create-stack --stack-name <stack_name> \ --capabilities <Value> \ --template-body file://<Full_Path> \ --parameters ParameterKey=DestinationEmailAddress,ParameterValue=<Value> \ ParameterKey=SNSTopicName,ParameterValue=<Value> \ ParameterKey=EnableRemediation ,ParameterValue=<Value> \ ParameterKey=AutomationAssumeRole,ParameterValue=<Value>`	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Geben Sie im nächsten Schritt Werte für die Vorlagenp arameter ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Füllen Sie die Vorlagenparameter aus.	Geben Sie die erforderlichen Werte für die Parameter ein. • `DestinationEmailAddress` – Die E-Mail-Adresse, die eine Warnung erhalten soll, wenn ein AWS KMS-Schlüssel zum Löschen geplant ist. • `SNSTopicName` – Der Name des Amazon SNS-Themas. • `EnableRemediation` – Beendigung der geplanten Schlüssellöschung mithilfe eines Systems Manager-Runbooks. Zulässige Werte sind `true` und `false`. • `AutomationAssumeRole` – Der Amazon-Ressourcenname (ARN) der Rolle, die es der Systems Manager-Automatisierung ermöglicht, die Aktionen in Ihrem Namen auszuführen. Weitere Informationen finden Sie im Abschnitt Erforderliche IAM-Berechtigungen in der AWSConfigRemediation-CancelKeyDeletionDokumentation. • `Capabilities` – Damit AWS den Stack erstellen CloudFormation kann,	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	müssen Sie explizit bestätigen, dass Ihre Stack-Vorlage bestimmte Funktionen enthält.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Überprüfen Sie Ihren E-Mail-Posteingang und wählen Sie in der E-Mail-Nachricht, die Sie von Amazon SNS erhalten, Abonnement bestätigen aus. Amazon SNS Ein Webbrowserfenster wird geöffnet und zeigt eine Abonnementbestätigung sowie Ihre Abonnement-ID an.	Entwickler, Sicherheitsingenieur

Zugehörige Ressourcen

Referenzen

- Erstellen einer Regel für einen AWS-Service
- Erstellen eines Amazon- CloudWatch Alarms, um die Verwendung eines AWS KMS-Schlüssels zu erkennen, dessen Löschung aussteht

Tutorials und Videos

- Erste Schritte mit Amazon EventBridge
- Detaillierter Einblick in Amazon EventBridge (AWS Online Tech Talks)

AWS-Workshop

- Arbeiten mit EventBridge Regeln

Zusätzliche Informationen

Der folgende Code enthält Beispiele für die Erweiterung der Lösung zur Überwachung und Benachrichtigung über Änderungen an einem AWS-Service. Die Beispiele umfassen vordefinierte und benutzerdefinierte Muster. Weitere Informationen finden Sie unter Ereignisse und Ereignismuster in EventBridge.

```
EventPattern:
        source:
        - aws.kms
        detail-type:
        - AWS API Call via CloudTrail
        detail:
          eventSource:
          - kms.amazonaws.com
          eventName:
          - ScheduleKeyDeletion
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Identifizieren öffentlicher S3-Buckets in AWS Organizations mithilfe von Security Hub

Erstellt von Mourad Cherfaoui (AWS), Arun Chadapillai (AWS) und Parag Nagwekar (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Speicherung und Sicherung	Workload: Alle anderen Workloads
AWS-Services: Amazon EventBridge; AWS Security Hub; Amazon SNS		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie einen Mechanismus zum Identifizieren öffentlicher Amazon Simple Storage Service (Amazon S3)-Buckets in Ihren AWS Organizations-Konten erstellen. Der Mechanismus funktioniert mithilfe von Kontrollen aus dem AWS Foundational Security Best Practices (FSBP)-Standard in AWS Security Hub zur Überwachung von S3-Buckets. Sie können Amazon verwenden, EventBridge um Security Hub-Ergebnisse zu verarbeiten, und diese Ergebnisse dann in einem Amazon Simple Notification Service (Amazon SNS)-Thema veröffentlichen. Stakeholder in Ihrer Organisation können das Thema abonnieren und sofortige E-Mail-Benachrichtigungen über die Ergebnisse erhalten.

Neue S3-Buckets und ihre Objekte erlauben standardmäßig keinen öffentlichen Zugriff. Sie können dieses Muster in Szenarien verwenden, in denen Sie Standardkonfigurationen von Amazon S3 entsprechend den Anforderungen Ihrer Organisation ändern müssen. Dies könnte beispielsweise ein Szenario sein, in dem Sie einen S3-Bucket haben, der eine öffentlich zugängliche Website hostet, oder Dateien, die jeder im Internet aus Ihrem S3-Bucket lesen kann.

Security Hub wird häufig als zentraler Service bereitgestellt, um alle Sicherheitsergebnisse zu konsolidieren, einschließlich solcher im Zusammenhang mit Sicherheitsstandards und Compliance-Anforderungen. Es gibt andere AWS-Services, die Sie verwenden können, um öffentliche S3-Buckets zu erkennen, aber dieses Muster verwendet eine vorhandene Security Hub-Bereitstellung mit minimaler Konfiguration.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Multi-Konto-Setup mit einem dedizierten Security Hub-Administratorkonto
- Security Hub und AWS Config, aktiviert in der AWS-Region, die Sie überwachen möchten (Hinweis: Sie müssen die regionsübergreifende Aggregation in Security Hub aktivieren, wenn Sie mehrere Regionen aus einer einzigen Aggregationsregion überwachen möchten.)
- Benutzerberechtigungen für den Zugriff auf und die Aktualisierung des Security Hub-Administratorkontos, Lesezugriff auf alle S3-Buckets in der Organisation und Berechtigungen zum Deaktivieren des öffentlichen Zugriffs (falls erforderlich)

Architektur

Technologie-Stack

- AWS Security Hub
- Amazon EventBridge
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Verwendung von Security Hub zur Identifizierung öffentlicher S3-Buckets.

Das Diagramm zeigt den folgenden Workflow:

1. Security Hub überwacht die Konfiguration von S3-Buckets in allen AWS Organizations-Konten (einschließlich des Administratorkontos) mithilfe der S3.2- und S3.3-Steuerelemente aus dem FSBP-Sicherheitsstandard und erkennt ein Ergebnis, wenn ein Bucket als öffentlich konfiguriert ist.
2. Das Security Hub-Administratorkonto greift auf die Ergebnisse (einschließlich der für S3.2 und S3.3) aus allen Mitgliedskonten zu.

3. Security Hub sendet automatisch alle neuen Erkenntnisse und alle Aktualisierungen vorhandener Erkenntnisse an EventBridge als Security Hub Findings – Importierte Ereignisse. Dazu gehören Ereignisse für Erkenntnisse sowohl aus dem Administrator- als auch aus dem Mitgliedskonto.
4. Eine EventBridge Regel filtert nach Ergebnissen aus S3.2 und S3.3`FAILED`, die einen `ComplianceStatus` von `NEW`, einen Workflow-Status von und einen `RecordState` von habenACTIVE.
5. Regeln verwenden die Ereignismuster, um Ereignisse zu identifizieren und sie nach der Übereinstimmung an ein SNS-Thema zu senden.
6. Ein SNS-Thema sendet die Ereignisse an seine Abonnenten (z. B. per E-Mail).
7. Sicherheitsanalysten, die für den Empfang der E-Mail-Benachrichtigungen bestimmt sind, überprüfen den betreffenden S3-Bucket.
8. Wenn der Bucket für den öffentlichen Zugriff genehmigt ist, legt der Sicherheitsanalyst den Workflow-Status der entsprechenden Erkenntnis in Security Hub auf fest`SUPPRESSED`. Andernfalls legt der Analyst den Status auf fest`NOTIFIED`. Dadurch werden zukünftige Benachrichtigungen für den S3-Bucket beseitigt und das Benachrichtigungsrauschen reduziert.
9. Wenn der Workflow-Status auf gesetzt ist`NOTIFIED`, überprüft der Sicherheitsanalyst die Erkenntnis mit dem Bucket-Eigentümer, um festzustellen, ob der öffentliche Zugriff berechtigt ist und den Datenschutzanforderungen entspricht. Die Untersuchung führt dazu, dass entweder der öffentliche Zugriff auf den Bucket entfernt oder der öffentliche Zugriff genehmigt wird. Im letzteren Fall legt der Sicherheitsanalyst den Workflow-Status auf fest`SUPPRESSED`.

Hinweis: Das Architekturdiagramm gilt sowohl für Bereitstellungen zur Aggregation einzelner Regionen als auch für regionsübergreifende Aggregationen. In den Konten A, B und C im Diagramm kann Security Hub zur gleichen Region wie das Administratorkonto oder zu verschiedenen Regionen gehören, wenn die regionsübergreifende Aggregation aktiviert ist.

Tools

AWS-Tools

- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software as a Service (SaaS)-Anwendungen und AWS-Services bereit. EventBridge leitet diese Daten an Ziele wie SNS-Themen und AWS Lambda-Funktionen weiter, wenn die Daten den benutzerdefinierten Regeln entsprechen.

- Amazon Simple Notification Service (Amazon SNS)hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Security Hub hilft Ihnen auch dabei, Ihre AWS-Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen. Security Hub sammelt Sicherheitsdaten aus allen AWS-Konten, Services und unterstützten Partnerprodukten von Drittanbietern und hilft dann bei der Analyse von Sicherheitstrends und der Identifizierung der Sicherheitsprobleme mit der höchsten Priorität.

Polen

Konfigurieren von Security Hub-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Security Hub in AWS Organizations-Konten.	Informationen zum Aktiviere n von Security Hub in den Organisationskonten, in denen Sie S3-Buckets überwache n möchten, finden Sie in den Richtlinien unter Festlegen eines Security Hub-Admin istratorkontos (Konsole) und Verwalten von Mitglieds konten, die zu einer Organisat ion gehören im AWS Security Hub-Benutzerhandbuch.	AWS-Administrator
(Optional) Aktivieren Sie die regionsübergreifende Aggregation.	Wenn Sie S3-Buckets in mehreren Regionen aus einer einzigen Region überwache n möchten, richten Sie	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die regionsübergreifende Aggregation ein.	
Aktivieren Sie die Kontrollen S3.2 und S3.3 für den FSBP-Sicherheitsstandard.	Sie müssen S3.2- und S3.3-Steuerelemente für den FSBP-Sicherheitsstandard aktivieren. 1. Um S3.2-Steuerelemente zu aktivieren, folgen Sie den Anweisungen unter [S3.2] S3-Buckets sollten den öffentlichen Lesezugriff im AWS Security Hub-Benutzerhandbuch verbieten. 2. Um S3.3-Steuerelemente zu aktivieren, folgen Sie den Anweisungen unter [3] S3-Buckets sollten den öffentlichen Schreibzugriff im AWS Security Hub-Benutzerhandbuch verbieten.	AWS-Administrator

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das SNS-Thema und das E-Mail-Abonnement.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon SNS-Konsole. 2. Wählen Sie im Navigationsbereich Topics (Themen)	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Create topic (Thema erstellen). 3. Wählen Sie unter Type (Typ) die Option Standard aus. 4. Geben Sie unter Name einen Namen für Ihr Thema ein (z. B. public-s3-buckets). 5. Wählen Sie Thema erstellen aus. 6. Wählen Sie auf der Registerkarte Abonnements für Ihr Thema die Option Abonnement erstellen aus. 7. Wählen Sie unter Protocol die Option Email aus. 8. Geben Sie für Endpunkt die E-Mail-Adresse ein, die die Benachrichtigungen erhält. Sie können die E-Mail-Adresse eines AWS-Administrators, IT-Experten oder Infosec-Experten verwenden. 9. Wählen Sie Create subscription (Abonnement erstellen) aus. Wiederholen Sie die Schritte 6 bis 8 nach Bedarf, um weitere E-Mail-Abonnements zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die EventBridge Regel.	1. Öffnen Sie die EventBridge -Konsole. 2. Wählen Sie im Abschnitt Erste Schritte EventBrid ge Regel und dann Regel erstellen aus. 3. Geben Sie auf der Detailsei te Regel definieren unter Name einen Namen für Ihre Regel ein (z. B. public-s3-buckets). Wählen Sie Weiter aus. 4. Wählen Sie im Abschnitt Ereignismuster die Option Muster bearbeiten aus. 5. Kopieren Sie den folgenden Code, fügen Sie ihn in den Ereignismuster-Code-Edi tor ein und wählen Sie dann Weiter aus. `{ "source": ["aws.sec urityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Compliance": { "Status": ["FAILED"] }, "RecordState": ["ACTIVE"],`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Workflow": {
	"Status":
	["NEW"]
	},
	"ProductFields":
	{
	"ControlId":
	["S3.2", "S3.3"]
	}
	}
	}
	}</pre>
	Führen Sie dann die folgenden Schritte aus:
	1. Wählen Sie auf der Seite Ziel(e) auswählen für Ziel auswählen ein SNS-Thema als Ziel aus und wählen Sie dann das Thema aus, das Sie zuvor erstellt haben.
	2. Wählen Sie Weiter, erneut Weiter und dann Regel erstellen aus.	

Fehlerbehebung

Problem	Lösung
Ich habe einen S3-Bucket mit aktiviertem öffentlichem Zugriff, erhalte aber keine E-Mail-Benachrichtigungen dafür.	Dies könnte daran liegen, dass der Bucket in einer anderen Region erstellt wurde und die regionsübergreifende Aggregation im Security Hub-Administratorkonto nicht aktiviert ist. Um dieses Problem zu beheben, aktivieren Sie die regionsübergreifende Aggregation oder

Problem	Lösung
	implementieren Sie die Lösung dieses Musters in der Region, in der sich Ihr S3-Bucket derzeit befindet.

Zugehörige Ressourcen

- Was ist AWS Security Hub? (Security Hub-Dokumentation)
- AWS Foundational Security Best Practices (FSBP)-Standard (Security Hub-Dokumentation)
- AWS Security Hub-Skripts für die Aktivierung mehrerer Konten (AWS Labs)
- Bewährte Methoden für die Sicherheit in Amazon S3 (Amazon S3-Dokumentation)

Zusätzliche Informationen

Workflow zur Überwachung öffentlicher S3-Buckets

Der folgende Workflow veranschaulicht, wie Sie die öffentlichen S3-Buckets in Ihrer Organisation überwachen können. Der Workflow geht davon aus, dass Sie die Schritte unter Konfigurieren des SNS-Themas und E-Mail-Abonnements dieses Musters ausgeführt haben.

1. Sie erhalten eine E-Mail-Benachrichtigung, wenn ein S3-Bucket mit öffentlichem Zugriff konfiguriert ist.
   - Wenn der Bucket für den öffentlichen Zugriff genehmigt ist, setzen Sie den Workflow-Status der entsprechenden Erkenntnis `SUPPRESSED` im Security Hub-Administratorkonto auf . Dadurch wird verhindert, dass Security Hub weitere Benachrichtigungen für diesen Bucket ausgibt, und es können doppelte Warnungen vermieden werden.
   - Wenn der Bucket nicht für den öffentlichen Zugriff genehmigt ist, legen Sie den Workflow-Status der entsprechenden Erkenntnis im Security Hub-Administratorkonto auf fest`NOTIFIED`. Dadurch wird verhindert, dass Security Hub weitere Benachrichtigungen für diesen Bucket von Security Hub aus aus aus ausgibt, und es kann Rauschen beseitigen.
2. Wenn der Bucket möglicherweise sensible Daten enthält, deaktivieren Sie den öffentlichen Zugriff sofort, bis die Überprüfung abgeschlossen ist. Wenn Sie den öffentlichen Zugriff deaktivieren, ändert Security Hub den Workflow-Status in `RESOLVED`. Anschließend werden E-Mail-Benachrichtigungen für den Bucket beendet.

3. Suchen Sie den Benutzer, der den Bucket als öffentlich konfiguriert hat (z. B. mithilfe von AWS CloudTrail), und starten Sie eine Überprüfung. Die Überprüfung führt dazu, dass entweder der öffentliche Zugriff auf den Bucket entfernt oder der öffentliche Zugriff genehmigt wird. Wenn der öffentliche Zugriff genehmigt ist, setzen Sie den Workflow-Status der entsprechenden Erkenntnis auf `SUPPRESSED`.

Verwalten von AWS IAM Identity Center-Berechtigungssätzen als Code mithilfe von AWS CodePipeline

Erstellt von Andre Cavalcante (AWS) und Claison Amorim (AWS)

Code-Repository: aws-iam-identity-center-pipeline	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; DevOps
AWS-Services: AWS CodeBuild; AWS CodeCommit; AWS CodePipeline; AWS IAM Identity Center		

Übersicht

AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) hilft Ihnen, den SSO-Zugriff (Single Sign-On) auf alle Ihre AWS-Konten und -Anwendungen zentral zu verwalten. Sie können Benutzeridentitäten in IAM Identity Center erstellen und verwalten oder eine vorhandene Identitätsquelle verbinden, z. B. eine Microsoft Active Directory-Domain oder einen externen Identitätsanbieter (IdP). IAM Identity Center bietet eine einheitliche Verwaltungserfahrung zum Definieren, Anpassen und Zuweisen eines differenzierten Zugriffs auf Ihre AWS-Umgebung mithilfe von Berechtigungssätzen. Berechtigungssätze gelten für die Verbundbenutzer und -gruppen aus Ihrem AWS IAM Identity Center-Identitätsspeicher oder Ihrem externen IdP.

Dieses Muster hilft Ihnen bei der Verwaltung von IAM Identity Center-Berechtigungssätzen als Code in Ihrer Umgebung mit mehreren Konten, die als Organisation in AWS Organizations verwaltet wird. Mit diesem Muster können Sie Folgendes erreichen:

- Erstellen, Löschen und Aktualisieren von Berechtigungssätzen
- Erstellen, aktualisieren oder löschen Sie Berechtigungssatzzuweisungen für AWS-Zielkonten, Organisationseinheiten (OUs) oder Ihr Organisationsstammverzeichnis.

Um IAM Identity Center-Berechtigungen und -Zuweisungen als Code zu verwalten, stellt diese Lösung eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) bereit CodeBuild, die AWS CodeCommit, AWS und AWS verwendet CodePipeline. Sie verwalten die

Berechtigungssätze und Zuweisungen in JSON-Vorlagen, die Sie im CodeCommit Repository speichern. Wenn Amazon- EventBridge Regeln eine Änderung am Repository oder Änderungen an den Konten in der Ziel-OU erkennen, wird eine AWS Lambda-Funktion gestartet. Die Lambda-Funktion initiiert die CI/CD-Pipeline, die die Berechtigungssätze und Zuweisungen im IAM Identity Center aktualisiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Umgebung mit mehreren Konten, die als Organisation in AWS Organizations verwaltet wird. Weitere Informationen finden Sie unter Erstellen einer Organisation.
- IAM Identity Center, aktiviert und mit einer Identitätsquelle konfiguriert. Weitere Informationen finden Sie unter Erste Schritte in der IAM-Identity-Center-Dokumentation.
- Ein Mitgliedskonto, das als delegierter Administrator für IAM Identity Center registriert ist. Anweisungen finden Sie unter Registrieren eines Mitgliedskontos in der IAM-Identity-Center-Dokumentation.
- Berechtigungen zum Bereitstellen von AWS- CloudFormation Stacks im delegierten Administratorkonto von IAM Identity Center und im Verwaltungskonto der Organisation. Weitere Informationen finden Sie unter Zugriffskontrolle in der - CloudFormation Dokumentation.
- Ein Amazon Simple Storage Service (Amazon S3)-Bucket im delegierten Identity Center-Administrator zum Hochladen des Artefaktcodes. Anweisungen finden Sie unter Erstellen eines Buckets.
- Die Konto-ID des Verwaltungskontos der Organisation. Anweisungen finden Sie unter Suchen Ihrer AWS-Konto-ID.

Einschränkungen

- Dieses Muster kann nicht verwendet werden, um Berechtigungssätze für Einzelkontoumgebungen oder für Konten zu verwalten oder zuzuweisen, die nicht als Organisation in AWS Organizations verwaltet werden.
- Berechtigungssatznamen, Zuweisungs-IDs und IAM-Identity-Center-Prinzipaltypen und -IDs können nach der Bereitstellung nicht mehr geändert werden.
- Dieses Muster hilft Ihnen beim Erstellen und Verwalten von benutzerdefinierten Berechtigungen. Sie können dieses Muster nicht verwenden, um vordefinierte Berechtigungen zu verwalten oder zuzuweisen.

- Dieses Muster kann nicht verwendet werden, um einen Berechtigungssatz für das Verwaltungskonto der Organisation zu verwalten.

Architektur

Technologie-Stack

- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- AWS Identity Center
- AWS Lambda
- AWS Organizations

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer nimmt eine der folgenden Änderungen vor:
   a. Überträgt eine oder mehrere Änderungen am CodeCommit Repository
   b. Ändert die Konten in der Organisationseinheit (OU) in AWS Organizations
2. Wenn der Benutzer eine Änderung am CodeCommit Repository vorgenommen hat, erkennt die `CodeChange` EventBridge Regel die Änderung und startet eine Lambda-Funktion im delegierten Administratorkonto von IAM Identity Center. Die Regel reagiert nicht auf Änderungen an bestimmten Dateien im Repository, z. B. der `-README.md`Datei.

   Wenn der Benutzer die Konten in der Organisationseinheit geändert hat, erkennt die `MoveAccount` EventBridge Regel die Änderung und startet eine Lambda-Funktion im Verwaltungskonto der Organisation.
3. Die initiierte Lambda-Funktion startet die CI/CD-Pipeline in CodePipeline.
4. CodePipeline startet das `CodebuildTemplateValidation` CodeBuild Projekt.

5. Das `CodebuildTemplateValidation` CodeBuild Projekt verwendet ein Python-Skript im CodeCommit Repository, um die Berechtigungssatzvorlagen zu validieren. CodeBuild validiert Folgendes:
   - Die Namen der Berechtigungssätze sind eindeutig.
   - Die Zuweisungsanweisungs-IDs (`Sid`) sind eindeutig.
   - Richtliniendefinitionen im `CustomPolicy` Parameter und gültig. (Diese Validierung verwendet AWS Identity and Access Management Access Analyzer.)
   - Die Amazon-Ressourcennamen (ARNs) der verwalteten Richtlinien sind gültig.
6. Das `CodebuildPermissionSet` CodeBuild Projekt verwendet AWS SDK for Python (Boto3), um die Berechtigungssätze in IAM Identity Center zu löschen, zu erstellen oder zu aktualisieren. Nur Berechtigungssätze mit dem `SSOPipeline:true` Tag sind betroffen. Alle Berechtigungssätze, die über diese Pipeline verwaltet werden, haben dieses Tag.
7. Das `CodebuildAssignments` CodeBuild Projekt verwendet Terraform, um die Zuweisungen im IAM Identity Center zu löschen, zu erstellen oder zu aktualisieren. Die Terraform-Backend-Statusdateien werden in einem S3-Bucket im selben Konto gespeichert.
8. CodeBuild übernimmt eine `lookup` IAM-Rolle im Verwaltungskonto der Organisation. Es ruft die Organisationen und Identitystore-APIs auf, um die Ressourcen aufzulisten, die zum Erteilen oder Widerrufen von Berechtigungen erforderlich sind.
9. CodeBuild aktualisiert die Berechtigungssätze und Zuweisungen in IAM Identity Center.

Automatisierung und Skalierung

Da alle neuen Konten in einer Umgebung mit mehreren Konten in eine bestimmte Organisationseinheit in AWS Organizations verschoben werden, wird diese Lösung automatisch ausgeführt und gewährt allen Konten, die Sie in den Zuweisungsvorlagen angeben, die erforderlichen Berechtigungssätze. Es sind keine zusätzlichen Automatisierungen oder Skalierungsaktionen erforderlich.

In großen Umgebungen kann die Anzahl der API-Anforderungen an IAM Identity Center dazu führen, dass diese Lösung langsamer ausgeführt wird. Terraform und Boto3 verwalten automatisch die Drosselung, um Leistungseinbußen zu minimieren.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Einheitentests ausführen und Artefakte erstellen können, die bereitgestellt werden können.
- AWS CodeCommit ist ein Service zur Versionskontrolle, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die erforderlich sind, um Softwareänderungen kontinuierlich zu veröffentlichen.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mit API-Zielen oder Event Buses in anderen AWS-Konten.
- AWS IAM Identity Center hilft Ihnen dabei, den SSO-Zugriff (Single Sign-On) auf alle Ihre AWS-Konten und Cloud-Anwendungen zentral zu verwalten.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS SDK for Python (Boto3) ist ein Software Development Kit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr -Skript in AWS-Services integrieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im aws-iam-identity-center-Pipeline-Repository verfügbar. Der Vorlagenordner im Repository enthält Beispielvorlagen sowohl für Berechtigungssätze als auch für Zuweisungen. Sie enthält auch AWS- CloudFormation Vorlagen für die Bereitstellung der CI/CD-Pipeline und der AWS-Ressourcen in den Zielkonten.

Bewährte Methoden

- Bevor Sie mit dem Ändern des Berechtigungssatzes und der Zuweisungsvorlagen beginnen, empfehlen wir Ihnen, Berechtigungssätze für Ihre Organisation zu planen. Überlegen Sie, was die Berechtigungen sein sollen, für welche Konten oder OUs der Berechtigungssatz gelten soll und

welche IAM-Identity-Center-Prinzipale (Benutzer oder Gruppen) vom Berechtigungssatz betroffen sein sollen. Berechtigungssatznamen, Zuordnungs-IDs und IAM-Identity-Center-Prinzipaltypen und -IDs können nach der Bereitstellung nicht mehr geändert werden.

- Halten Sie sich an das Prinzip der geringsten Berechtigung und erteilen Sie die Mindestberechtigungen, die zum Ausführen einer Aufgabe erforderlich sind. Weitere Informationen finden Sie unter Gewähren von geringsten Berechtigungen und Bewährte Methoden für die Sicherheit in der IAM-Dokumentation.

Sekunden

Planberechtigungssätze und Zuweisungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dies klont das aws-iam-identity-center-Pipeline-Repository von GitHub. `git clone https://github.com/aws-samples/aws-iam-identity-center-pipeline.git`	DevOps Techniker
Definieren Sie die Berechtigungssätze.	1. Navigieren Sie im geklonten Repository zum `templates/permissionsets` Ordner und öffnen Sie dann eine der verfügbaren Vorlagen. 2. Geben Sie im `Name` Parameter einen Namen für den Berechtigungssatz ein. Dieser Wert muss eindeutig sein und kann nach der	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung nicht mehr geändert werden. 3. Beschreiben Sie im `Description` Parameter kurz den Berechtigungssatz, z. B. seinen Anwendungsfall. 4. Geben Sie im `SessionDuration` Parameter die Zeitspanne an, über die ein Benutzer bei einem AWS-Konto angemeldet werden kann. Verwenden Sie das ISO-8601-Dauerformat (Wikipedia), z. B. `PT4H` für 4 Stunden. Wenn kein Wert definiert ist, ist der Standardwert in IAM Identity Center 1 Stunde. 5. Passen Sie die Richtlinien im Berechtigungssatz an. Alle folgenden Parameter sind optional und können nach der Bereitstellung geändert werden. Sie müssen mindestens einen der Parameter verwenden, um die Richtlinien im Berechtigungssatz zu definieren: • Geben Sie im `ManagedPolicies` Parameter die ARNs aller von AWS verwalteten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Richtlinien ein, die Sie zuweisen möchten.
	• Geben Sie im `CustomerManagedPolicies` Parameter die Namen aller vom Kunden verwalteten Richtlinien ein, die Sie zuweisen möchten. Verwenden Sie nicht den ARN.
	• Gehen Sie im `PermissionBoundary` Parameter wie folgt vor, um eine Berechtigungsgrenze zuzuweisen:
	  • Wenn Sie eine von AWS verwaltete Richtlinie als Berechtigungsgrenze verwenden, `PolicyType` geben Sie in ein `AWS` und `Policy` geben Sie in den ARN der Richtlinie ein.
	  • Wenn Sie eine vom Kunden verwaltete Richtlinie als Berechtigungsgrenze verwenden, `PolicyType` geben Sie in ein `Customer` und `Policy` geben Sie in den Namen der Richtlinie ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwenden Sie nicht den ARN. • Definieren Sie im `CustomPolicy` Parameter alle benutzerdefinierten Richtlinien im JSON-Format, die Sie zuweisen möchten. Weitere Informationen zur JSON-Richtlinienstruktur finden Sie unter Übersicht über JSON-Richtlinien. 6. Speichern und schließen Sie die Vorlage für den Berechtigungssatz. Wir empfehlen, die Datei mit einem Namen zu speichern, der dem Namen des Berechtigungssatzes entspricht. 7. Wiederholen Sie diesen Vorgang, um so viele Berechtigungssätze wie nötig für Ihre Organisation zu erstellen, und löschen Sie alle nicht erforderlichen Beispielvorlagen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Zuweisungen.	1. Navigieren Sie im geklonten Repository zum `templates/assignments` Ordner und öffnen Sie dann `iam-identitycenter-assigments.json` . Diese Datei beschreibt, wie Sie die Berechtigungssätze AWS-Konten oder OUs zuweisen möchten. 2. Geben Sie im `SID` Parameter eine Kennung für die Zuweisung ein. Dieser Wert muss eindeutig sein und kann nach der Bereitstellung nicht mehr geändert werden. 3. Definieren Sie im `Target` Parameter die Konten oder Organisationen, auf die Sie den Berechtigungssatz anwenden möchten. Gültige Werte sind Konto-IDs , OU-IDs , OU-Namen oder `root`. `root` weist den Berechtigungssatz allen Mitgliedskonten in der Organisation zu, mit Ausnahme des Verwaltungskontos. Geben Sie die Werte in doppelte Anführungszeichen ein und trennen Sie mehrere Werte	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	durch Kommas. Anweisungen zum Suchen von IDs finden Sie unter Anzeigen von Details eines Kontos oder Anzeigen der Details einer Organisationseinheit. 4. Geben Sie im `PrincipalType` Parameter den Typ des IAM-Identity-Center-Prinzipals ein, der vom Berechtigungssatz betroffen ist. Gültige Werte sind `USER` oder `GROUP`. Dieser Wert kann nach der Bereitstellung nicht mehr geändert werden. 5. Geben Sie im `PrincipalID` Parameter den Namen des Benutzers oder der Gruppe im IAM-Identity-Center-Identitätsspeicher ein, der vom Berechtigungssatz betroffen sein wird. Dieser Wert kann nach der Bereitstellung nicht mehr geändert werden. 6. Geben Sie im `PermissionSetName` Parameter den Namen des Berechtigungssatzes ein, den Sie zuweisen möchten. 7. Wiederholen Sie die Schritte 2 bis 6, um so	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	viele Zuweisungen wie nötig in dieser Datei zu erstellen. In der Regel gibt es eine Zuweisung für jeden Berechtigungssatz. Löschen Sie alle nicht erforderlichen Beispielz uweisungen. 8. Speichern und schließen Sie die Datei `iam-identitycenter-assigments.json` .	

Bereitstellen der Berechtigungssätze und Zuweisungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Dateien in einen S3-Bucket hoch.	1. Komprimieren Sie das geklonte Repository in eine ZIP-Datei. 2. Melden Sie sich beim delegierten Administr atorkonto von IAM Identity Center an. 3. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/. 4. Wählen Sie im linken Navigationsbereich Buckets aus. 5. Wählen Sie den Bucket aus, den Sie für die	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung dieser Lösung verwenden möchten. 6. Laden Sie die ZIP-Datei in den S3-Ziel-Bucket hoch. Eine Anleitung finden Sie unter Hochladen von Objekten.	
Stellen Sie Ressourcen im delegierten Administratorkonto von IAM Identity Center bereit.	1. Öffnen Sie im delegierten Administratorkonto von IAM Identity Center die - CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Stellen Sie die `iam-identitycenter-pipeline.yaml` Vorlage bereit. Geben Sie dem Stack einen eindeutigen und beschreibenden Namen und aktualisieren Sie die Parameter wie angewiesen. Anweisungen finden Sie unter Erstellen eines Stacks in der - CloudFormation Dokumentation.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im AWS Organization-Verwaltungskonto bereit.	1. Melden Sie sich beim Verwaltungskonto der Organisation an. 2. Öffnen Sie die - CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 3. Wählen Sie in der Navigationsleiste den Namen der aktuell angezeigten AWS-Region aus. Wählen Sie dann die `us-east-1` Region aus. Diese Region ist erforderlich, damit die `MoveAccount` EventBridge Regel AWS- CloudTrail Ereignisse erkennen kann, die mit Änderungen der Organisation verbunden sind. 4. Stellen Sie die `iam-identitycenter-organization` Vorlage bereit. Geben Sie dem Stack einen eindeutigen und beschreibenden Namen und aktualisieren Sie die Parameter wie angewiesen. Anweisungen finden Sie unter Erstellen eines Stacks in der - CloudFormation Dokumentation.	DevOps Techniker

Aktualisieren der Berechtigungssätze und Zuweisungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Berechtigungssätze und Zuweisungen.	Wenn die `MoveAccount` Amazon- EventBridge Regel Änderungen an den Konten in der Organisation erkennt, startet die CI/CD-Pipeline automatisch und aktualisiert die Berechtigungssätze. Wenn Sie beispielsweise ein Konto zu einer Organisationseinheit hinzufügen, die in der JSON-Datei für Zuweisungen angegeben ist, wendet die CI/CD-Pipeline den Berechtigungssatz auf das neue Konto an. Wenn Sie die bereitgestellten Berechtigungssätze und Zuweisungen ändern möchten, aktualisieren Sie die JSON-Dateien und übertragen Sie sie dann in das CodeCommit Repository im delegierten Administratorkonto von IAM Identity Center. Anweisungen finden Sie unter Erstellen eines Commit in der - CodeCommit Dokumentation. Beachten Sie Folgendes, wenn Sie die CI/CD-Pipeline verwenden, um zuvor bereitgestellte Berechtig	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ungssätze und Zuordnungen zu verwalten: • Wenn Sie den Namen eines Berechtigungssatze s ändern, löscht die CI/CD-Pipeline den ursprünglichen Berechtigungssatz und erstellt einen neuen. • Diese Pipeline verwaltet nur Berechtigungssätze, die das `-SSOPipeline:true` Tag haben. • Sie können mehrere Berechtigungssatz- und Zuweisungsvorlagen im selben Ordner im Repositor y haben. • Wenn Sie eine Vorlage löschen, löscht die Pipeline den Zuweisungs- oder Berechtigungssatz. • Wenn Sie einen gesamten JSON-Block für die Zuweisung löschen, löscht die Pipeline die Zuweisung aus dem IAM Identity Center. • Sie können keinen Berechtigungssatz löschen, der einem AWS-Konto zugewiesen ist. Zuerst müssen Sie die Zuweisung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Berechtigungssatzes aufheben.	

Fehlerbehebung

Problem	Lösung
Fehler aufgrund einer Zugriffsverweigerung	Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen, um die CloudFormation Vorlagen und die darin definierten Ressourcen bereitzustellen. Weitere Informationen finden Sie unter Zugriffskontrolle in der - CloudFormation Dokumentation.
Pipeline-Fehler in der Validierungsphase	Dieser Fehler wird angezeigt, wenn Fehler im Berechtigungssatz oder in den Zuweisung svorlagen vorliegen. 1. Zeigen Sie CodeBuildin die Build-Details an. 2. Suchen Sie im Build-Protokoll den Validieru ngsfehler, der weitere Informationen darüber enthält, was dazu geführt hat, dass der Build fehlschlägt. 3. Aktualisieren Sie den Berechtigungssatz oder die Zuweisungsvorlagen und übertrage n Sie sie dann in das Repository. 4. Die CI/CD-Pipeline startet das CodeBuild Projekt neu. Überwachen Sie den Status, um zu bestätigen, dass der Validierungsfehler behoben wurde.

Zugehörige Ressourcen

- Berechtigungssätze (Dokumentation zu IAM Identity Center)

Verwalten von Anmeldeinformationen mit AWS Secrets Manager

Erstellt von Durga Prasad Bolepuri (AWS)

Erstellt von: AWS	Umgebung: PoC oder Pilotprojekt	Technologien: Datenbanken; Sicherheit, Identität, Compliance
AWS-Services: AWS Secrets Manager		

Übersicht

Dieses Muster führt Sie durch die Verwendung von AWS Secrets Manager zum dynamischen Abrufen von Datenbankanmeldeinformationen für eine Java Spring-Anwendung.

Wenn Sie eine angepasste Anwendung erstellt haben, die Informationen aus einer Datenbank abruft, mussten Sie bisher normalerweise die Anmeldeinformationen (das Secret) für den Zugriff auf die Datenbank direkt in die Anwendung einbetten. Als es an der Zeit war, die Anmeldeinformationen zu rotieren, mussten Sie Zeit investieren, um die Anwendung zu aktualisieren, um die neuen Anmeldeinformationen zu verwenden, und dann die aktualisierte Anwendung verteilen. Wenn Sie mehrere Anwendungen hätten, die Anmeldeinformationen gemeinsam genutzt haben, und Sie eine von ihnen nicht aktualisiert haben, schlägt die Anwendung fehl. Aufgrund dieses Risikos haben sich viele Benutzer dafür entschieden, ihre Anmeldeinformationen nicht regelmäßig zu rotieren, wodurch effektiv ein Risiko durch ein anderes ersetzt wurde.

Mit Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code (einschließlich Passwörtern) durch einen API-Aufruf ersetzen, um das Secret programmgesteuert abzurufen. Dadurch wird sichergestellt, dass das Secret nicht von jemandem kompromittiert werden kann, der Ihren Code untersucht, da das Secret einfach nicht vorhanden ist. Sie können Secrets Manager auch so konfigurieren, dass das Secret automatisch nach einem von Ihnen angegebenen Zeitplan rotiert wird. Auf diese Weise können Sie langfristige Geheimnisse durch kurzfristige ersetzen, wodurch das Risiko einer Kompromittierung erheblich reduziert wird. Weitere Informationen finden Sie in der AWS Secrets Manager-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto mit Zugriff auf Secrets Manager
- Eine Java Spring-Anwendung

Architektur

Quelltechnologie-Stack

- Eine Java Spring-Anwendung mit Code, der auf eine Datenbank zugreift, wobei die DB-Anmeldeinformationen von der Datei application.properties verwaltet werden.

Zieltechnologie-Stack

- Eine Java Spring-Anwendung mit Code, der auf eine Datenbank zugreift, wobei die DB-Anmeldeinformationen in Secrets Manager verwaltet werden. Die Datei application.properties enthält die Secrets für Secrets Manager.

Integration von Secrets Manager mit einer Anwendung

Tools

- Secrets Manager – AWS Secrets Manager ist ein AWS-Service, der Ihnen die Verwaltung von Secrets erleichtert. Bei den Secrets kann es sich um Datenbank-Anmeldeinformationen, Passwörter, API-Schlüssel von Drittanbietern und sogar beliebigen Text handeln. Sie können den Zugriff auf diese Secrets zentral speichern und steuern, indem Sie die Secrets-Manager-Konsole, die Secrets-Manager-Befehlszeilenschnittstelle (CLI) oder die Secrets-Manager-API und SDKs verwenden.

Polen

Speichern von Secrets in Secrets Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die DB-Anmeld einformationen als Secret in Secrets Manager.	Speichern Sie Amazon Relational Database Service (Amazon RDS) oder andere DB-Anmeldeinformationen als Secret in Secrets Manager, indem Sie die Schritte unter Erstellen eines Secrets in der Secrets-Manager-Dokumentati on ausführen.	Sys-Admin
Legen Sie Berechtigungen für die Spring-Anwendung fest, um auf Secrets Manager zuzugreifen.	Legen Sie die entsprechenden Berechtigungen basierend darauf fest, wie die Java Spring-Anwendung Secrets Manager verwendet. Um den Zugriff auf das Secret zu steuern, erstellen Sie eine Richtlinie basierend auf den Informationen in der Secrets-Manager-Do kumentation in den Abschnitt en Verwenden von identität sbasierten Richtlinien (IAM-Richtlinien) und ABAC für Secrets Manager und Verwenden von ressource nbasierten Richtlinien für Secrets Manager . Befolgen Sie die Schritte im Abschnitt Abrufen des Secret-Werts	Sys-Admin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der Secrets-Manager-Do kumentation.	

Aktualisieren der Spring-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie JAR-Abhän gigkeiten hinzu, um Secrets Manager zu verwenden.	Einzelheiten finden Sie im Abschnitt Zusätzliche Informati onen.	Java-Entwickler
Fügen Sie die Details des Secrets zur Spring-An wendung hinzu.	Aktualisieren Sie die Datei application.properties mit dem Secret-Namen, den Endpunkten und der AWS-Region. Ein Beispiel finden Sie im Abschnitt Zusätzliche Informationen.	Java-Entwickler
Aktualisieren Sie den Abrufcode für DB-Anmeld einformationen in Java.	Aktualisieren Sie in der Anwendung den Java-Code, der die DB-Anmeldeinformat ionen abruft, um diese Details von Secrets Manager abzurufen. Beispielcode finden Sie im Abschnitt Zusätzliche Informationen.	Java-Entwickler

Zugehörige Ressourcen

- AWS Secrets Manager-Dokumentation
- Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) und ABAC für Secrets Manager
- Verwenden von ressourcenbasierten Richtlinien für Secrets Manager
- Beispielcode

Zusätzliche Informationen

Hinzufügen von JAR-Abhängigkeiten für die Verwendung von Secrets Manager

Maven:

```
<groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-secretsmanager</artifactId>
    <version>1.11. 355 </version>
```

Gradle:

```
compile group: 'com.amazonaws', name: 'aws-java-sdk-secretsmanager', version:
 '1.11.355'
```

Aktualisieren der Datei application.properties mit den Details des Secrets

```
spring.aws.secretsmanager.secretName=postgres-local
spring.aws.secretsmanager.endpoint=secretsmanager.us-east-1.amazonaws.com
spring.aws.secretsmanager.region=us-east-1
```

Aktualisieren des DB-Anmeldeinformationsabrufcodes in Java

```
String  secretName  =  env.getProperty("spring.aws.secretsmanager.secretName");
String  endpoints  =  env.getProperty("spring.aws.secretsmanager.endpoint");
String  AWS Region  =  env.getProperty("spring.aws.secretsmanager.region");
AwsClientBuilder.EndpointConfiguration  config  =  new
  AwsClientBuilder.EndpointConfiguration(endpoints, AWS Region);
AWSSecretsManagerClientBuilder  clientBuilder  =
  AWSSecretsManagerClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AWSSecretsManager  client  =  clientBuilder.build();

ObjectMapper  objectMapper  =  new  ObjectMapper();

JsonNode  secretsJson  =  null;

ByteBuffer  binarySecretData;

GetSecretValueRequest  getSecretValueRequest  =  new
  GetSecretValueRequest().withSecretId(secretName);
```

```
GetSecretValueResult  getSecretValueResponse  =  null;

try  {
     getSecretValueResponse  =  client.getSecretValue(getSecretValueRequest);
    }

catch  (ResourceNotFoundException  e)  {
     log.error("The requested secret "  +  secretName  +  " was not found");
    }

catch  (InvalidRequestException  e)  {
     log.error("The request was invalid due to: "  +  e.getMessage());
     }

catch  (InvalidParameterException  e)  {
     log.error("The request had invalid params: "  +  e.getMessage());
     }
if  (getSecretValueResponse  ==  null)  {
     return  null;
     }  // Decrypted secret using the associated KMS key // Depending on whether the
 secret was a string or binary, one of these fields will be populated


String secret = getSecretValueResponse.getSecretString();

if (secret != null) {
     try {
                secretsJson  =  objectMapper.readTree(secret);
          }

     catch  (IOException  e)  {
                log.error("Exception while retrieving secret values: "  +
  e.getMessage());
          }
}

else  {
     log.error("The Secret String returned is null");

     return null;

     }
     String  host  =  secretsJson.get("host").textValue();
```

```
    String  port  =  secretsJson.get("port").textValue();
    String  dbname  =  secretsJson.get("dbname").textValue();
    String  username  =  secretsJson.get("username").textValue();
    String  password  =  secretsJson.get("password").textValue();
}
```

Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung

Umgebung: Produktion	Technologien: Analytik; Große Datenmengen; Cloud-nativ; Sicherheit, Identität, Compliance	Arbeitslast: Open Source
AWS-Dienste: Amazon EMR; Amazon SNS; AWS CloudTrail; Amazon CloudWatch		

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die Amazon EMR-Cluster beim Start überwacht und eine Warnung sendet, wenn die Verschlüsselung während der Übertragung nicht aktiviert wurde.

Amazon EMR ist ein Webservice, mit dem Sie auf einfache Weise Big-Data-Frameworks wie Apache Hadoop ausführen können, um Daten zu verarbeiten und zu analysieren. Amazon EMR ermöglicht es Ihnen, riesige Datenmengen auf kostengünstige Weise zu verarbeiten, indem Sie Mapping- und Reduction-Schritte parallel ausführen.

Die Datenverschlüsselung verhindert, dass unbefugte Benutzer auf Daten im Ruhezustand oder Daten während der Übertragung zugreifen oder diese lesen. Daten im Ruhezustand beziehen sich auf Daten, die auf Medien wie einem lokalen Dateisystem auf jedem Knoten, Hadoop Distributed File System (HDFS) oder dem EMR File System (EMRFS) über Amazon Simple Storage Service (Amazon S3) gespeichert sind. Bei der Übertragung von Daten handelt es sich um Daten, die über das Netzwerk übertragen werden und zwischen Aufträgen übertragen werden. Die Verschlüsselung während der Übertragung unterstützt Open-Source-Verschlüsselungsfunktionen für Apache Spark, Apache TEZ, Apache Hadoop, Apache HBase und Presto. Sie aktivieren die Verschlüsselung, indem Sie über die AWS-Befehlszeilenschnittstelle (AWS CLI), die Konsole oder die AWS-SDKs eine Sicherheitskonfiguration erstellen und die Datenverschlüsselungseinstellungen angeben. Sie können die Verschlüsselungsartefakte für die Verschlüsselung während der Übertragung auf zwei Arten bereitstellen:

- Durch Hochladen einer komprimierten Zertifikatsdatei auf Amazon S3.

- Durch Verweisen auf eine benutzerdefinierte Java-Klasse, die Verschlüsselungsartefakte bereitstellt.

Die in diesem Muster enthaltene Sicherheitskontrolle überwacht API-Aufrufe und generiert ein Amazon CloudWatch Events-Ereignis für die RunJobFlow-Aktion. Das Ereignis ruft eine AWS-Lambda-Funktion auf, die ein Python-Skript ausführt. Die Funktion ruft die EMR-Cluster-ID aus der JSON-Eingabe des Ereignisses ab und führt die folgenden Prüfungen durch, um festzustellen, ob eine Sicherheitsverletzung vorliegt:

- Überprüft, ob der EMR-Cluster über eine Amazon EMR-spezifische Sicherheitskonfiguration verfügt.
- Wenn der Cluster über eine Sicherheitskonfiguration verfügt, wird geprüft, ob die Verschlüsselung bei der Übertragung aktiviert ist.
- Wenn der Cluster nicht über eine Sicherheitskonfiguration verfügt, sendet er mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Warnung an eine von Ihnen angegebene E-Mail-Adresse. In der Benachrichtigung werden der EMR-Clustername, Einzelheiten zum Verstoß, AWS-Regions- und Kontoinformationen sowie der AWS-Lambda-ARN (Amazon-Ressourcenname) angegeben, von dem die Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Bucket zum Hochladen des Lambda-Codes, der mit diesem Muster bereitgestellt wird.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- Amazon EMR-Protokollierung aktiviert, für den Zugriff auf alle API-Protokolle.

Einschränkungen

- Diese Detective Control ist regional und muss in jeder AWS-Region eingesetzt werden, die Sie überwachen möchten.

Produktversionen

- Amazon EMR Version 4.8.0 oder höher.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um die Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- Amazon EMR — Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks wie Apache Hadoop und Apache Spark auf AWS vereinfacht, um riesige Datenmengen zu verarbeiten und zu analysieren. Mithilfe dieser Frameworks und verwandter Open-Source-Projekte können Sie Daten für Analysezwecke und Business Intelligence-Workloads verarbeiten. Darüber hinaus können Sie Amazon EMR verwenden, um große Datenmengen in und aus anderen AWS-Datenspeichern und Datenbanken wie Amazon S3 und Amazon DynamoDB zu transformieren und zu verschieben.
- AWS Cloudformation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.
- AWS Cloudwatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten, und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch von wenigen Anfragen pro Tag auf Tausende pro Sekunde. Sie bezahlen nur

für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.

- AWS SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `EMRInTransitEncryption.zip`ist eine komprimierte Datei, die die Sicherheitskontrolle (Lambda-Code) enthält.
- `EMRInTransitEncryption.yml`ist eine CloudFormation Vorlage, die die Sicherheitskontrolle bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `EMRInTransitEncryption.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die Ressourcen, die Sie bewerten möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `EMRInTransitEncryption.yml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt,

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die Ressource, die ausgewertet werden.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket ohne führende Schrägstriche an (z. B. `EMRInTransitEncryption.zip` oder).	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`controls/EMRInTransitEncryption.zip`	
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, an die Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokollierungsebene an.	Geben Sie die Protokollierungsebene und die Ausführlichkeit für die Lambda-Protokolle an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachric	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	htigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Verschlüsselungsoptionen (Amazon EMR-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen Sie ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Datenbanken; Infrastruktur; Cloud-nativ	Arbeitslast: Open Source
AWS-Dienste: Amazon SNS; Amazon CloudWatch; Amazon ElastiCache		

Übersicht

Amazon ElastiCache ist ein Service von Amazon Web Services (AWS), der eine leistungsstarke, skalierbare und kostengünstige Caching-Lösung für die Verteilung eines In-Memory-Datenspeichers oder einer Cache-Umgebung in der Cloud bietet. Er ruft Daten aus In-Memory-Datenspeichern mit hohem Durchsatz und niedriger Latenz ab. Diese Funktionalität macht sie zu einer beliebten Wahl für Echtzeit-Anwendungsfälle wie Caching, Sitzungsspeicher, Spiele, Geodatendienste, Echtzeitanalysen und Warteschlangen. ElastiCache bietet Redis- und Memcached-Datenspeicher, die beide Reaktionszeiten unter einer Millisekunde bieten.

Datenverschlüsselung verhindert, dass unbefugte Benutzer sensible Daten lesen, die auf Ihren Redis-Clustern und den zugehörigen Cache-Speichersystemen verfügbar sind. Dazu gehören Daten, die auf persistenten Medien gespeichert sind (sogenannte Data at Rest), und Daten, die auf ihrem Weg durch das Netzwerk zwischen Clients und Cache-Servern abgefangen werden können (sogenannte Daten während der Übertragung).

Sie können die Verschlüsselung im Ruhezustand ElastiCache für Redis aktivieren, wenn Sie eine Replikationsgruppe erstellen, indem Sie den AtRestEncryptionEnabledParameter auf true setzen. Wenn dieser Parameter aktiviert ist, verschlüsselt er die Festplatte bei Synchronisierungs-, Sicherungs- und Swap-Vorgängen und verschlüsselt Backups, die in Amazon Simple Storage Service (Amazon S3) gespeichert sind. Sie können die Verschlüsselung im Ruhezustand nicht für eine bestehende Replikationsgruppe aktivieren. Wenn Sie eine Replikationsgruppe erstellen, können Sie die Verschlüsselung im Ruhezustand auf folgende zwei Arten aktivieren:

- Indem Sie die Standardoption wählen, bei der vom Service verwaltete Verschlüsselung im Ruhezustand verwendet wird.
- Indem Sie einen vom Kunden verwalteten Schlüssel verwenden und die Schlüssel-ID oder den Amazon-Ressourcennamen (ARN) von AWS Key Management Service (AWS KMS) angeben.

Dieses Muster bietet eine Sicherheitskontrolle, die API-Aufrufe überwacht und ein Amazon CloudWatch Events-Ereignis für den CreateReplicationGruppenvorgang generiert. Dieses Ereignis ruft eine AWS-Lambda-Funktion auf, die ein Python-Skript ausführt. Die Funktion ruft die Replikationsgruppen-ID aus der JSON-Eingabe des Ereignisses ab und führt die folgenden Prüfungen durch, um festzustellen, ob eine Sicherheitsverletzung vorliegt:

- Prüft, ob der AtRestEncryptionEnabledSchlüssel existiert.
- Falls AtRestEncryptionEnabledvorhanden, wird der Wert überprüft, um festzustellen, ob er wahr ist.
- Wenn der AtRestEncryptionEnabledWert auf False gesetzt ist, wird eine Variable festgelegt, die Verstöße verfolgt und mithilfe einer Amazon Simple Notification Service (Amazon SNS) - Benachrichtigung eine Verstoßmeldung an eine von Ihnen angegebene E-Mail-Adresse sendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Bucket zum Hochladen des bereitgestellten Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- ElastiCache Protokollierung aktiviert, für den Zugriff auf alle API-Protokolle.

Einschränkungen

- Diese Detective Control ist regional und muss in jeder AWS-Region eingesetzt werden, die Sie überwachen möchten.
- Das Steuerelement unterstützt Replikationsgruppen, die in einer Virtual Private Cloud (VPC) ausgeführt werden.
- Das Steuerelement unterstützt Replikationsgruppen, auf denen die folgenden Knotentypen ausgeführt werden:
  - R5, R4, R3

- M5, M4, M3
- T3, T2

Produktversionen

- ElastiCache für Redis Version 3.2.6 oder höher

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- Amazon ElastiCache — Amazon ElastiCache macht es einfach, verteilte In-Memory-Cache-Umgebungen in der AWS-Cloud einzurichten, zu verwalten und zu skalieren. Es bietet einen leistungsstarken, in der Größe anpassbaren und kostengünstigen In-Memory-Cache und verringert gleichzeitig die Komplexität, die mit der Bereitstellung und Verwaltung einer verteilten Cache-Umgebung verbunden ist. ElastiCache funktioniert sowohl mit der Redis- als auch mit der Memcached-Engine.
- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.
- AWS Cloudwatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten, und ergreift bei

Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.

- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch von wenigen Anfragen pro Tag auf Tausende pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `ElasticCache-EncryptionAtRest.zip`ist eine komprimierte Datei, die die Sicherheitskontrolle (Lambda-Code) enthält.
- `elasticache_encryption_at_rest.yml`ist eine CloudFormation Vorlage, die die Sicherheitskontrolle bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `ElastiCache-EncryptionAtRest.zip` Datei hochzuladen (Lambda-C	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ode). Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen, die Sie bewerten möchten.	
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `elasticache_encryption_at_rest.yml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die Ressource, die ausgewertet werden.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an,	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ohne vorangestellte Schrägstriche (z. B. `ElasticCache-EncryptionAtRest.zip` oder). `controls/ElasticCache-EncryptionAtRest.zip`	
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokollierungsebene an.	Geben Sie die Protokollierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Verschlüsselung im Ruhezustand ElastiCache für Redis (ElastiCache Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen Sie EC2-Instance-Schlüsselpaare mit AWS Config

Umwelt: Produktion	Technologien: Sicherheit, Identität, Compliance	AWS-Dienste: Amazon SNS; AWS Config; AWS Lambda

Übersicht

Beim Starten einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in der Amazon Web Services (AWS) -Cloud empfiehlt es sich, ein vorhandenes key pair zu erstellen oder zu verwenden, um eine Verbindung mit der Instance herzustellen. Das key pair, das aus einem in der Instanz gespeicherten öffentlichen Schlüssel und einem privaten Schlüssel besteht, der dem Benutzer zur Verfügung gestellt wird, ermöglicht den sicheren Zugriff über Secure Shell (SSH) auf die Instanz und vermeidet die Verwendung von Passwörtern. Manchmal können Benutzer jedoch versehentlich Instances starten, ohne ein key pair anzuhängen. Da Schlüsselpaare nur beim Start einer Instance zugewiesen werden können, ist es wichtig, Instances, die ohne Schlüsselpaare gestartet wurden, schnell zu identifizieren und als nicht konform zu kennzeichnen. Dies ist besonders nützlich, wenn Sie in Konten oder Umgebungen arbeiten, die die Verwendung von Schlüsselpaaren für den Instanzzugriff vorschreiben.

Dieses Muster beschreibt, wie Sie in AWS Config eine benutzerdefinierte Regel zur Überwachung von EC2-Instance-Schlüsselpaaren erstellen. Wenn Instances als nicht konform identifiziert werden, wird eine Warnung mithilfe von Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungen gesendet, die durch ein EventBridge Amazon-Ereignis ausgelöst wurden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Config ist für die AWS-Region aktiviert, die Sie überwachen möchten, und ist so konfiguriert, dass alle AWS-Ressourcen aufgezeichnet werden

Einschränkungen

- Diese Lösung ist regionsspezifisch. Alle Ressourcen sollten in derselben AWS-Region erstellt werden.

Architektur

Zieltechnologie-Stack

- AWS Config
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Zielarchitektur

1. AWS Config initiiert die Regel.
2. Die Regel ruft die Lambda-Funktion auf, um die Konformität von EC2-Instances zu bewerten.
3. Die Lambda-Funktion sendet den aktualisierten Konformitätsstatus an AWS Config.
4. AWS Config sendet ein Ereignis an EventBridge.
5. EventBridge veröffentlicht Benachrichtigungen über Compliance-Änderungen zu einem SNS-Thema.
6. Amazon SNS sendet eine Warnung per E-Mail.

Automatisierung und Skalierung

Die Lösung kann eine beliebige Anzahl von EC2-Instanzen innerhalb einer Region überwachen.

Tools

Tools

- AWS Config — AWS Config ist ein Service, mit dem Sie die Konfigurationen Ihrer AWS-Ressourcen bewerten, prüfen und bewerten können. AWS Config überwacht und zeichnet Ihre AWS-Ressourcenkonfigurationen kontinuierlich auf und ermöglicht Ihnen, die Auswertung aufgezeichneter Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren.
- Amazon EventBridge — Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können.

- AWS Lambda — AWS Lambda ist ein serverloser Rechenservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern, die Erstellung einer auslastungsorientierten Cluster-Skalierungslogik, die Verwaltung von Eventintegrationen oder die Verwaltung von Laufzeiten unterstützt.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein vollständig verwalteter Messaging-Dienst sowohl für application-to-application (A2A) als auch für (A2P application-to-person) Kommunikation.

Code

Der Code für die Lambda-Funktion ist angehängt.

Epen

Erstellen Sie eine Lambda-Funktion zur Bewertung der Amazon EC2 EC2-Konformität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Identity and Access Management (IAM) -Rolle für Lambda.	Wählen Sie in der AWS-Managementkonsole IAM und erstellen Sie dann die Rolle. Verwenden Sie Lambda als vertrauenswürdige Entität und fügen Sie die `AmazonEventBridgeFullAccess` Berechtigungen und hinzu. `AWSConfigRulesExecutionRole` Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps
Erstellen und implementieren Sie die Lambda-Funktion.	1. Erstellen Sie auf der Lambda-Konsole mithilfe von Author von Grund auf eine Funktion mit Python 3.6 als Laufzeit und der zuvor erstellten IAM-Rolle.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Notieren Sie den Amazon-Ressourcennamen (ARN). 2. Wählen Sie auf der Registerkarte Code den Code aus`lambda_function.py`, der an dieses Muster angehängt ist, und fügen Sie ihn ein. 3. Um Ihre Änderungen zu speichern, wählen Sie Bereitstellen.	

Erstellen Sie eine benutzerdefinierte AWS Config-Regel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine benutzerdefinierte AWS Config-Regel hinzu.	Fügen Sie in der AWS Config-Konsole eine benutzerdefinierte Regel mit den folgenden Einstellungen hinzu: • ARN — Der ARN der zuvor erstellten Lambda-Funktion • Triggertyp — Konfigurationsänderungen • Umfang der Änderungen — Ressourcen • Ressourcentyp — Amazon EC2 EC2-Instance Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps

Konfigurieren Sie E-Mail-Benachrichtigungen, wenn ein Compliance-Änderungsereignis erkannt wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SNS-Thema und das Abonnement.	Erstellen Sie in der Amazon SNS SNS-Konsole ein Thema mit dem Typ Standard und anschließend ein Abonnement mit E-Mail als Protokoll. Wenn Sie die Bestätigungs-E-Mail erhalten, wählen Sie den Link zur Bestätigung des Abonnements. Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps
Erstellen Sie eine EventBridge Regel, um Amazon SNS SNS-Benachrichtigungen zu initiieren.	Erstellen Sie auf der EventBridge Konsole eine Regel mit den folgenden Einstellungen: • Dienstname — AWS Config • Ereignistyp — Änderung der Konformität der Konfigurationsregeln • Nachrichtentyp — Spezifische Nachrichtentypen, ComplianceChangeNotification • Spezifischer Regelname — Der Name Ihrer zuvor erstellten AWS Config-Regel • Ziel — SNS-Thema, Ihr zuvor erstelltes Thema	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der AWS-Dokumentation.	

Überprüfen Sie die Regel und die Benachrichtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie EC2-Instanzen.	Erstellen Sie zwei EC2-Instances eines beliebigen Typs und fügen Sie ein key pair hinzu, und erstellen Sie eine EC2-Instance ohne key pair.	DevOps
Überprüfen Sie die Regel.	1. Wählen Sie in der AWS Config-Konsole auf der Seite Regeln Ihre Regel aus. 2. Um konforme und nicht konforme EC2-Instances zu sehen, ändern Sie Ressourcen im Geltungsbereich auf Alle. Stellen Sie sicher, dass zwei Instances als konform und eine Instance als nicht konform aufgeführt sind. 3. Warten Sie, bis Sie eine E-Mail-Benachrichtigung von Amazon SNS über den Compliance-Status der EC2-Instances erhalten.	DevOps

Zugehörige Ressourcen

- Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service
- Erstellen einer benutzerdefinierten Regel in AWS Config
- Ein Amazon SNS SNS-Thema erstellen
- Ein Amazon SNS SNS-Thema abonnieren
- Eine Regel in Amazon erstellen EventBridge

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen von ElastiCache Clustern für Sicherheitsgruppen

Erstellt von Susanne Kangnoh (AWS) und Archit Mat microSD (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Datenbanken; Infrastruktur; Cloudnativ	AWS-Services: Amazon SNS ; AWS CloudTrail; Amazon CloudWatch; Amazon ElastiCache

Übersicht

Amazon ElastiCache ist ein Amazon Web Services (AWS)-Service, der eine leistungsstarke, skalierbare und kostengünstige Caching-Lösung für die Verteilung eines In-Memory-Datenspeichers oder einer Cache-Umgebung in der Cloud bietet. Es ruft Daten aus In-Memory-Datenspeichern mit hohem Durchsatz und geringer Latenz ab. Diese Funktionalität macht sie zu einer beliebten Wahl für Echtzeit-Anwendungsfälle wie Caching, Sitzungsspeicher, Spiele, Geodatendienste, Echtzeitanalysen und queuing. ElastiCache offers Redis- und Memcached-Datenspeicher, die beide Reaktionszeiten von unter einer Millisekunde bieten.

Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre ElastiCache Instances, indem sie den ein- und ausgehenden Datenverkehr steuert. Sicherheitsgruppen fungieren auf Instance-Ebene, nicht auf Subnetzebene. Für jede Sicherheitsgruppe fügen Sie einen Regelsatz hinzu, der den eingehenden Datenverkehr zu Instances steuert, und einen separaten Regelsatz, der den ausgehenden Datenverkehr steuert. Sie können Zulassungsregeln angeben, aber keine Ablehnungsregeln.

Dieses Muster bietet eine Sicherheitskontrolle, die auf API-Aufrufe überwacht und ein Amazon CloudWatch Events-Ereignis für die ModifyReplicationGroup Operationen CreateReplicationGroup, CreateCacheClusterModifyCacheCluster, und generiert. Dieses Ereignis ruft eine AWS Lambda-Funktion auf, die ein Python-Skript ausführt. Die Funktion ruft die Replikationsgruppen-ID aus der Ereignis-JSON-Eingabe ab und führt die folgenden Prüfungen durch, um festzustellen, ob ein Sicherheitsverstoß vorliegt:

- Prüft, ob die Sicherheitsgruppe des Clusters mit der Sicherheitsgruppe übereinstimmt, die in der Lambda-Funktion konfiguriert ist.

- Wenn die Sicherheitsgruppe des Clusters nicht übereinstimmt, sendet die Funktion mithilfe einer Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung eine Verletzungsmeldung an eine von Ihnen angegebene E-Mail-Adresse.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Bucket zum Hochladen des bereitgestellten Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- ElastiCache -Protokollierung aktiviert, für den Zugriff auf alle API-Protokolle.

Einschränkungen

- Diese detektivische Kontrolle ist regional und muss in jeder AWS-Region bereitgestellt werden, die Sie überwachen möchten.
- Die Kontrolle unterstützt Replikationsgruppen, die in einer Virtual Private Cloud (VPC) ausgeführt werden.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- Amazon ElastiCache erleichtert das Einrichten, Verwalten und Skalieren verteilter In-Memory-Cache-Umgebungen in der AWS Cloud. Es bietet eine hohe Leistung, anpassbare und

kostengünstige In-Memory-Cache, ohne die mit der Bereitstellung und Verwaltung einer verteilten Cache-Umgebung verbundene Komplexität. ElastiCache funktioniert sowohl mit den Redis- als auch mit den Memcached-Engines.

- AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.
- AWS Cloudwatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt. CloudWatch Ereignisse erkennen betriebliche Änderungen, sobald sie auftreten, und ergreifen bei Bedarf Korrekturmaßnahmen, indem sie Nachrichten senden, um an die Umgebung zu reagieren, Funktionen zu aktivieren, Änderungen vorzunehmen und Zustandsinformationen zu erfassen.
- AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch von einigen Anfragen pro Tag auf Tausende pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet das Senden von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster enthält eine Anfügung mit zwei Dateien:

- `ElastiCacheAllowedSecurityGroup.zip` ist eine komprimierte Datei, die den Lambda-Code (Security Control) enthält.
- `ElastiCacheAllowedSecurityGroup.yml` ist eine CloudFormation Vorlage, die die Sicherheitskontrolle bereitstellt.

Weitere Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Ices.

Polen

Bereitstellen der Sicherheitskontrolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `ElastiCacheAllowedSecurityGroup.zip` Datei (Lambda-Code) hochzuladen. Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen, die Sie auswerten möchten.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `ElastiCacheAllowedSecurityControl.yml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt

Schließen Sie die Parameter in der CloudFormation Vorlage ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen des S3-Buckets an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epos erstellt	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region wie die CloudFormation Vorlage und die Ressource befinden, die ausgewertet werden soll.	
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket ohne voranstehende Schrägstriche an (z. B. `ElasticCacheAllowedSecurityGroup.zip` oder `controls/ElasticCacheAllowedSecurityGroup.zip`).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, an die Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie eine Protokoll ierungsebene an.	Geben Sie die Protokoll ierungsebene und die Ausführlichkeit an. `Info` bezeichnet detaillierte Informationsmeldun gen zum Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichne t Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. `Warning` bezeichnet potenziell schädliche Situation en.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Ab onnement.	Wenn die CloudFormation Vorlage erfolgreich bereitges tellt wird, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachric htigungen zu erhalten, müssen Sie dieses E-Mail-Ab onnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines Stacks in der AWS- CloudFormation Konsole (AWS- CloudFormation Dokumentation)
- Amazon VPCs und ElastiCache Sicherheit (Dokumentation zu Amazon ElastiCache for Redis)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

IAM-Root-Benutzeraktivitäten überwachen

Erstellt von Mostefa Brougui (AWS)

Code-Repository: aws-iam-root-user-activity-monitor	Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Management und Governance
Workload: Alle anderen Workloads	AWS-Services: Amazon EventBridge; AWS Lambda ; Amazon SNS ; AWS Identity and Access Management	

Übersicht

Jedes Amazon Web Services (AWS)-Konto hat einen Root-Benutzer. Als bewährte Sicherheitsmethode für AWS Identity and Access Management (IAM) empfehlen wir, den Root-Benutzer zu verwenden, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im AWS-Kontoverwaltungsreferenzhandbuch. Da der Root-Benutzer vollen Zugriff auf alle Ihre AWS-Ressourcen und Fakturierungsdaten hat, empfehlen wir, dieses Konto nicht zu verwenden und es auf Aktivitäten zu überwachen, die darauf hindeuten könnten, dass die Anmeldeinformationen des Root-Benutzers kompromittiert wurden.

Mit diesem Muster richten Sie eine ereignisgesteuerte Architektur ein, die den IAM-Root-Benutzer überwacht. Dieses Muster richtet eine hub-and-spoke Lösung ein, die mehrere AWS-Konten, die Spoke-Konten, überwacht und die Verwaltung und Berichterstattung in einem einzigen Konto, dem Hub-Konto, zentralisiert.

Wenn die Anmeldeinformationen des IAM-Stammbenutzers verwendet werden, CloudTrail zeichnet Amazon CloudWatch und AWS die Aktivität im Protokoll bzw. im Trail auf. Im Spoke-Konto sendet eine Amazon- EventBridge Regel das Ereignis an den zentralen Event Bus im Hub-Konto. Im Hub-Konto sendet eine - EventBridge Regel das Ereignis an eine AWS Lambda-Funktion. Die Funktion verwendet ein Amazon Simple Notification Service (Amazon SNS)-Thema, das Sie über die Root-Benutzeraktivität benachrichtigt.

In diesem Muster verwenden Sie eine AWS- CloudFormation Vorlage, um die Überwachungs- und Ereignisbehandlungsservices in den Spoke-Konten bereitzustellen. Sie verwenden eine HashiCorp Terraform-Vorlage, um die Ereignisverwaltungs- und Benachrichtigungsservices im Hub-Konto bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

1. Berechtigungen zum Bereitstellen von AWS-Ressourcen in Ihrer AWS-Umgebung.
2. Berechtigungen zum Bereitstellen von CloudFormation Stack-Sets. Weitere Informationen finden Sie unter Voraussetzungen für Stack-Set-Operationen (CloudFormation Dokumentation).
3. Terraform installiert und einsatzbereit. Weitere Informationen finden Sie unter Erste Schritte – AWS (Terraform-Dokumentation).
4. Ein vorhandener Trail in jedem Spoke-Konto. Weitere Informationen finden Sie unter Erste Schritte mit AWS CloudTrail (CloudTrail Dokumentation).
5. Der Trail ist so konfiguriert, dass Ereignisse an - CloudWatch Protokolle gesendet werden. Weitere Informationen finden Sie unter Senden von Ereignissen an CloudWatch Protokolle (CloudTrail Dokumentation).
6. Ihre Hub- und Spoke-Konten müssen von AWS Organizations verwaltet werden.

Architektur

Das folgende Diagramm veranschaulicht die Bausteine der Implementierung.

1. Wenn die Anmeldeinformationen des IAM-Stammbenutzers verwendet werden, CloudWatch CloudTrail zeichnen Sie die Aktivität im Protokoll bzw. im Trail auf.
2. Im Spoke-Konto sendet eine - EventBridge Regel das Ereignis an den zentralen Event Bus im Hub-Konto.
3. Im Hub-Konto sendet eine - EventBridge Regel das Ereignis an eine Lambda-Funktion.
4. Die Lambda-Funktion verwendet ein Amazon SNS-Thema, das Sie über die Root-Benutzeraktivität benachrichtigt.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen, AWS-Ressourcen einzurichten, schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und -Regionen hinweg zu verwalten.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Governance, Compliance und des Betriebsrisikos Ihres AWS-Kontos.
- Amazon CloudWatch Logs hilft Ihnen, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, damit Sie sie überwachen und sicher archivieren können.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mit API-Zielen oder Event Buses in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.

Andere Tools und Services

- Terraform ist eine CLI-Anwendung für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen mithilfe von Code in Form von Konfigurationsdateien.

Code-Repository

Der Quellcode und die Vorlagen für dieses Muster sind in einem GitHub Repository verfügbar. Dieses Muster bietet zwei Vorlagen:

- Eine Terraform-Vorlage mit den Ressourcen, die Sie im Hub-Konto bereitstellen
- Eine CloudFormation Vorlage, die Sie als Stack-Set-Instance in den Spoke-Konten bereitstellen

Das Repository hat die folgende Gesamtstruktur.

```
.
 |__README.md
 |__spoke-stackset.yaml
 |__hub.tf
 |__root-activity-monitor-module
     |__main.tf  # contains Terraform code to deploy resources in the Hub account
     |__iam      # contains IAM policies JSON files
         |__ lambda-assume-policy.json          # contains trust policy of the IAM role
 used by the Lambda function
         |__ lambda-policy.json                 # contains the IAM policy attached to
 the IAM role used by the Lambda function
     |__outputs  # contains Lambda function zip code
```

Der Abschnitt „PiCs“ enthält step-by-step Anweisungen zur Bereitstellung der Vorlagen.

Polen

Bereitstellen von Ressourcen für das Hub-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispielcode-Repository.	1. Öffnen Sie das AWS IAM Root User Activity Monitor-Repository. 2. Wählen Sie auf der Registerkarte Code über der Dateiliste Code aus und kopieren Sie dann die HTTPS-URL. 3. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis an den Speicherort, an dem Sie die Beispieldateien speichern möchten. 4. Geben Sie den folgenden Befehl ein:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone <repoURL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Terraform-Vorlage.	1. Rufen Sie Ihre Organisations-ID ab. Anweisungen finden Sie unter Anzeigen der Details einer Organisation über das Verwaltungskonto (Dokumentation zu AWS Organizations). 2. Öffnen Sie im geklonten Repository `hub.tf`. 3. Aktualisieren Sie Folgendes mit den entsprechenden Werten für Ihre Umgebung: • `OrganizationId` – Fügen Sie Ihre Organisations-ID hinzu. • `SNSTopicName` – Fügen Sie einen Namen für das Amazon SNS-Thema hinzu. • `SNSSubscriptions` – Fügen Sie die E-Mail hinzu, an die Amazon SNS-Benachrichtigungen gesendet werden sollen. • `Region` – Fügen Sie den AWS-Regionscode hinzu, in dem Sie die Ressourcen bereitstellen. Beispiel: `eu-west-1` • `Tags` – Fügen Sie Ihre Tags hinzu. Weitere Informationen finden Sie unter Markieren von	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS-Ressourcen (AWS General Reference). 4. Speichern und schließen Sie die Datei `hub.tf`.	

Stellen Sie die Ressourcen für das AWS Hub-Konto bereit.	1. Navigieren Sie in der Terraform-Befehlsz eilenschnittstelle zum Stammordner des geklonten Repositorys und geben Sie dann den folgenden Befehl ein.
	`terraform init && terraform plan`
	2. Überprüfen Sie die Ausgabe und bestätigen Sie, dass Sie die beschrieb enen Ressourcen erstellen möchten.
	3. Geben Sie den folgenden Befehl ein.
	`terraform apply`
	4. Wenn Sie dazu aufgefordert werden, bestätigen Sie die Bereitstellung, indem Sie eingeben `yes`.
		Allgemeines AWS

Bereitstellen von Ressourcen für Ihre Spoke-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. StackSets. 3. Wählen Sie oben auf der StackSets Seite Erstellen aus StackSet. 4. Wählen Sie unter Berechtigungen die Option Serviceverwaltete Berechtigungen aus. konfiguriert CloudFormation automatisch die Berechtigungen, die für die Bereitstellung auf den von AWS Organizations verwalteten Zielkonten erforderlich sind. 5. Wählen Sie unter Voraussetzung – Vorlage vorbereiten die Option Vorlage ist bereit aus. 6. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. 7. Wählen Sie Datei auswählen und dann im geklonten Repository aus`spoke-stackset.yaml` .	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie Weiter aus. 9. Geben Sie auf der Seite StackSet Details angeben einen Namen für das Stack-Set ein. 10. Geben Sie unter Parameter die Konto-ID des Hub-Kontos ein und wählen Sie dann Weiter aus. 11. Fügen Sie auf der Seite StackSet Optionen konfigurieren unter Tags Ihre Tags hinzu. 12. Wählen Sie unter Ausführungskonfiguration die Option Inaktiv und dann Weiter aus. 13. Geben Sie auf der Seite Bereitstellungsoptionen festlegen die Organisationseinheiten und Regionen an, in denen Sie das Stack-Set bereitstellen möchten, und wählen Sie dann Weiter aus. 14. Wählen Sie auf der Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt, und wählen Sie dann .startet die Bereitstellung Ihres Stack-Sets. CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen und Anweisungen finden Sie unter Erstellen eines Stack-Sets (CloudFormation Dokumentation).	

(Optional) Testen der Benachrichtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Anmeldeinformationen des Root-Benutzers.	1. Melden Sie sich mit den Anmeldeinformationen des Root-Benutzers bei einem Spoke-Konto oder dem Hub-Konto an. 2. Vergewissern Sie sich, dass das angegebene E-Mail-Konto die Amazon SNS-Benachrichtigung erhält.	Allgemeines AWS

Zugehörige Ressourcen

- Bewährte Methoden für die Sicherheit (IAM-Dokumentation)
- Arbeiten mit StackSets (CloudFormation Dokumentation)
- Erste Schritte (Terraform-Dokumentation)

Zusätzliche Informationen

Amazon GuardDuty ist ein kontinuierlicher Sicherheitsüberwachungsservice, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Als Alternative zu dieser Lösung können Sie, wenn Sie aktiviert haben GuardDuty, warnen, wenn die Anmeldeinformationen des Root-Benutzers verwendet wurden. Die GuardDuty

Erkenntnis ist `Policy:IAMUser/RootCredentialUsage`und der Standardschweregrad ist Niedrig. Weitere Informationen finden Sie unter Verwalten von Amazon- GuardDuty Erkenntnissen.

Senden einer Benachrichtigung, wenn ein IAM-Benutzer erstellt wird

Erstellt von Mansi Suratwala (AWS) und Sergiy Shevchenko (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Infrastruktur	Workload: Alle anderen Workloads
AWS-Services: Amazon SNS ;AWS Identity and Access Management ;AWS Lambda; Amazon CloudWatch		

Übersicht

Auf Amazon Web Services (AWS) können Sie dieses Muster verwenden, um eine AWS-CloudFormation Vorlage bereitzustellen, die automatisch Benachrichtigungen empfängt, wenn AWS Identity and Access Management (IAM)-Benutzer erstellt werden.

Mit IAM können Sie den Zugriff auf AWS-Services und -Ressourcen sicher verwalten. Sie können AWS-Benutzer und -Gruppen erstellen und verwalten sowie Berechtigungen verwenden, um diesen Benutzern und Gruppen den Zugriff auf AWS-Ressourcen zu erlauben und zu verweigern.

Die CloudFormation Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS Lambda-Funktion. Das Ereignis verwendet AWS CloudTrail zur Überwachung aller IAM-Benutzer, die im AWS-Konto erstellt werden. Wenn ein Benutzer erstellt wird, initiiert das CloudWatch Ereignis Ereignisse eine Lambda-Funktion, die Ihnen eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung sendet, die Sie über das neue Benutzererstellungsereignis informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein erstellter und bereitgestellter AWS- CloudTrail Trail

Einschränkungen

- Die AWS- CloudFormation Vorlage darf `CreateUser` nur für bereitgestellt werden.

Architektur

Zieltechnologie-Stack

- IAM
- AWS CloudTrail
- Amazon CloudWatch -Ereignisse
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die AWS- CloudFormation Vorlage mehrmals für verschiedene AWS-Regionen und -Konten verwenden. Sie müssen sie nur einmal in jeder Region oder jedem Konto ausführen. Um die Bereitstellung für mehrere Konten zu automatisieren, verwenden Sie AWS CloudFormation StackSets. Die CloudFormation Vorlage kann alle erforderlichen Ressourcen in jedem Konto bereitstellen.

Tools

Tools

- IAM – AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher steuern können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer Amazon Web Services-Ressourcen, sodass Sie weniger Zeit für die Verwaltung dieser Ressourcen aufwenden müssen und sich mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden. Sie erstellen eine Vorlage, die alle gewünschten AWS-Ressourcen

beschreibt, und CloudFormation übernimmt die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

- AWS CloudTrail – AWS CloudTrail unterstützt Sie bei der Verwaltung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos. Aktionen eines Benutzers, einer Rolle oder eines AWS-Services werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen, die in der AWS-Managementkonsole, der AWS-Befehlszeilenschnittstelle und den AWS SDKs und APIs durchgeführt werden.
- Amazon CloudWatch Events – Amazon CloudWatch Events liefert einen near-real-time Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung mithilfe von Lambda, HTTP, E-Mail, mobilen Push-Benachrichtigungen und mobilen Textnachrichten (SMS) bereitstellt.

Code

Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Polen

Erstellen des S3-Buckets für das Lambda-Skript

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Öffnen Sie die Amazon S3-Konsole und wählen oder erstellen Sie einen S3-Bucket . Dieser S3-Bucket hostet die ZIP-Datei des Lambda-Co des. Der S3-Bucket-Name darf	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	keine führenden Schrägstriche enthalten.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code hoch.	Laden Sie die im Abschnitt Anhänge bereitgestellte ZIP-Datei mit dem Lambda-Code in den von Ihnen definierten S3-Bucket hoch.	Cloud-Architekt

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Stellen Sie in der CloudFormation Konsole die CloudFormation `createIAMuser.yaml` Vorlage bereit, die als Anhang zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt

Schließen Sie die Parameter in der CloudFormation Vorlage ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen des S3-Buckets an.	Geben Sie den Namen des S3-Buckets ein, den Sie im	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ersten Epos erstellt oder ausgewählt haben.	
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der ZIP-Datei des Lambda-Codes in Ihrem S3-Bucket ohne voranstehende Schrägstriche an (z. B. `<directory>/<file-name>.zip`).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und -häufigkeit für Ihre Lambda-Funktion. `Info` bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. `Error` bezeichnet Fehlerereignisse, die der Anwendung weiterhin die Ausführung ermöglichen könnten. `Warning` bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnemen	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	t-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätige n.	

Zugehörige Ressourcen

- Erstellen eines Trails
- Erstellen eines S3-Buckets
- Hochladen von Dateien in einen S3-Bucket
- Bereitstellen einer CloudFormation Vorlage
- Erstellen eines IAM-Benutzers
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Verhindern Sie den Internetzugang auf Kontoebene mithilfe einer Dienststeuerungsrichtlinie

Erstellt von Sergiy Shevchenko (AWS), Sean O'Sullivan (AWS) und Victor Mazeo Whitaker (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Netzwerke	AWS-Services: AWS Organizations

Übersicht

Organizations möchten häufig den Internetzugang für Kontoressourcen einschränken, die privat bleiben sollten. Bei diesen Konten sollten die Ressourcen in virtuellen privaten Clouds (VPCs) auf keinen Fall auf das Internet zugreifen. Viele Unternehmen entscheiden sich für eine zentralisierte Inspektionsarchitektur. Für den Ost-West-Verkehr (VPC-zu-VPC) in einer zentralen Inspektionsarchitektur müssen Sie sicherstellen, dass die Spoke-Konten und ihre Ressourcen keinen Zugriff auf das Internet haben. Für Nord-Süd-Verkehr (ausgehender und lokaler Internetverkehr) möchten Sie den Internetzugang nur über die Inspektions-VPC zulassen.

Dieses Muster verwendet eine Service Control Policy (SCP), um den Internetzugang zu verhindern. Sie können dieses SCP auf Konto- oder Organisationseinheitsebene (OU) anwenden. Das SCP schränkt die Internetkonnektivität ein, indem es Folgendes verhindert:

- Erstellen oder Anhängen eines IPv4- oder IPv6-Internet-Gateways, das direkten Internetzugang zur VPC ermöglicht
- Erstellen oder Annehmen einer VPC-Peering-Verbindung, die möglicherweise indirekten Internetzugang über eine andere VPC ermöglicht
- Erstellen oder Aktualisieren einer AWS Global AcceleratorKonfiguration, die direkten Internetzugriff auf VPC-Ressourcen ermöglichen könnte

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine oder mehrere AWS-Konten werden als Organisation verwaltet in AWS Organizations.

- Alle Funktionen sind in aktiviert AWS Organizations.
- SCPs sind in der Organisation aktiviert.
- Berechtigungen für:
  - Greifen Sie auf das Verwaltungskonto der Organisation zu.
  - SCPs erstellen. Weitere Informationen zu den Mindestberechtigungen finden Sie unter SCP erstellen.
  - Ordnen Sie den SCP den Zielkonten oder Organisationseinheiten (OUs) zu. Weitere Informationen zu den Mindestberechtigungen finden Sie unter Dienststeuerungsrichtlinien anhängen und trennen.

Einschränkungen

- SCPs haben keine Auswirkungen auf Benutzer oder Rollen im Verwaltungskonto. Sie wirken sich nur auf die Mitgliedskonten Ihrer Organisation aus.
- SCPs betreffen nur AWS Identity and Access Management (IAM-) Benutzer und Rollen, die von Konten verwaltet werden, die Teil der Organisation sind. Weitere Informationen zu SCP-Auswirkungen auf Berechtigungen.

Tools

AWS-Services

- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten. In diesem Muster verwenden Sie Service Control Policies (SCPs) in AWS Organizations.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Bewährte Methoden

Nachdem Sie dieses SCP in Ihrem Unternehmen eingerichtet haben, stellen Sie sicher, dass Sie es regelmäßig aktualisieren, um alle neuen Funktionen AWS-Services oder Funktionen zu berücksichtigen, die den Internetzugang beeinträchtigen könnten.

Epen

Erstelle das SCP und hänge es an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SCP.	1. Melden Sie sich an der AWS Organizations - Konsole an. Sie müssen sich mit dem Verwaltungskonto der Organisation anmelden. 2. Wählen Sie im linken Bereich Richtlinien aus. 3. Wählen Sie auf der Seite mit den Richtlinien die Option Dienststeuerungsrichtlinien aus. 4. Wählen Sie auf der Seite Service-Kontrollrichtlinien die Option Richtlinie erstellen aus. 5. Geben Sie auf der Seite Neue Dienststeuerungsrichtlinie erstellen einen Richtliniennamen und optional eine Richtlinienbeschreibung ein. 6. (Optional) Fügen Sie Ihrer Richtlinie AWS Tags hinzu. 7. Löschen Sie im JSON-Editor die Platzhalterrichtlinie. 8. Fügen Sie die folgende - Richtlinie in den JSON-Editor ein.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	  "Version":
	 "2012-10-17",
	  "Statement": [
	  {
	  "Action": [
	  "ec2:Atta
	chInternetGateway",
	  "ec2:Crea
	teInternetGateway",
	
	  "ec2:Crea
	teVpcPeeringConnec
	tion",
	  "ec2:Acce
	ptVpcPeeringConnec
	tion",
	  "ec2:Crea
	teEgressOnlyIntern
	etGateway"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  },
	  {
	  "Action": [
	  "globalac
	celerator:Create*",
	  "globalac
	celerator:Update*"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  }
	  ]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Richtlinie erstellen aus.	
Hängen Sie das SCP an.	1. Wählen Sie auf der Seite Service Control-Richtlinie n die Richtlinie aus, die Sie erstellt haben. 2. Klicken Sie in der Registerk arte Ziele auf Anfügen. 3. Wählen Sie die Organisat ionseinheit oder das Konto aus, an das Sie die Richtlinie anhängen möchten. Möglicherweise müssen Sie die Organisat ionseinheiten erweitern , um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden. 4. Wählen Sie Richtlinie anfügen aus.	AWS-Administrator

Zugehörige Ressourcen

- AWS Organizations Dokumentation
- Service-Kontrollrichtlinien (SCPs)
- Zentralisierte Inspektionsarchitektur mit AWS Gateway Load Balancer und AWS Transit Gateway (AWS Blogbeitrag)

Scannen Sie Git-Repositorys mithilfe von git-secrets auf sensible Informationen und Sicherheitsprobleme

Erstellt vonrabh Singh (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance	Workload: Open-Source

Übersicht

Dieses Muster beschreibt, wie Sie das Open-Source-Tool Git-Secrets von AWS Labs verwenden, um Git-Quell-Repositorys zu scannen und Code zu finden, der möglicherweise sensible Informationen wie Benutzerpasswörter oder AWS-Zugriffsschlüssel enthalten könnte oder bei dem andere Sicherheitsprobleme auftreten.

`git-secrets` scannt Commits, Commit-Nachrichten und Zusammenführungen, um zu verhindern, dass vertrauliche Informationen wie Secrets zu Ihren Git-Repositorys hinzugefügt werden. Wenn beispielsweise ein Commit, eine Commit-Nachricht oder ein Commit in einem Zusammenführungsverlauf mit einem Ihrer konfigurierten, verbotenen regulären Ausdrucksmuster übereinstimmt, wird der Commit abgelehnt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Git-Repository, das einen Sicherheitsscan erfordert
- Ein installierter Git-Client (Version 2.37.1 und höher)

Architektur

Zielarchitektur

- Git

- `git-secrets`

Tools

- git-secrets ist ein Tool, das verhindert, dass Sie vertrauliche Informationen in Git-Repositorys übertragen.
- Git ist ein verteiltes Open-Source-Versionsverwaltungssystem.

Bewährte Methoden

- Scannen Sie ein Git-Repository immer, indem Sie alle Revisionen einschließen:

```
git secrets --scan-history
```

Polen

Herstellen einer Verbindung mit einer EC2-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe von SSH eine Verbindung zu einer EC2-Instance her.	Stellen Sie mithilfe von SSH und einer Schlüsselpaardatei eine Verbindung zu einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance her. Sie können diesen Schritt überspringen, wenn Sie ein Repository auf Ihrem lokalen Computer scannen.	Allgemeines AWS

Installieren Sie Git

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Git.	Installieren Sie Git mit dem Befehl : `yum install git -y` Wenn Sie Ihren lokalen Computer verwenden, können Sie einen Git-Client für eine bestimmte Betriebssystemversion installieren. Weitere Informationen finden Sie auf der Git-Website .	Allgemeines AWS

Klonen Sie das Quell-Repository und installieren Sie git-secrets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Git-Quell-Repository.	Um das Git-Repository zu klonen, das Sie scannen möchten, wählen Sie den Git-Klonbefehl aus Ihrem Stammverzeichnis aus.	Allgemeines AWS
Klonen Sie git-secrets.	Klonen Sie das `git-secrets` Git-Repository. `git clone https://github.com/awslabs/git-secrets.git` Platzieren Sie `git-secrets` irgendwo in Ihrem , `PATH`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	damit Git es abholt, wenn Sie ausführen`git-secrets .`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie git-secrets.	Für Unix und Varianten (Linux/macOS):
	
	Sie können das `install` Ziel des `Makefile` (im `git-secrets` Repository bereitgestellt) verwenden, um das Tool zu installieren. Sie können den Installationspfad mithilfe der `MANPREFIX` Variablen `PREFIX` und anpassen.
	
	`make install`
	
	Für Windows:
	
	Führen Sie das PowerShell `install.ps1` im `git-secrets` Repository bereitgestellte Skript aus. Dieses Skript kopiert die Installationsdateien in ein Installationsverzeichnis (`%USERPROFILE%/.git-secrets` standardmäßig) und fügt das Verzeichnis dem aktuellen Benutzer hinzu`PATH`.
	
	`PS > ./install.ps1`
	
	Für Homebrew (macOS-Benutzer):
	
	Führen Sie Folgendes aus:
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`brew install git-secrets` Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	

Git-Code-Repository scannen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie zum Quell-Repository.	Wechseln Sie zum Verzeichnis für das Git-Repository, das Sie scannen möchten: `cd my-git-repository`	Allgemeines AWS
Registrieren Sie den AWS-Regelsatz (Git-Hooks).	Um so zu konfigurieren`git-secrets` , dass Ihr Git-Repository bei jedem Commit gescannt wird, führen Sie den Befehl aus: `git secrets --register-aws`	Allgemeines AWS
Scannen Sie das Repository.	Führen Sie den folgenden Befehl aus, um mit dem Scannen Ihres Repositorys zu beginnen: `git secrets --scan`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Ausgabedatei.	Das Tool generiert eine Ausgabedatei, wenn es eine Schwachstelle in Ihrem Git-Repository findet. Beispielsweise:
	`example.sh:4:AWS_SECRET_ACCESS_KEY = *********`
	
	`[ERROR] Matched one or more prohibited patterns`
	
	`Possible mitigations:`
	`- Mark false positives as allowed using: git config --add secrets.allowed ...`
	`- Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory`
	`- List your configured patterns: git config --get-all secrets.patterns`
	`- List your configured allowed patterns: git config --get-all secrets.allowed`
	`- List your configured allowed patterns in .gitallowed at repository's root directory`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`- Use --no-verify if this is a one-time false positive`	

Zugehörige Ressourcen

- Git-Webhooks mit AWS-Services (AWS-Schnellstart)
- git-secrets-Tool
- Migrieren eines Git-Repositorys zu AWS (praxisorientiertes AWS-Tutorial)
- AWS CodeCommit -API-Referenz

Senden von Warnungen von AWS Network Firewall an einen Slack-Kanal

Erstellt von Venki Srivatsav (AWS) und Boll Raj Jayarajan (AWS)

Code-Repository: NfwSlackIntegration	Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Netzwerk
AWS-Services: AWS Lambda; AWS Network Firewall; Amazon S3		

Übersicht

Dieses Muster beschreibt, wie eine Firewall mithilfe der Amazon Web Services (AWS) Network Firewall mit dem verteilten Bereitstellungsmodell bereitgestellt wird und wie die von AWS Network Firewall generierten Warnungen an einen konfigurierbaren Slack-Kanal weitergegeben werden.

Compliance-Standards wie Payment Card Industry Data Security Standard (PCI DSS) erfordern die Installation und Wartung einer Firewall zum Schutz von Kundendaten. In der AWS Cloud wird eine Virtual Private Cloud (VPC) im Kontext dieser Compliance-Anforderungen als physisches Netzwerk betrachtet. Sie können Network Firewall verwenden, um den Netzwerkverkehr zwischen VPCs zu überwachen und Ihre Workloads zu schützen, die in VPCs ausgeführt werden, die einem Compliance-Standard unterliegen. Die Netzwerk-Firewall blockiert den Zugriff oder generiert Warnungen, wenn sie unbefugten Zugriff von anderen VPCs im selben Konto erkennt. Network Firewall unterstützt jedoch eine begrenzte Anzahl von Zielen für die Bereitstellung der Warnungen. Zu diesen Zielen gehören Amazon Simple Storage Service (Amazon S3)-Buckets, Amazon- CloudWatch Protokollgruppen und Amazon Data Firehose-Bereitstellungsdatenströme. Jede weitere Aktion für diese Benachrichtigungen erfordert eine Offline-Analyse mithilfe von Amazon Athena oder Amazon Kinesis .

Dieses Muster bietet eine Methode zum Weitergeben von Warnungen, die von Network Firewall generiert werden, an einen konfigurierbaren Slack-Kanal, um weitere Aktionen nahezu in Echtzeit auszuführen. Sie können die Funktionalität auch auf andere Warnmechanismen wie PagerDuty, J Bol und E-Mail erweitern. (Diese Anpassungen liegen außerhalb des Bereichs dieses Musters.)

Voraussetzungen und Einschränkungen

Voraussetzungen

- Slack-Kanal (siehe Erste Schritte im Slack-Hilfecenter)
- Erforderliche Berechtigungen zum Senden einer Nachricht an den Kanal
- Die Slack-Endpunkt-URL mit einem API-Token (wählen Sie Ihre App aus und wählen Sie einen eingehenden Webhook aus, um die URL anzuzeigen. Weitere Informationen finden Sie unter Erstellen eines eingehenden Webhooks in der Slack-API-Dokumentation).
- Eine Amazon Elastic Compute Cloud (Amazon EC2)-Test-Instance in den Workload-Subnetzen
- Testregeln in Network Firewall
- Tatsächlicher oder simulierter Datenverkehr zum Auslösen der Testregeln
- Ein S3-Bucket für die Quelldateien, die bereitgestellt werden sollen

Einschränkungen

- Derzeit unterstützt diese Lösung nur einen einzigen CIDR-Bereich (Classless Inter-Domain Routing) als Filter für Quell- und Ziel-IPs.

Architektur

Zieltechnologie-Stack

- Eine VPC
- Vier Subnetze (zwei für die Firewall und zwei für Workloads)
- Internet-Gateway
- Vier Routing-Tabellen mit Regeln
- S3-Bucket, der als Warnziel verwendet wird und mit einer Bucket-Richtlinie und Ereigniseinstellungen zum Ausführen einer Lambda-Funktion konfiguriert ist
- Lambda-Funktion mit einer Ausführungsrolle zum Senden von Slack-Benachrichtigungen
- AWS Secrets Manager-Secret zum Speichern der Slack-URL
- Netzwerk-Firewall mit Warnkonfiguration
- Slack-Kanal

Alle Komponenten mit Ausnahme des Slack-Kanals werden von den CloudFormation Vorlagen und der Lambda-Funktion bereitgestellt, die mit diesem Muster bereitgestellt werden (siehe Abschnitt Code).

Zielarchitektur

Dieses Muster richtet eine verteilte Netzwerk-Firewall mit Slack-Integration ein. Diese Architektur besteht aus einer VPC mit zwei Availability Zones. Die VPC umfasst zwei geschützte Subnetze und zwei Firewall-Subnetze mit Netzwerk-Firewall-Endpunkten. Der gesamte Datenverkehr, der in und aus den geschützten Subnetzen fließt, kann durch die Erstellung von Firewall-Richtlinien und -Regeln überwacht werden. Die Netzwerk-Firewall ist so konfiguriert, dass alle Warnungen in einem S3-Bucket platziert werden. Dieser S3-Bucket ist so konfiguriert, dass er eine Lambda-Funktion aufruft, wenn er ein `put`Ereignis empfängt. Die Lambda-Funktion ruft die konfigurierte Slack-URL von Secrets Manager ab und sendet die Benachrichtigung an den Slack-Workspace.

Weitere Informationen zu dieser Architektur finden Sie im AWS-BlogbeitragDeployment-Modelle für AWS Network Firewall .

Tools

AWS-Services

- AWS Network Firewall ist eine zustandsbehaftete, verwaltete Netzwerk-Firewall sowie ein Service zur Erkennung und Verhinderung von Eindringlingen für VPCs in der AWS Cloud. Sie können Network Firewall verwenden, um den Datenverkehr am Perimeter Ihrer VPC zu filtern und Ihre Workloads auf AWS zu schützen.
- AWS Secrets Manager ist ein Service zum Speichern und Abrufen von Anmeldeinformationen. Mit Secrets Manager können Sie fest codierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager ersetzen, um das Secret programmgesteuert abzurufen. Dieses Muster verwendet Secrets Manager, um die Slack-URL zu speichern.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen. Dieses Muster verwendet Amazon S3, um die CloudFormation Vorlagen und das Python-Skript für die Lambda-Funktion zu speichern. Es verwendet auch einen S3-Bucket als Ziel für Netzwerk-Firewall-Warnungen.

- AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Dieses Muster verwendet AWS CloudFormation , um automatisch eine verteilte Architektur für Firewall Manager bereitzustellen.

Code

Der Code für dieses Muster ist auf GitHubim Network Firewall Slack Integration Repository verfügbar. Im `src` Ordner des Repositorys finden Sie:

- Eine Reihe von CloudFormation Dateien im YAML-Format. Sie verwenden diese Vorlagen, um die Komponenten für dieses Muster bereitzustellen.
- Eine Python-Quelldatei (`slack-lambda.py`) zum Erstellen der Lambda-Funktion.
- Ein ZIP-Archiv-Bereitstellungspaket (`slack-lambda.py.zip`) zum Hochladen Ihres Lambda-Funktionscodes.

Um diese Dateien zu verwenden, folgen Sie den Anweisungen im nächsten Abschnitt.

Polen

Einrichten des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3. 2. Wählen oder erstellen Sie einen S3-Bucket zum Hosten des Codes. Ein S3-Bucket-Name ist global eindeutig und	App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Namespace wird von allen AWS-Konten gemeinsam genutzt. Der Name des S3-Bucket s darf keine führenden Schrägstriche enthalten. Wir empfehlen Ihnen, ein Präfix zu verwenden, um den Code für dieses Muster zu organisieren. Weitere Informationen finden Sie unter Erstellen eines Buckets in der Amazon S3-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlagen und den Lambda-Code hoch.	1. Laden Sie die folgenden Dateien aus dem GitHub Repository für dieses Muster herunter: • `base.yml` • `igw-ingress-route.yml` • `slack-lambda.py` • `slackLambda.yml` • `decentralized-deployment.yml` • `protected-subnet-route.yml` • `slack-lambda.py.zip` 2. Laden Sie die Dateien in den von Ihnen erstellten S3-Bucket hoch.	App-Entwickler, App-Besitzer, Cloud-Administrator

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage.	Öffnen Sie die AWS-CloudFormation Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die Vorlage bereit`base.yml`. Diese Vorlage erstellt die erforderlichen AWS-Ressourcen und Lambda-Funktionen für die Übertragung der	App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Warnungen an den Slack-Kanal. Weitere Informationen zum Bereitstellen von CloudFormation Vorlagen finden Sie unter Erstellen eines Stacks auf der AWS- CloudFormation Konsole in der - CloudFormation Dokumentation.	
Schließen Sie die Parameter in der Vorlage ab.	Geben Sie den Stack-Namen an und konfigurieren Sie die Parameterwerte. Eine Liste der Parameter, ihrer Beschreibungen und Standardwerte finden Sie unter CloudFormation Parameter im Abschnitt Zusätzliche Informationen.	App-Entwickler, App-Besitzer, Cloud-Administrator
Erstellen Sie den Stack.	1. Überprüfen Sie die Stack-Details und aktualisieren Sie die Werte basierend auf Ihren Umgebungsanforderungen. 2. Wählen Sie Stack erstellen, um die Vorlage bereitzustellen.	App-Entwickler, App-Besitzer, Cloud-Administrator

Überprüfen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Bereitstellung.	Verwenden Sie die AWS-CloudFormation Konsole	App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder die AWS Command Line Interface (AWS CLI), um zu überprüfen, ob die im Abschnitt Zieltechnologie-Stack aufgeführten Ressourcen erstellt wurden. Wenn die CloudFormation Vorlage nicht erfolgreich bereitgestellt werden kann, überprüfen Sie die Werte, die Sie für die `pAvailabilityZone2` Parameter `pAvailabilityZone1` und angegeben haben. Diese sollten für die AWS-Region geeignet sein, in der Sie die Lösung bereitstellen. Eine Liste der Availability Zones für jede Region finden Sie unter Regionen und Zonen in der Amazon EC2-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Funktionalität.	1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
	
	2. Erstellen Sie eine EC2-Instance in einem der geschützten Subnetze. Wählen Sie ein Amazon Linux 2 AMI (HVM) aus, das als HTTPS-Server verwendet werden soll. Anweisungen finden Sie unter Starten einer Instance in der Amazon EC2-Dokumentation.
	
	3. Verwenden Sie die folgenden Benutzerdaten, um einen Webserver auf der EC2-Instance zu installieren:
	
	`#!/bin/bash`
	`yum install httpd -y`
	`systemctl start httpd`
	`systemctl stop firewalld`
	`cd /var/www/html`
	`echo "Hello!! this is a NFW alert test page, 200 OK" > index.html`
	
	4. Erstellen Sie die folgenden Netzwerk-Firewall-Regeln:
	
	Zustandslose Regel:
	
	`Source: 0.0.0.0/0`
		App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Destination 10.0.3.65 /32 (private IP of the EC2 instance) Action: Forward`
	
	Zustandsbehaftete Regel:
	
	`Protocol: HTTP Source ip/port: Any / Any Destination ip/port: Any /Any`
	
	5. Rufen Sie die öffentliche IP des Webservers ab, den Sie in Schritt 3 erstellt haben.
	
	6. Greifen Sie in einem Browser auf die öffentliche IP zu. Die folgende Meldung sollte im Browser angezeigt werden:
	
	`Hello!! this is a NFW alert test page, 200 OK`
	
	Sie erhalten auch eine Benachrichtigung im Slack-Kanal. Die Benachrichtigung kann sich je nach Größe der Nachricht verzögern. Erwägen Sie zu Testzwecken, einen CIDR-Filter bereitzustellen, der nicht zu eng ist (z. B. würde ein CIDR-Wert mit /32 als zu eng und /8 als zu breit	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	angesehen). Weitere Informationen finden Sie im Abschnitt Filterverhalten unter Zusätzliche Informationen.	

Zugehörige Ressourcen

- Bereitstellungsmodelle für AWS Network Firewall (AWS-Blogbeitrag)
- AWS Network Firewall-Richtlinien (AWS-Dokumentation)
- Network Firewall Slack Integration (GitHub Repository)
- Einen Slack-Workspace erstellen (Slack-Hilfecenter)

Zusätzliche Informationen

CloudFormation -Parameter

Parameter	Beschreibung	Standard- oder Beispielwert
`pVpcName`	Der Name der zu erstellenden VPC.	Überprüfung
`pVpcCidr`	Der CIDR-Bereich, den die VPC erstellen soll.	10.0.0.0/16
`pVpcInstanceTenancy`	Wie EC2-Instances auf physische Hardware verteilt werden. Optionen sind `default` (Shared Tenancy) oder `dedicated` (Single Tenancy).	default
`pAvailabilityZone1`	Die erste Availability Zone für die Infrastruktur.	us-east-2a

pAvailabilityZone2	Die zweite Availability Zone für die Infrastruktur.	us-east-2b
pNetworkFirewallSubnet1Cidr	Der CIDR-Bereich für das erste Firewall-Subnetz (mindestens /28).	10.0.1.0/24
pNetworkFirewallSubnet2Cidr	Der CIDR-Bereich für das zweite Firewall-Subnetz (mindestens /28).	10.0.2.0/24
pProtectedSubnet1Cidr	Der CIDR-Bereich für das erste geschützte Subnetz (Workload).	10.0.3.0/24
pProtectedSubnet2Cidr	Der CIDR-Bereich für das zweite geschützte Subnetz (Workload).	10.0.4.0/24
pS3BucketName	Der Name des vorhandenen S3-Buckets, in den Sie den Lambda-Quellcode hochgeladen haben.	us-w2-yourname-lambda-functions
pS3KeyPrefix	Das Präfix des S3-Buckets, in den Sie den Lambda-Quellcode hochgeladen haben.	Aod-Test
pAWSSecretName4Slack	Der Name des Secrets, das die Slack-URL enthält.	SlackEnpoint-Cfn
pSlackChannelName	Der Name des von Ihnen erstellten Slack-Kanals.	Einige Namensbenachrichtigungen
pSlackUserName	Slack-Benutzername.	Slack-Benutzer

`pSecretKey`	Dies kann ein beliebiger Schlüssel sein. Wir empfehlen Ihnen, die Standardeinstellung zu verwenden.	webhookUrl
`pWebHookUrl`	Der Wert der Slack-URL.	https://hooks.slack.com/services/T???9T??/A031885JRM7/9D4Y
`pAlertS3Bucket`	Der Name des S3-Buckets, der als Ziel für Netzwerk-Firewall-Warnungen verwendet werden soll. Dieser Bucket wird für Sie erstellt.	us-w2-yourname-security-aod-alerts
`pSecretTagName`	Der Tag-Name für das Secret.	AppName
`pSecretTagValue`	Der Tag-Wert für den angegebenen Tag-Namen.	LambdaSlackIntegration
`pdestCidr`	Der Filter für den Ziel-CIDR-Bereich. Weitere Informationen finden Sie im nächsten Abschnitt, Filterverhalten .	10.0.0.0/16
`pdestCondition`	Ein Flag, das angibt, ob die Zielübereinstimmung ausgeschlossen oder eingeschlossen werden soll. Weitere Informationen finden Sie im folgenden Abschnitt. Gültige Werte sind `include` und `exclude`.	include

`psrcCidr`	Der Filter für den zu warnenden Quell-CIDR-Bereich. Weitere Informati onen finden Sie im folgenden Abschnitt.	118.2.0.0/16
`psrcCondition`	Das Flag, das die Quellüber einstimmung ausschließen oder einschließen soll. Weitere Informationen finden Sie im folgenden Abschnitt.	include

Filterverhalten

Wenn Sie keine Filter in AWS Lambda konfiguriert haben, werden alle generierten Warnungen an Ihren Slack-Kanal gesendet. Die Quell- und Ziel-IPs der generierten Warnungen werden mit den CIDR-Bereichen abgeglichen, die Sie bei der Bereitstellung der CloudFormation Vorlage konfiguriert haben. Wenn eine Übereinstimmung gefunden wird, wird die Bedingung angewendet. Wenn entweder die Quelle oder das Ziel innerhalb des konfigurierten CIDR-Bereichs liegt und mindestens eine davon mit der Bedingung konfiguriert ist`include`, wird eine Warnung generiert. Die folgenden Tabellen enthalten Beispiele für CIDR-Werte, Bedingungen und Ergebnisse.

	Konfiguriertes CIDR	Warnungs-IP	Configured	Warnung
Quelle	10.0.0.0/16	10.0.0.25	include	Ja
Zieladresse	100.0.0.0/16	202.0.0.13	include	

	Konfiguriertes CIDR	Warnungs-IP	Configured	Warnung
Quelle	10.0.0.0/16	10.0.0.25	exclude	Nein
Zieladresse	100.0.0.0/16	202.0.0.13	include	

	Konfiguriertes CIDR	Warnungs-IP	Configured	Warnung
Quelle	10.0.0.0/16	10.0.0.25	include	Ja
Zieladresse	100.0.0.0/16	100.0.0.13	include	

	Konfiguriertes CIDR	Warnungs-IP	Configured	Warnung
Quelle	10.0.0.0/16	90.0.0.25	include	Ja
Zieladresse	Null	202.0.0.13	include	

	Konfiguriertes CIDR	Warnungs-IP	Configured	Warnung
Quelle	10.0.0.0/16	90.0.0.25	include	Nein
Zieladresse	100.0.0.0/16	202.0.0.13	include	

Vereinfachen der Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM

Erstellt von Bolett Hinckley (AWS) und Vivek Goyal (AWS)

Code-Repository: ACMPCA-Hierarchie	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Infrastruktur; Migration
AWS-Services: AWS Certificate Manager (ACM); AWS Organizations; AWS RAM		

Übersicht

Sie können AWS Private Certificate Authority (AWS Private CA) verwenden, um private Zertifikate für die Authentifizierung interner Ressourcen und die Signierung von Computercode auszustellen. Dieses Muster bietet eine AWS- CloudFormation Vorlage für die schnelle Bereitstellung einer mehrstufigen CA-Hierarchie und eine konsistente Bereitstellungserfahrung. Optional können Sie AWS Resource Access Manager (AWS RAM) verwenden, um die CA innerhalb Ihrer Organisationen oder Organisationseinheiten (OUs) in AWS Organizations sicher freizugeben und die CA zu zentralisieren, während Sie AWS RAM zur Verwaltung von Berechtigungen verwenden. In jedem Konto ist keine private Zertifizierungsstelle erforderlich, daher spart Ihnen dieser Ansatz Geld. Darüber hinaus können Sie Amazon Simple Storage Service (Amazon S3) verwenden, um die Zertifikatsperrliste (CRL) und Zugriffsprotokolle zu speichern.

Diese Implementierung bietet die folgenden Funktionen und Vorteile:

- Zentralisiert und vereinfacht die Verwaltung der privaten CA-Hierarchie mithilfe von AWS Private CA.
- Exportiert Zertifikate und Schlüssel auf vom Kunden verwaltete Geräte in AWS und On-Premises.
- Verwendet eine AWS- CloudFormation Vorlage für eine schnelle Bereitstellung und konsistente Bereitstellung.
- Erstellt eine private Stammzertifizierungsstelle zusammen mit der Hierarchie von 1, 2, 3 oder 4 untergeordneten Zertifizierungsstellen.

- verwendet optional AWS RAM, um die untergeordnete CA der Endentität für andere Konten auf Organisations- oder Organisationseinheitsebene freizugeben.
- Spart Geld, indem die Notwendigkeit einer privaten Zertifizierungsstelle in jedem Konto mithilfe von AWS RAM entfällt.
- Erstellt einen optionalen S3-Bucket für die CRL.
- Erstellt einen optionalen S3-Bucket für CRL-Zugriffsprotokolle.

Voraussetzungen und Einschränkungen

Voraussetzungen

Wenn Sie die CA in einer AWS Organizations-Struktur freigeben möchten, identifizieren oder richten Sie Folgendes ein:

- Ein Sicherheitskonto für die Erstellung der CA-Hierarchie und -Freigabe.
- Eine separate Organisationseinheit oder ein separates Konto für Tests.
- Freigabe aktiviert im AWS Organizations-Verwaltungskonto. Weitere Informationen finden Sie unter Aktivieren der Ressourcenfreigabe innerhalb von AWS Organizations in der AWS RAM-Dokumentation.

Einschränkungen

- CAs sind regionale Ressourcen. Alle CAs befinden sich in einem einzigen AWS-Konto und in einer einzigen AWS-Region.
- Benutzergenerierte Zertifikate und Schlüssel werden nicht unterstützt. Für diesen Anwendungsfall empfehlen wir Ihnen, diese Lösung so anzupassen, dass eine externe Stammzertifizierungsstelle verwendet wird.
- Ein öffentlicher CRL-Bucket wird nicht unterstützt. Wir empfehlen Ihnen, die CRL privat zu halten. Wenn ein Internetzugang auf die CRL erforderlich ist, lesen Sie den Abschnitt zur Verwendung von Amazon CloudFront zur Bereitstellung von CRLs unter Aktivieren der S3 Block Public Access (BPA)-Funktion in der AWS Private CA-Dokumentation.
- Dieses Muster implementiert einen einzelregionalen Ansatz. Wenn Sie eine multiregionale Zertifizierungsstelle benötigen, können Sie Untergeordnete in einer zweiten AWS-Region oder On-Premises implementieren. Diese Komplexität liegt außerhalb des Geltungsbereichs dieses

Musters, da die Implementierung von Ihrem spezifischen Anwendungsfall, Workload-Volumen, Abhängigkeiten und Anforderungen abhängt.

Architektur

Zieltechnologie-Stack

- AWS Private CA
- AWS RAM
- Amazon S3
- AWS Organizations
- AWS CloudFormation

Zielarchitektur

Dieses Muster bietet zwei Optionen für die Freigabe für AWS Organizations:

Option 1 – Erstellen Sie die Freigabe auf Organisationsebene. Alle Konten in der Organisation können die privaten Zertifikate mithilfe der freigegebenen CA ausstellen, wie im folgenden Diagramm gezeigt.

Option 2 Bol Erstellen Sie die Freigabe auf Organisationseinheitsebene (OU). Nur die Konten in der angegebenen Organisationseinheit können die privaten Zertifikate mithilfe der freigegebenen Zertifizierungsstelle ausstellen. Wenn die Freigabe beispielsweise im folgenden Diagramm auf der Ebene der Sandbox-OU erstellt wird, können sowohl Entwickler 1 als auch Entwickler 2 private Zertifikate mithilfe der gemeinsam genutzten CA ausstellen.

Tools

AWS-Services

- AWS Private CA – AWS Private Certificate Authority (AWS Private CA) ist ein gehosteter privater CA-Service zum Ausstellen und Widerrufen privater digitaler Zertifikate. Es hilft Ihnen, private CA-

Hierarchien zu erstellen, einschließlich Stamm- und untergeordneter CAs, ohne die Investitionen und Wartungskosten für den Betrieb einer On-Premises-CA.

- AWS RAM – AWS Resource Access Manager (AWS RAM) hilft Ihnen, Ihre Ressourcen sicher über AWS-Konten und innerhalb Ihrer Organisation oder OUs in AWS Organizations freizugeben. Um den betrieblichen Aufwand in einer Umgebung mit mehreren Konten zu reduzieren, können Sie eine Ressource erstellen und AWS RAM verwenden, um diese Ressource für mehrere Konten freizugeben.
- AWS Organizations – AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen. Dieses Muster verwendet Amazon S3 zum Speichern der Zertifikatsperrliste (CRL) und der Zugriffsprotokolle.
- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Dieses Muster verwendet AWS CloudFormation , um automatisch eine mehrstufige CA-Hierarchie bereitzustellen.

Code

Der Quellcode für dieses Muster ist auf GitHubim Hierarchie-Repository von AWS Private CA verfügbar. Das Repository enthält:

- Die AWS- CloudFormation Vorlage `ACMPCA-RootCASubCA.yaml`. Sie können diese Vorlage verwenden, um die CA-Hierarchie für diese Implementierung bereitzustellen.
- Testen Sie Dateien auf Anwendungsfälle wie das Anfordern, Exportieren, Beschreiben und Löschen eines Zertifikats.

Um diese Dateien zu verwenden, folgen Sie den Anweisungen im Abschnitt Clarics.

Polen

Architektur der CA-Hierarchie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie die Informationen zum Zertifikatantragsteller.	Sammeln Sie Informationen zum Zertifikatantragsteller: Organisationsname, Organisationseinheit, Land, Bundesland, Ort und allgemeiner Name.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker
Sammeln Sie optionale Informationen über AWS Organizations .	Wenn die CA Teil einer AWS Organizations-Struktur sein wird und Sie die CA-Hierarchie innerhalb dieser Struktur teilen möchten, erfassen Sie die Verwaltungskontonummer, die Organisations-ID und optional die OU-ID (wenn Sie die CA-Hierarchie nur für eine bestimmte OU freigeben möchten). Bestimmen Sie außerdem die AWS Organizations-Konten oder OUs, falls vorhanden, für die Sie die CA freigeben möchten.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker
Entwerfen Sie die CA-Hierarchie.	Bestimmen Sie, welches Konto die Stamm- und untergeordneten CAs enthält. Bestimmen Sie, wie viele untergeordnete Ebenen die Hierarchie zwischen dem Stamm und den Endentitätszertifikaten benötigt. Weitere Informationen finden Sie unter	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Entwerfen einer CA-Hierarchie in der AWS Private CA-Dokumentation.	
Legen Sie die Namens- und Markierungskonventionen für die CA-Hierarchie fest.	Bestimmen Sie die Namen für die AWS-Ressourcen: die Stammzertifizierungsstelle und jede untergeordnete Zertifizierungsstelle. Legen Sie fest, welche Tags jeder CA zugewiesen werden sollen.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker
Bestimmen Sie die erforderlichen Verschlüsselungs- und Signaturalgorithmen.	Bestimmen Sie Folgendes: • Die Anforderungen Ihres Unternehmens an den Verschlüsselungsalgorithmus für die öffentlichen Schlüssel, die Ihre Zertifizierungsstelle verwendet, wenn sie ein Zertifikat ausstellt. Der Standardwert ist RSA_2048. • Der Schlüsselalgorithmus, den Ihre Zertifizierungsstelle zum Signieren von Zertifikaten verwendet. Der Standardwert ist SHA256WITHRSA .	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie die Anforderungen an den Zertifikatswiderruf für die CA-Hierarchie.	Wenn Funktionen zum Widerrufen von Zertifikaten erforderlich sind, legen Sie eine Namenskonvention für den S3-Bucket fest, der die Zertifikatsperrliste (CRL) enthält.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker
Bestimmen Sie die Protokollierungsanforderungen für die CA-Hierarchie.	Wenn Funktionen zur Zugriffsprotokollierung erforderlich sind, legen Sie eine Namenskonvention für den S3-Bucket fest, der die Zugriffsprotokolle enthält.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker
Bestimmen Sie die Gültigkeitsdauer von Zertifikaten.	Bestimmen Sie das Ablaufdatum für das Stammzertifikat (Standard ist 10 Jahre), Endentitätszertifikate (Standard ist 13 Monate) und untergeordnete CA-Zertifikate (Standard ist 3 Jahre). Untergeordnete CA-Zertifikate sollten früher ablaufen als die CA-Zertifikate auf höheren Ebenen in der Hierarchie. Weitere Informationen finden Sie unterVerwalten des Lebenszyklus einer privaten Zertifizierungsstellein der AWS Private CA-Dokumentation.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Techniker

Bereitstellen der CA-Hierarchie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfüllen von -Voraussetzungen	Führen Sie die Schritte im Abschnitt Voraussetzungen dieses Musters aus.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure
Erstellen Sie CA-Rollen für verschiedene Personas.	1. Bestimmen Sie die Typen von AWS Identity and Access Management (IAM)-Rollen oder -Benutzern in AWS IAM Identity Center (Nachfolger von AWS Single Sign-On), die für die Verwaltung der verschiedenen Ebenen der CA-Hierarchie erforderlich sind, z. B. RootCAAdmin ,SubordinateCAAdmin und CertificateConsumer. 2. Bestimmen Sie die Granularität der Richtlinien, die zur Trennung von Aufgaben erforderlich sind. 3. Erstellen Sie die erforderlichen IAM-Rollen oder -Benutzer in IAM Identity Center in dem Konto, in dem sich die CA-Hierarchie befindet.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure
Stellen Sie den CloudFormation Stack bereit.	1. Laden Sie die Vorlage AWSPCA-RootCASubCA.yaml aus dem GitHub Repository für dieses Muster herunter.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Stellen Sie die Vorlage über die AWS- CloudFormation Konsole oder über die AWS Command Line Interface (AWS CLI) bereit. Weitere Informationen finden Sie unter Arbeiten mit Stacks in der - CloudFormation Dokumentation. 3. Vervollständigen Sie die Parameter in der Vorlage, einschließlich des Organisationsnamens, des OU-Namens, des Schlüsselalgorithmus, des Signaturalgorithmus und anderer Optionen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwerfen Sie eine Lösung zum Aktualisieren von Zertifikaten, die von benutzerverwalteten Ressourcen verwendet werden.	Ressourcen von integrierten AWS-Services, wie Elastic Load Balancing, aktualisieren Zertifikate vor Ablauf automatisch. Benutzerverwaltete Ressourcen wie Webserver, die auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances ausgeführt werden, erfordern jedoch einen anderen Mechanismus. 1. Bestimmen Sie, welche benutzerverwalteten Ressourcen Endentitätszertifikate von der privaten Zertifizierungsstelle benötigen. 2. Planen Sie einen Prozess, um über den Ablauf von benutzerverwalteten Ressourcen und Zertifikaten benachrichtigt zu werden. -Beispiele finden Sie nachfolgend. • Verwenden einer verwalteten AWS Config-Regel • Verwenden von Amazon CloudWatch und Amazon EventBridge 3. Schreiben Sie benutzerdefinierte Skripte, um	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zertifikate auf benutzerv erwalteten Ressourcen zu aktualisieren, und integrier en Sie sie in AWS-Servi ces, um die Updates zu automatisieren. Weitere Informationen zu integrier ten AWS-Services finden Sie unter In AWS Certifica te Manager integrierte Services in der ACM-Dokumentation.	

Validieren und dokumentieren Sie die CA-Hierarchie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die optionale AWS RAM-Freigabe.	Wenn die CA-Hierarchie für andere Konten in AWS Organizations freigegeben ist, melden Sie sich über die AWS-Managementkons ole bei einem dieser Konten an, navigieren Sie zur AWS Private CA-Konsole und bestätigen Sie, dass die neu erstellte CA für dieses Konto freigegeben ist. Nur die CA der niedrigsten Ebene in der Hierarchie wird angezeigt , da dies die CA ist, die die Endentitätszertifikate generiert . Wiederholen Sie diesen Vorgang für eine Stichprob	Cloud-Administrator, Sicherhei tsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e der Konten, für die die CA freigegeben ist.	
Validieren Sie die CA-Hierarchie mit Tests des Zertifikatlebenszyklus.	Suchen Sie im GitHub Repository für dieses Muster die Lebenszyklustests. Führen Sie die Tests von der AWS CLI aus, um ein Zertifikat anzufordern, ein Zertifikat zu exportieren, ein Zertifikat zu beschreiben und ein Zertifikat zu löschen.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure
Importieren Sie die Zertifikatkette in Vertrauensspeicher.	Damit Browser und andere Anwendungen einem Zertifikat vertrauen können, muss der Aussteller des Zertifikats in den Trust Store des Browsers aufgenommen werden. Dabei handelt es sich um eine Liste CAs. Fügen Sie die Zertifikatkette für die neue CA-Hierarchie zum Trust Store Ihres Browsers und Ihrer Anwendung hinzu. Vergewissern Sie sich, dass die Endentitätszertifikate vertrauenswürdig sind.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Runbook, um die CA-Hierarchie zu dokumentieren.	Erstellen Sie ein Runbook-Dokument, um die Architektur der CA-Hierarchie, die Kontostruktur, die Endentitätszertifikate anfordern kann, den Erstellungsprozess und grundlegende Verwaltungsaufgaben wie die Ausstellung von Endentitätszertifikaten (es sei denn, Sie möchten Self-Service durch untergeordnete Konten zulassen), die Verwendung und die Nachverfolgung zu beschreiben.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Zugehörige Ressourcen

- Entwerfen einer CA-Hierarchie (Dokumentation von AWS Private CA)
- Erstellen einer privaten Zertifizierungsstelle (Dokumentation zu AWS Private CA)
- So verwenden Sie AWS RAM, um Ihr kontoübergreifendes AWS Private CA freizugeben (AWS-Blogbeitrag)
- Bewährte Methoden für AWS Private CA (AWS-Blogbeitrag)
- Aktivieren der Ressourcenfreigabe in AWS Organizations (AWS RAM-Dokumentation)
- Verwaltung des Lebenszyklus privater Zertifizierungsstellen (Dokumentation von AWS Private CA)
- acm-certificate-expiration-check für AWS Config (AWS Config-Dokumentation)
- AWS Certificate Manager bietet jetzt die Überwachung des Zertifikatablaufs über Amazon CloudWatch (AWS-Ankündigung)
- In AWS Certificate Manager integrierte Services (ACM-Dokumentation)

Zusätzliche Informationen

Wenn Sie Zertifikate exportieren, verwenden Sie eine Passphrase, die kryptografisch stark ist und der Strategie Ihrer Organisation zur Verhinderung von Datenverlust entspricht.

Deaktivieren von Sicherheitsstandardkontrollen für alle Security Hub-Mitgliedskonten in einer Umgebung mit mehreren Konten

Erstellt vonlbier (AWS) und Ahmed Bakry (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Serverless	AWS-Services: Amazon DynamoDB; Amazon EventBridge; AWS Lambda; AWS Security Hub; AWS Step Functions

Übersicht

> Wichtig: AWS Security Hub unterstützt jetzt eine zentrale Konfiguration für Sicherheitsstandards und -kontrollen über -Konten hinweg. Dieses neue Feature behandelt viele der Szenarien, die von der Lösung in diesem APG-Muster abgedeckt werden. Bevor Sie die Lösung in diesem Muster bereitstellen, lesen Sie Zentrale Konfiguration in Security Hub .

In der Amazon Web Services (AWS) Cloud können AWS Security Hub-Standardkontrollen wie CIS AWS Foundations Benchmark oder AWS Foundational Security Best Practices nur manuell innerhalb eines einzigen AWS-Kontos deaktiviert (deaktiviert) werden. In einer Umgebung mit mehreren Konten können Sie die Steuerelemente nicht über mehrere Security Hub-Mitgliedskonten hinweg mit einem Klick deaktivieren (d. h. einem API-Aufruf). Dieses Muster zeigt, wie Sie mit einem Klick die Security Hub-Standardsteuerelemente für alle Security Hub-Mitgliedskonten deaktivieren, die von Ihrem Security Hub-Administratorkonto verwaltet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Umgebung mit mehreren Konten, die aus einem Security Hub-Administratorkonto besteht, das mehrere Mitgliedskonten verwaltet
- AWS Command Line Interface (AWS CLI) Version 2, installiert
- AWS Serverless Application Model Command Line Interface (AWS SAM CLI), installiert

Einschränkungen

- Dieses Muster funktioniert nur in einer Umgebung mit mehreren Konten, in der ein einzelnes Security Hub-Administratorkonto mehrere Mitgliedskonten verwaltet.
- Die Ereignisauslösung führt zu mehreren parallelen Aufrufen, wenn Sie viele Kontrollen in einem sehr kurzen Zeitrahmen ändern. Dies kann zu einer API-Drosselung führen und dazu führen, dass die Aufrufe fehlschlagen. Dieses Szenario kann beispielsweise eintreten, wenn Sie mithilfe der Security Hub Controls CLI viele Kontrollen programmgesteuert ändern.

Architektur

Zieltechnologie-Stack

- Amazon DynamoDB
- Amazon EventBridge
- AWS CLI
- AWS Lambda
- AWS SAM-CLI
- AWS Security Hub
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm zeigt ein Beispiel für einen Step-Functions-Workflow, der Security-Hub-Standardsteuerelemente für mehrere Security-Hub-Mitgliedskonten deaktiviert (wie vom Security-Hub-Administratorkonto aus angezeigt).

Das Diagramm enthält den folgenden Workflow:

1. Eine EventBridge Regel wird nach einem täglichen Zeitplan initiiert und ruft den Zustandsautomaten auf. Sie können das Timing der Regel ändern, indem Sie den Parameter Zeitplan in Ihrer AWS- CloudFormation Vorlage aktualisieren.
2. Eine EventBridge Regel wird immer dann ausgelöst, wenn eine Kontrolle im Security Hub-Administratorkonto aktiviert oder deaktiviert wird.

3. Ein Step-Functions-Zustandsautomat überträgt den Status der Sicherheitsstandardkontrollen (d. h. Kontrollen, die aktiviert oder deaktiviert sind) vom Security-Hub-Administratorkonto an die Mitgliedskonten.
4. Eine kontoübergreifende AWS Identity and Access Management (IAM)-Rolle wird in jedem Mitgliedskonto bereitgestellt und vom Zustandsautomaten übernommen. Der Zustandsautomat aktiviert oder deaktiviert die Kontrollen in jedem Mitgliedskonto.
5. Eine DynamoDB-Tabelle enthält Ausnahmen und Informationen darüber, welche Steuerelemente in einem bestimmten Konto aktiviert oder deaktiviert werden sollen. Diese Informationen überschreiben die Konfigurationen, die vom Security Hub-Administratorkonto für das angegebene Mitgliedskonto abgerufen wurden.

Hinweis: Der Zweck der geplanten EventBridge Regel besteht darin, sicherzustellen, dass neu hinzugefügte Security Hub-Mitgliedskonten denselben Kontrollstatus wie vorhandene Konten haben.

Tools

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda-Funktionen, HTTP-Aufrufendpunkte mithilfe von API-Zielen oder Event Buses in anderen AWS-Konten.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie Serverless-Anwendungen in der AWS Cloud erstellen können.
- AWS Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS-Umgebung anhand von Standards und bewährten Methoden der Sicherheitsbranche zu überprüfen.
- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Code

Der Code für dieses Muster ist im GitHub AWS Security Hub Cross-Account Controls Disabler-Repository verfügbar. Das Code-Repository enthält die folgenden Dateien und Ordner:

- `UpdateMembers/template.yaml` – Diese Datei enthält Komponenten, die im Security Hub-Administratorkonto bereitgestellt werden, einschließlich des Step Functions-Zustandsautomaten und der EventBridge Regeln.
- `member-iam-role/template.yaml` – Diese Datei enthält den Code zum Bereitstellen der kontoübergreifenden IAM-Rolle in einem Mitgliedskonto.
- `stateMachine.json` – Diese Datei definiert den Workflow des Zustandsautomaten.
- `GetMembers/index.py` – Diese Datei enthält den Code für den GetMembersZustandsautomaten. Ein Skript ruft den Status der Sicherheitsstandardkontrollen in allen vorhandenen Security Hub-Mitgliedskonten ab.
- `UpdateMember/index.py` – Diese Datei enthält ein Skript, das den Kontrollstatus in jedem Mitgliedskonto aktualisiert.
- `CheckResult/index.py` – Diese Datei enthält ein Skript, das den Status des Workflow-Aufrufs überprüft (akzeptiert oder fehlgeschlagen).

Polen

Bereitstellen einer kontoübergreifenden IAM-Rolle in den Security Hub-Mitgliedskonten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Konto-ID des Security Hub-Administratorkontos.	Richten Sie ein Security Hub-Administratorkonto ein und notieren Sie sich dann die Konto-ID des Administratorkontos.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit, die die kontoübergreifende IAM-Rolle in den Mitgliedskonten enthält.	Führen Sie den folgenden Befehl aus, um die `member-iam-role/template.yaml` Vorlage in allen Mitgliedskonten bereitzustellen, die	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	vom Security Hub-Admin istratorkonto verwaltet werden: `aws cloudformation deploy --template-file member-iam-role/template.yaml --capabilities CAPABILITY_NAMED_IAM --stack-name <your-stack-name> --parameter-overrides SecurityHubAdminAccountId=<your-account-ID>` Der `SecurityHubAdminAccountId` Parameter muss mit der ID des Security Hub-Administratorkontos übereinstimmen, die Sie zuvor notiert haben.	

Bereitstellen eines Zustandsautomaten im Security Hub-Administratorkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verpacken Sie die CloudFormation Vorlage, die den Zustandsautomaten enthält, mit AWS SAM.	Führen Sie den folgenden Befehl aus, um die `UpdateMembers/template.yaml` Vorlage im Security Hub-Administratorkonto zu verpacken: `sam package --template-file UpdateMembers/template.yaml --output-template-`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`file UpdateMembers/ template-out.yaml -- s3-bucket <your-s3- bucket-name>` Hinweis: Ihr Amazon Simple Storage Service (Amazon S3)-Bucket muss sich in derselben AWS-Region befinden, in der Sie die CloudFormation Vorlage bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die verpackte CloudFormation Vorlage im Security Hub-Administratork onto bereit.	Führen Sie den folgenden Befehl aus, um die CloudForm ation Vorlage im Security Hub-Administratorkonto bereitzus tellen: `aws cloudformation deploy --template-file UpdateMembers/template-out.yaml --capabilities CAPABILITY_IAM --stack-name <your-stack-name>` In der `member-iam-role/template.yaml` Vorlage muss der MemberIAM RolePath-Parameter mit dem IAMRolePath-Paramete r übereinstimmen und MemberIAMRoleName muss mit IAMRoleName übereinst immen. Hinweis: Da Security Hub ein regionaler Service ist, müssen Sie die Vorlage in jeder AWS-Region einzeln bereitstellen. Stellen Sie sicher, dass Sie die Lösung zuerst in einen S3-Bucket in jeder Region verpacken.	AWS DevOps

Zugehörige Ressourcen

- Benennen eines Security Hub-Administratorkontos (AWS Security Hub-Dokumentation)
- Umgang mit Fehlern, Wiederholungsversuchen und Hinzufügen von Warnungen zu Step Function State Machine Executions (AWS-Blogbeitrag)

Aktualisieren von AWS CLI-Anmeldeinformationen von AWS IAM Identity Center mithilfe von PowerShell

Erstellt von Chad Bol (AWS) und Andyen (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Cloudnativ	Workload: Open-Source
AWS-Services: AWS-Tools für PowerShell; AWS IAM Identity Center		

Übersicht

Wenn Sie AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Anmeldeinformationen mit AWS Command Line Interface (AWS CLI), AWS SDKs oder AWS Cloud Development Kit (AWS CDK) verwenden möchten, müssen Sie die Anmeldeinformationen in der Regel aus der IAM Identity Center-Konsole kopieren und in die Befehlszeilenschnittstelle einfügen. Dieser Vorgang kann beträchtliche Zeit in Anspruch nehmen und muss für jedes Konto wiederholt werden, das Zugriff benötigt.

Eine gängige Lösung ist die Verwendung des AWS CLI-`aws sso configure`Befehls . Dieser Befehl fügt Ihrer AWS CLI oder Ihrem AWS SDK ein IAM Identity Center-fähiges Profil hinzu. Der Nachteil dieser Lösung besteht jedoch darin, dass Sie den Befehl `aws sso login` für jedes AWS CLI-Profil oder -Konto ausführen müssen, das Sie auf diese Weise konfiguriert haben.

Als alternative Lösung beschreibt dieses Muster, wie Sie AWS CLI-benannte Profile und AWS-Tools für verwenden, PowerShell um Anmeldeinformationen für mehrere Konten gleichzeitig von einer einzelnen IAM Identity Center-Instance aus zu speichern und zu aktualisieren. Das Skript speichert auch IAM-Identity-Center-Sitzungsdaten im Speicher, um Anmeldeinformationen zu aktualisieren, ohne sich erneut bei IAM Identity Center anzumelden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- PowerShell, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren von PowerShell (Microsoft-Dokumentation).
- AWS-Tools für PowerShell, installiert und konfiguriert. Aus Leistungsgründen empfehlen wir dringend, die modularisierte Version von AWS-Tools für zu installieren PowerShell. `AWS.Tools` Jeder AWS-Service wird von einem eigenen individuellen, kleinen Modul unterstützt. Geben Sie in der PowerShell Eingabeaufforderung die folgenden Befehle ein, um die für dieses Muster erforderlichen Module zu installieren: `AWS.Tools.Installer`SSO, und `SSOIDC`.

  ```
  Install-Module AWS.Tools.Installer
  Install-AWSToolsModule SSO, SSOOIDC
  ```

  Weitere Informationen finden Sie unter Installieren von AWS.Tools unter Windows oder Installieren von AWS.Tools unter Linux oder macOS.
- AWS CLI oder das AWS SDK müssen zuvor mit funktionierenden Anmeldeinformationen konfiguriert werden, indem Sie einen der folgenden Schritte ausführen:
  - Verwenden Sie den AWS CLI-`aws configure`Befehl . Weitere Informationen finden Sie unter Schnellkonfiguration (AWS-CLI-Dokumentation).
  - Konfigurieren Sie AWS CLI oder AWS CDK, um temporären Zugriff über eine IAM-Rolle zu erhalten. Weitere Informationen finden Sie unter Abrufen von IAM-Rollenanmeldeinformationen für den CLI-Zugriff (Dokumentation zu IAM Identity Center).

Einschränkungen

- Dieses Skript kann nicht in einer Pipeline oder vollständig automatisierten Lösung verwendet werden. Wenn Sie dieses Skript bereitstellen, müssen Sie den Zugriff manuell vom IAM Identity Center autorisieren. Das Skript wird dann automatisch fortgesetzt.

Produktversionen

- Für alle Betriebssysteme wird empfohlen, Version PowerShell 7.0 oder höher zu verwenden.

Architektur

Sie können das Skript in diesem Muster verwenden, um mehrere IAM Identity Center-Anmeldeinformationen gleichzeitig zu aktualisieren, und Sie können eine Datei mit Anmeldeinformationen für die Verwendung mit AWS CLI, AWS SDKs oder AWS CDK erstellen.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS IAM Identity Center hilft Ihnen dabei, den SSO-Zugriff (Single Sign-On) auf alle Ihre AWS-Konten und Cloud-Anwendungen zentral zu verwalten.
- AWS-Tools für PowerShell sind eine Reihe von PowerShell Modulen, mit denen Sie Skriptoperationen für Ihre AWS-Ressourcen über die PowerShell Befehlszeile ausführen können.

Andere Tools

- PowerShell ist ein Microsoft-Automatisierungs- und Konfigurationsmanagementprogramm, das unter Windows, Linux und macOS ausgeführt wird.

Bewährte Methoden

Behalten Sie eine Kopie dieses Skripts für jede IAM-Identity-Center-Instance bei. Die Verwendung eines Skripts für mehrere Instances wird nicht unterstützt.

Polen

Ausführen des SSO-Skripts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das SSO-Skript an.	1. Kopieren Sie das SSO-Skript im Abschnitt Zusätzliche Informationen. 2. Definieren Sie im `Param` Abschnitt für Ihre AWS-Umgebung die Werte für die folgenden Variablen:	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `DefaultRoleName` – Die IAM-Rolle oder der Berechtigungssatz, die/der standardmäßig verwendet werden soll. • `Region` – Die AWS-Region, in der IAM Identity Center bereitgestellt wird. Eine vollständige Liste der Regionen und ihrer Codes finden Sie unter Regionale Endpunkte. • `StartUrl` – Die URL, die für den Zugriff auf Ihre IAM-Identity-Center-Anmeldeseite verwendet wird. Verwenden Sie dasselbe Format wie der Beispielwert im Skript. • `EnvironmentName` – Ein Kurzname, der auf diese Kopie des Skripts verweist und verwendet werden soll, wenn Sie mehrere Skriptkopien in derselben Sitzung ausführen. 3. Bearbeiten Sie in Zeile 10, die liest `# Add your Account Information`, die folgenden Werte in den Hash-Tabellen, um	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre Umgebung widerzuspiegeln: • `Profile` – Der AWS CLI-Profilname, in dem die temporären Anmeldeinformationen gespeichert werden sollen. • `AccountId` – Die ID des AWS-Kontos, für das Sie Anmeldeinformationen abrufen. • `RoleName` – Der Name der IAM-Identity-Center-Rolle oder des Berechtigungssatzes, den Sie verwenden möchten. Sie können dies so belassen `$DefaultRoleName`, als ob Sie dieselbe Rolle verwenden möchten, die Sie im `Param` Abschnitt definiert haben. Jede Zeile in der Hash-Tabelle muss mit einem Komma enden, mit Ausnahme der letzten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie das SSO-Skript aus.	Es wird empfohlen, Ihr benutzerdefiniertes Skript in der PowerShell Shell mit dem folgenden Befehl auszuführen.
	`./Set-AwsCliSsoCredentials.ps1`
	Alternativ können Sie das Skript von einer anderen Shell aus ausführen, indem Sie den folgenden Befehl eingeben.
	`pwsh Set-AwsCliSsoCredentials.ps1`
		Cloud-Administrator

Fehlerbehebung

Problem	Lösung
`No Access`-Fehler	Die IAM-Rolle, die Sie verwenden, verfügt nicht über Berechtigungen für den Zugriff auf die Rolle oder den Berechtigungssatz, den Sie in einem `RoleName` Parameter definiert haben. Aktualisieren Sie die Berechtigungen für die Rolle, die Sie verwenden, oder definieren Sie eine andere Rolle oder einen anderen Berechtigungssatz im Skript.

Zugehörige Ressourcen

- Wo werden Konfigurationseinstellungen gespeichert? (AWS-CLI-Dokumentation)

- Konfigurieren der AWS CLI für die Verwendung von AWS IAM Identity Center (AWS CLI-Dokumentation)
- Verwenden benannter Profile (AWS-CLI-Dokumentation)

Zusätzliche Informationen

SSO-Skript

Ersetzen Sie im folgenden Skript Platzhalter in spitzen Klammern (**<>**) durch Ihre eigenen Informationen und entfernen Sie die spitzen Klammern.

```
Set-AwsCliSsoCredentials.ps1
Param(
    $DefaultRoleName = '<AWSAdministratorAccess>',
    $Region          = '<us-west-2>',
    $StartUrl        = "<https://d-12345abcde.awsapps.com/start/>",
    $EnvironmentName = "<CompanyName>"
)
Try {$SsoAwsAccounts = (Get-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Scope
 Global -ErrorAction 'SilentlyContinue').Value.Clone()}
Catch {$SsoAwsAccounts = $False}
if (-not $SsoAwsAccounts) { $SsoAwsAccounts = @(
# Add your account information in the list of hash tables below, expand as necessary,
 and do not forget the commas
    @{Profile = "<Account1>"      ; AccountId = "<012345678901 >"; RoleName =
 $DefaultRoleName },
    @{Profile = "<Account2>"      ; AccountId = "<123456789012>"; RoleName =
 "<AWSReadOnlyAccess>" }
)}
$ErrorActionPreference = "Stop"
if (-not (Test-Path ~\.aws))      { New-Item ~\.aws -type Directory }
if (-not (Test-Path ~\.aws\credentials)) { New-Item ~\.aws\credentials -type File }
$CredentialFile = Resolve-Path ~\.aws\credentials
$PsuedoCreds    = @{AccessKey =
 'AKAEXAMPLE123ACCESS';SecretKey='PsuedoS3cret4cceSSKey123PsuedoS3cretKey'} # Pseudo
 Creds, do not edit.
Try {$SSOTokenExpire = (Get-Variable -Scope Global -Name
 "$($EnvironmentName)SSOTokenExpire" -ErrorAction 'SilentlyContinue').Value} Catch
 {$SSOTokenExpire = $False}
Try {$SSOToken       = (Get-Variable -Scope Global -Name "$($EnvironmentName)SSOToken"
 -ErrorAction 'SilentlyContinue').Value }      Catch {$SSOToken       = $False}
if ( $SSOTokenExpire -lt (Get-Date) ) {
```

```
    $SSOToken = $Null
    $Client   = Register-SSOOIDCClient -ClientName cli-sso-client -ClientType public -
Region $Region @PsuedoCreds
    $Device   = $Client | Start-SSOOIDCDeviceAuthorization -StartUrl $StartUrl -Region
 $Region @PsuedoCreds
    Write-Host "A Browser window should open. Please login there and click ALLOW." -
NoNewline
    Start-Process $Device.VerificationUriComplete
    While (-Not $SSOToken){
        Try {$SSOToken = $Client | New-SSOOIDCToken -DeviceCode $Device.DeviceCode -
GrantType "urn:ietf:params:oauth:grant-type:device_code" -Region $Region @PsuedoCreds}
        Catch {If ($_.Exception.Message -notlike "*AuthorizationPendingException*")
{Write-Error $_.Exception} ; Start-Sleep 1}
    }
    $SSOTokenExpire = (Get-Date).AddSeconds($SSOToken.ExpiresIn)
    Set-Variable -Name "$($EnvironmentName)SSOToken" -Value $SSOToken -Scope Global
    Set-Variable -Name "$($EnvironmentName)SSOTokenExpire" -Value $SSOTokenExpire -
Scope Global
}
$CredsTime     = $SSOTokenExpire - (Get-Date)
$CredsTimeText = ('{0:D2}:{1:D2}:{2:D2} left on SSO Token' -f $CredsTime.Hours,
 $CredsTime.Minutes, $CredsTime.Seconds).TrimStart("0 :")
for ($i = 0; $i -lt $SsoAwsAccounts.Count; $i++) {
    if (([DateTimeOffset]::FromUnixTimeSeconds($SsoAwsAccounts[$i].CredsExpiration /
 1000)).DateTime -lt (Get-Date).ToUniversalTime()) {
        Write-host "`r
    `rRegistering Profile $($SsoAwsAccounts[$i].Profile)" -NoNewline
        $TempCreds = $SSOToken | Get-SSORoleCredential -AccountId
 $SsoAwsAccounts[$i].AccountId -RoleName $SsoAwsAccounts[$i].RoleName -Region $Region
 @PsuedoCreds
        [PSCustomObject]@{AccessKey = $TempCreds.AccessKeyId; SecretKey =
 $TempCreds.SecretAccessKey; SessionToken = $TempCreds.SessionToken
        } | Set-AWSCredential -StoreAs $SsoAwsAccounts[$i].Profile -ProfileLocation
 $CredentialFile
        $SsoAwsAccounts[$i].CredsExpiration = $TempCreds.Expiration
    }
}
Set-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Value $SsoAwsAccounts.Clone() -
Scope Global
Write-Host "`r$($SsoAwsAccounts.Profile) Profiles registered, $CredsTimeText"
```

Verwenden von AWS Config zur Überwachung von Amazon Redshift-Sicherheitskonfigurationen

Erstellt von Lucas Kauffman (AWS) und abhishek Sengar (AWS)

Code-Repository: awslabs/aws-config-rules	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance
AWS-Services: AWS Config; Amazon Redshift; AWS Lambda		

Übersicht

Mit AWS Config können Sie die Sicherheitskonfigurationen für Ihre AWS-Ressourcen auswerten. AWS Config kann die Ressourcen überwachen. Wenn Konfigurationseinstellungen gegen Ihre definierten Regeln verstoßen, kennzeichnet AWS Config die Ressource als nicht konform.

Sie können AWS Config verwenden, um Ihre Amazon-Redshift-Cluster und -Datenbanken auszuwerten und zu überwachen. Weitere Informationen zu Sicherheitsempfehlungen und -funktionen finden Sie unter Sicherheit in Amazon Redshift. Dieses Muster enthält benutzerdefinierte AWS Lambda-Regeln für AWS Config . Sie können diese Regeln in Ihrem Konto bereitstellen, um die Sicherheitskonfigurationen Ihrer Amazon-Redshift-Cluster und -Datenbanken zu überwachen. Die Regeln in diesem Muster helfen Ihnen, AWS Config zu verwenden, um Folgendes zu bestätigen:

- Prüfungsprotokollierung ist für die Datenbanken im Amazon-Redshift-Cluster aktiviert
- SSL ist erforderlich, um eine Verbindung zum Amazon-Redshift-Cluster herzustellen
- Federal Information Processing Standards (FIPS)-Verschlüsselungen werden verwendet
- Datenbanken im Amazon-Redshift-Cluster sind verschlüsselt
- Überwachung der Benutzeraktivität ist aktiviert

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Config muss in Ihrem AWS-Konto aktiviert sein. Weitere Informationen finden Sie unter Einrichten von AWS Config mit der Konsole oder Einrichten von AWS Config mit der AWS CLI.
- Python Version 3.9 oder höher muss für den AWS Lambda-Handler verwendet werden. Weitere Informationen finden Sie unter Arbeiten mit Python (AWS Lambda-Dokumentation).

Produktversionen

- Python Version 3.9 oder höher

Architektur

Zieltechnologie-Stack

- AWS Config

Zielarchitektur

1. AWS Config führt die benutzerdefinierte Regel regelmäßig aus.
2. Die benutzerdefinierte Regel ruft die Lambda-Funktion auf.
3. Die Lambda-Funktion prüft die Amazon-Redshift-Cluster auf nicht konforme Konfigurationen.
4. Die Lambda-Funktion meldet den Compliance-Status jedes Amazon Redshift-Clusters an AWS Config .

Automatisierung und Skalierung

Die benutzerdefinierten AWS Config-Regeln werden skaliert, um alle Amazon Redshift-Cluster in Ihrem Konto zu bewerten. Für die Skalierung dieser Lösung sind keine zusätzlichen Maßnahmen erforderlich.

Tools

AWS-Services

- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und wie sie konfiguriert sind. Auf diese Weise können Sie feststellen, wie Ressourcen miteinander in Beziehung stehen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Redshift ist ein verwalteter Data Warehouse-Service im Petabyte-Bereich in der AWS Cloud.

Code-Repository

Der Code für dieses Muster ist im GitHub aws-config-rulesRepository verfügbar. Die benutzerdefinierten Regeln in diesem Repository sind Lambda-Regeln in der Programmiersprache Python. Dieses Repository enthält viele benutzerdefinierte Regeln für AWS Config . In diesem Muster werden nur die folgenden Regeln verwendet:

- `REDSHIFT_AUDIT_ENABLED` – Vergewissern Sie sich, dass die Prüfungsprotokollierung auf dem Amazon-Redshift-Cluster aktiviert ist. Wenn Sie auch bestätigen möchten, dass die Überwachung der Benutzeraktivitäten aktiviert ist, stellen Sie stattdessen die `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED` Regel bereit.
- `REDSHIFT_SSL_REQUIRED` – Vergewissern Sie sich, dass SSL erforderlich ist, um eine Verbindung zum Amazon-Redshift-Cluster herzustellen. Wenn Sie auch bestätigen möchten, dass FIPS-Verschlüsselungen (Federal Information Processing Standards) verwendet werden, stellen Sie stattdessen die `REDSHIFT_FIPS_REQUIRED` Regel bereit.
- `REDSHIFT_FIPS_REQUIRED` – Vergewissern Sie sich, dass SSL erforderlich ist und FIPS-Verschlüsselungen verwendet werden.
- `REDSHIFT_DB_ENCRYPTED` – Vergewissern Sie sich, dass die Datenbanken im Amazon-Redshift-Cluster verschlüsselt sind.
- `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED` – Vergewissern Sie sich, dass die Prüfungsprotokollierung und die Überwachung von Benutzeraktivitäten aktiviert ist.

Polen

Vorbereiten der Bereitstellung der Regeln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM-Richtlinien.	1. Erstellen Sie eine benutzerdefinierte identitätsbasierte IAM-Richtlinie, die es der Lambda-Ausführungsrolle ermöglicht, die Amazon-Redshift-Clusterkonfigurationen zu lesen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf -Ressourcen (Amazon-Redshift-Dokumentation) und Erstellen von IAM-Richtlinien (IAM-Dokumentation). `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "redshift:DescribeClusterParameterGroups", "redshift:DescribeClusterParameters", "redshift:DescribeClusters", "redshift:DescribeClusterSecurityGroups",`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"redshift
	:DescribeClusterSn
	apshots",
	"redshift
	:DescribeClusterSu
	bnetGroups",
	"redshift
	:DescribeEventSubs
	criptions",
	"redshift
	:DescribeLoggingSt
	atus"
	],
	"Resource":
	"*"
	}
	]
	}</pre> 2. Weisen Sie die AWSConfig RulesExecutionRole verwalteten Richtlinien AWSLambdaExecute und als Berechtigungsrichtlinie für die Lambda-Ausführungsrolle zu. Anweisungen finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (IAM-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie in einer Bash-Shell den folgenden Befehl aus. Dadurch wird das aws-config-rulesRepository von geklont GitHub. `git clone https://github.com/awslabs/aws-config-rules.git`	Allgemeines AWS

Bereitstellen der Regeln in AWS Config

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Regeln in AWS Config bereit.	Befolgen Sie die Anweisungen unter Erstellen von benutzerdefinierten Lambda-Regeln (AWS Config-Dokumentation) und stellen Sie eine oder mehrere der folgenden Regeln in Ihrem Konto bereit: • `REDSHIFT_AUDIT_ENABLED` • `REDSHIFT_SSL_REQUIRED` • `REDSHIFT_FIPS_REQUIRED` • `REDSHIFT_DB_ENCRYPTED` • `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob die Regeln funktionieren.	Folgen Sie nach der Bereitstellung der Regeln den Anweisungen unter Auswerten Ihrer Ressourcen (AWS Config-Dokumentation), um zu bestätigen, dass AWS Config Ihre Amazon Redshift-Ressourcen korrekt auswertet.	Allgemeines AWS

Zugehörige Ressourcen

AWS-Servicedokumentation

- Sicherheit in Amazon Redshift (Amazon-Redshift-Dokumentation)
- Verwalten der Datenbanksicherheit (Amazon-Redshift-Dokumentation)
- Benutzerdefinierte AWS Config-Regeln (AWS Config-Dokumentation)

AWS Prescriptive Guidance

- Stellen Sie sicher, dass neue Amazon-Redshift-Cluster über erforderliche SSL-Endpunkte verfügen
- Sicherstellen, dass ein Amazon-Redshift-Cluster bei der Erstellung verschlüsselt wird

Zusätzliche Informationen

Sie können die folgenden von AWS verwalteten Regeln in AWS Config verwenden, um die folgenden Sicherheitskonfigurationen für Amazon Redshift zu bestätigen:

- redshift-cluster-configuration-check – Verwenden Sie diese Regel, um zu bestätigen, dass die Prüfungsprotokollierung für die Datenbanken im Amazon-Redshift-Cluster aktiviert ist, und um zu bestätigen, dass die Datenbanken verschlüsselt sind.
- redshift-require-tls-ssl – Verwenden Sie diese Regel, um zu bestätigen, dass SSL erforderlich ist, um eine Verbindung zum Amazon-Redshift-Cluster herzustellen.

Verwenden Sie die Network Firewall, um die DNS-Domänennamen von der Server Name Indication (SNI) für ausgehenden Datenverkehr zu erfassen

Erstellt von Kirankumar Chandrashekar (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Sicherheit, Identität, Compliance; Netzwerke; Web- und mobile Apps	Arbeitslast: Alle anderen Workloads
AWS-Services: AWS Lambda; AWS-Netzwerk-Firewall; Amazon VPC; Amazon-Protokolle CloudWatch		

Übersicht

Dieses Muster zeigt Ihnen, wie Sie die Amazon Web Services (AWS) Network Firewall verwenden, um die DNS-Domainnamen zu sammeln, die von der Server Name Indication (SNI) im HTTPS-Header Ihres ausgehenden Netzwerkverkehrs bereitgestellt werden. Network Firewall ist ein verwalteter Service, der es einfach macht, wichtige Netzwerkschutzmaßnahmen für Amazon Virtual Private Cloud (Amazon VPC) bereitzustellen, einschließlich der Fähigkeit, ausgehenden Datenverkehr mit einer Firewall zu sichern, die Pakete blockiert, die bestimmte Sicherheitsanforderungen nicht erfüllen. Die Sicherung des ausgehenden Datenverkehrs zu bestimmten DNS-Domainnamen wird als Ausgangsfilterung bezeichnet. Dabei handelt es sich um eine Methode, bei der der Fluss ausgehender Informationen von einem Netzwerk in ein anderes überwacht und möglicherweise eingeschränkt wird.

Nachdem Sie die SNI-Daten erfasst haben, die die Network Firewall passieren, können Sie Amazon CloudWatch Logs und AWS Lambda verwenden, um die Daten in einem Amazon Simple Notification Service (Amazon SNS) -Thema zu veröffentlichen, das E-Mail-Benachrichtigungen generiert. Die E-Mail-Benachrichtigungen enthalten den Servernamen und andere relevante SNI-Informationen. Darüber hinaus können Sie die Ausgabe dieses Musters verwenden, um ausgehenden Datenverkehr anhand des Domainnamens im SNI mithilfe von Firewallregeln zuzulassen oder einzuschränken.

Weitere Informationen finden Sie unter Arbeiten mit statusbehafteten Regelgruppen in der AWS-Netzwerk-Firewall in der Dokumentation zur Network Firewall.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows
- Network Firewall, eingerichtet und konfiguriert in Amazon VPC und wird zur Überprüfung des ausgehenden Datenverkehrs verwendet

Hinweis: Die Network Firewall kann jede der folgenden VPC-Konfigurationen verwenden:

- Einfache Einzelzonenarchitektur mit einem Internet-Gateway
- Mehrzonenarchitektur mit einem Internet-Gateway
- Architektur mit einem Internet-Gateway und einem NAT-Gateway

Architektur

Das folgende Diagramm zeigt, wie die Network Firewall verwendet wird, um SNI-Daten aus ausgehendem Netzwerkverkehr zu sammeln und diese Daten dann mithilfe von CloudWatch Logs und Lambda in einem SNS-Thema zu veröffentlichen.

Das Diagramm zeigt den folgenden Workflow:

1. Die Network Firewall erfasst Domainnamen aus den SNI-Daten im HTTPS-Header Ihres ausgehenden Netzwerkverkehrs.
2. CloudWatch Logs überwacht die SNI-Daten und ruft eine Lambda-Funktion auf, wenn der ausgehende Netzwerkverkehr die Network Firewall passiert.
3. Die Lambda-Funktion liest die von CloudWatch Logs erfassten SNI-Daten und veröffentlicht diese Daten dann in einem SNS-Thema.
4. Das SNS-Thema sendet Ihnen eine E-Mail-Benachrichtigung, die die SNI-Daten enthält.

Automatisierung und Skalierung

- Sie können AWS verwenden CloudFormation, um dieses Muster zu erstellen, indem Sie Infrastruktur als Code verwenden.

Technologie-Stack

- CloudWatch Amazon-Protokolle
- Amazon SNS
- Amazon VPC
- AWS Lambda
- AWS Network Firewall

Tools

AWS-Services

- Amazon CloudWatch Logs — Sie können Amazon CloudWatch Logs verwenden, um Ihre Protokolldateien von Amazon Elastic Compute Cloud (Amazon EC2) -Instances, AWS CloudTrail, Amazon Route 53 und anderen Quellen zu überwachen, zu speichern und darauf zuzugreifen.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) stellt einen logisch isolierten Bereich der AWS-Cloud bereit, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.
- AWS Lambda — AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten.
- AWS Network Firewall — Die AWS Network Firewall ist ein verwalteter Service, mit dem Sie auf einfache Weise wichtige Netzwerkschutzmaßnahmen für all Ihre Amazon-VPCs bereitstellen können.

Epen

Erstellen Sie eine CloudWatch Protokollgruppe für die Network Firewall

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudWatch Protokollgruppe.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch Konsole. 2. Wählen Sie im Navigationsbereich Protokollgruppen aus. 3. Wählen Sie Actions (Aktionen) und anschließend Create log group (Protokollgruppe erstellen) aus. 4. Geben Sie einen Namen für die Protokollgruppe ein. Wählen Sie anschließend Create log group (Protokollgruppe erstellen) aus. Weitere Informationen finden Sie in der CloudWatch Dokumentation unter Arbeiten mit Protokollgruppen und Protokollströmen.	Cloud-Administrator

Erstellen Sie ein SNS-Thema und ein Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Um ein SNS-Thema zu erstellen, folgen Sie den Anweisungen in der Amazon SNS SNS-Dokumentation.	Cloud-Administrator
Abonnieren Sie einen Endpunkt für das SNS-Thema.	Um eine E-Mail-Adresse als Endpunkt für das von Ihnen erstellte SNS-Thema zu abonnieren, folgen Sie den Anweisungen in der Amazon SNS SNS-Dokumentation. Wählen Sie unter Protokoll die Option Email/Email-JSON aus. Hinweis: Sie können je nach Ihren Anforderungen auch einen anderen Endpunkt auswählen.	Cloud-Administrator

Logging in der Network Firewall einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Firewall-Protokollierung.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter NETWORK FIREWALL die Option Firewalls aus. 3. Wählen Sie im Abschnitt Firewalls die Firewall aus,	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für die Sie den Servernamen vom SNI für ausgehenden Datenverkehr erfassen möchten. 4. Wählen Sie die Registerkarte Firewall-Details und dann im Abschnitt Protokollierung die Option Bearbeiten aus. 5. Wählen Sie als Protokolltyp die Option Warnung aus. Wählen Sie unter Protokollziel für Warnungen die Option CloudWatch Protokollgruppe aus. 6. Suchen Sie unter CloudWatch Protokollgruppe nach der Protokollgruppe, die Sie zuvor erstellt haben, wählen Sie sie aus, und klicken Sie dann auf Speichern. Weitere Informationen zur Verwendung von CloudWatch Logs als Protokollziel für die Network Firewall finden Sie unter Amazon CloudWatch Logs in der Dokumentation zur Network Firewall.	

Richten Sie eine statusbehaftete Regel in der Network Firewall ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Stateful-Regel.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Netzwerkfirewall-Regelgruppen aus. 3. Wählen Sie „Netzwerk-Firewall-Regelgruppe erstellen“. 4. Wählen Sie auf der Seite „Netzwerk-Firewall-Regelgruppe erstellen“ als Regelgruppentyp die Option Stateful-Regelgruppe aus. Hinweis: Weitere Informationen finden Sie unter Arbeiten mit statusbehafteten Regelgruppen in der AWS-Netzwerk-Firewall. 5. Geben Sie im Abschnitt Stateful-Regelgruppe einen Namen und eine Beschreibung für die Regelgruppe ein. 6. Geben Sie unter Kapazität die maximale Kapazität an, die Sie für die statusbehaftete Regelgruppe zulassen möchten (bis zum	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Maximum von 30.000). Hinweis: Sie können diese Einstellung nicht ändern, nachdem Sie die Regelgruppe erstellt haben. Informationen zur Berechnung der Kapazität finden Sie unter Einstellung der Regelgruppenkapazität in der AWS-Netzwerk-Firewall. Informationen zur Maximaleinstellung finden Sie unter AWS-Netzwerk-Firewall-Kontingente. 7. Wählen Sie für Stateful-Regelgruppenoptionen die Option 5-Tuple aus. 8. Wählen Sie im Abschnitt Reihenfolge der Stateful-Regeln die Option Standard aus. 9. Behalten Sie im Abschnitt Regelvariablen die Standardwerte bei. 10. Wählen Sie im Abschnitt Regel hinzufügen die Option TLS als Protokoll aus. Wählen Sie als Quelle die Option Beliebig aus. Wählen Sie für Quellport die Option Beliebiger Port aus. Wählen Sie als Ziel die Option Beliebig aus. Wählen Sie für Zielport	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Option Beliebiger Port aus. Wählen Sie für Verkehrsrichtung die Option Forward aus. Wählen Sie für Aktion die Option Warnung aus. Wählen Sie Regel hinzufügen aus. 11. Wählen Sie Stateful-Regelgruppe erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die statusbehaftete Regel der Network Firewall zu.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter NETWORK FIREWALL die Option Firewalls aus. 3. Wählen Sie die Firewall aus, in der Sie den Servernamen vom SNI für ausgehenden Datenverkehr erfassen möchten. 4. Wählen Sie im Abschnitt Stateful-Regelgruppen die Option Aktionen und dann Unverwaltete statusbehaftete Regelgruppen hinzufügen aus. 5. Wählen Sie auf der Seite Nicht verwaltete statusbehaftete Regelgruppen hinzufügen die statusbehaftete Regelgruppe aus, die Sie zuvor erstellt haben, und klicken Sie dann auf Stateful-Regelgruppe hinzufügen.	Cloud-Administrator

Erstellen Sie eine Lambda-Funktion zum Lesen der Protokolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Code für die Lambda-Funktion.	Fügen Sie in einer integrierten Entwicklungsumgebung (IDE), die das CloudWatch Logs-Ereignis von der Network Firewall für ausgehenden Datenverkehr lesen kann, den folgenden Python-3-Code ein und `<SNS-topic-ARN>` ersetzen Sie ihn durch Ihren Wert:
	`import json`
	`import gzip`
	`import base64`
	`import boto3`
	`sns_client = boto3.client('sns')`
	`def lambda_handler(event, context):`
	`  decoded_event = json.loads(gzip.decompress(base64.b64decode(event['awslogs']['data'])))`
	`  body = '''`
	`  {filtermatch}`
	`  '''.format(`
	`  loggroup=decoded_event['logGroup'],`
	`  logstream=decoded_event['logStream'],`
	`  filtermatch=decoded_event['logEvents'][0]['message'],`
	`  )`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	print(body)
	filterMatch = json.loads(body)
	data = []
	if 'http' in filterMatch['event']:
	data.append(filterMatch['event']['http']['hostname'])
	elif 'tls' in filterMatch['event']:
	data.append(filterMatch['event']['tls']['sni'])
	result = 'Domain accessed ' + 1*' ' + (data[0]) + 1*' ' 'via AWS Network Firewall ' + 1*' ' + (filterMatch['firewall_name'])
	print(result)
	message = {'ServerName': result}
	send_to_sns = sns_client.publish(
	TargetArn=<SNS-topic-ARN>,
	#Replace with the SNS topic ARN
	Message=json.dumps({'default': json.dumps(message),
	'sms': json.dumps(message),
	'email': json.dumps(message)}),
	Subject='Server Name passed through the Network Firewall',	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>MessageSt
	ructure='json'
	)</pre>
	In diesem Codebeispiel wird der Inhalt der CloudWatch Protokolle analysiert und der vom SNI im HTTPS-Header angegebene Servername erfasst.	

So erstellen Sie die Lambda-Funktion:	Um die Lambda-Funktion zu erstellen, folgen Sie den Anweisungen in der Lambda-Dokumentation und wählen Sie Python 3.9 für Runtime.	Cloud-Administrator
Fügen Sie den Code zur Lambda-Funktion hinzu.	Folgen Sie den Anweisungen in der Lambda-Dokumentation, um Ihren Python-Code zu der zuvor erstellten Lambda-Funktion hinzuzufügen.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie CloudWatch Logs als Trigger zur Lambda-Funktion hinzu.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Lambda-Konsole. 2. Wählen Sie im Navigationsbereich Funktionen und dann die Funktion aus, die Sie zuvor erstellt haben. 3. Wählen Sie im Abschnitt Funktionsübersicht die Option Auslöser hinzufügen aus. 4. Wählen Sie auf der Seite Trigger hinzufügen im Abschnitt Trigger-Konfiguration die Option CloudWatch Logs und dann Add aus. 5. Wählen Sie unter Protokollgruppe die CloudWatch Protokollgruppe aus, die Sie zuvor erstellt haben. 6. Geben Sie unter Filtername einen Namen für Ihren Filter ein. 7. Wählen Sie Hinzufügen aus. 8. Wählen Sie auf der Seite Ihrer Funktion auf der Registerkarte Konfiguration im Abschnitt Trigger den Trigger aus, den Sie gerade hinzugefügt haben, und	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Aktivieren aus. Weitere Informationen finden Sie unter Using Lambda with CloudWatch Logs in der Lambda-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie SNS-Veröffentlichungsberechtigungen hinzu.	Fügen Sie der Lambda-Ausführungsrolle die Berechtigung sns:publish hinzu, sodass Lambda API-Aufrufe zum Veröffentlichen von Nachrichten in SNS tätigen kann. 1. Suchen Sie die Ausführungsrolle der Lambda-Funktion, die Sie zuvor erstellt haben. 2. Fügen Sie Ihrer AWS Identity and Access Management (IAM) -Rolle die folgende Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "AllowSNSPublish", "Effect": "Allow", "Action": [ "sns:GetTopicAttributes", "sns:Subscribe", "sns:Unsubscribe", "sns:Publish" ],`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Resource": "*"
	}
	]
	}</pre>	

Testen Sie die Funktionalität Ihrer SNS-Benachrichtigung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie den Datenverkehr über die Network Firewall.	1. Senden oder warten Sie, bis der HTTPS-Verkehr die Network Firewall passiert.
	2. Überprüfen Sie die SNS-Benachrichtigungs-E-Mail, die Sie von AWS erhalten, wenn der Datenverkehr die Network Firewall passiert. Die E-Mail enthält die SNI-Details für ausgehenden Datenverkehr. Die aus dem obigen Lambda-Code generierte E-Mail hat beispielsweise den folgenden Inhalt, wenn der aufgerufene Domainnam e https://aws.amazon.com lautet und das Abonnemen tprotokoll EMAIL-JSON lautet:
	<pre>{
	"Type": "Notifica tion",</pre>
		Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"MessageId": "<messageID>", "TopicArn": "arn:aws:sns:us-west-2:123456789:testSNSTopic", "Subject": "Server Name passed through the Network Firewall", "Message": "{\"ServerName\": \"Domain 'aws.amazon.com' accessed via AWS Network Firewall 'AWS-Network-Firewall-Multi-AZ-firewall\"}", "Timestamp": "2022-03-22T04:10:04.217Z", "SignatureVersion": "1", "Signature": "<Signature>", "SigningCertURL": "<SigningCertUrl>", "UnsubscribeURL": "<UnsubscribeURL>" } Überprüfen Sie dann das Warnprotokoll der Network Firewall bei Amazon, CloudWatch indem Sie den Anweisungen in der CloudWatch Amazon-Dokumentation folgen. Das Warnungsprotokoll zeigt die folgende Ausgabe:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	{
	"firewall_name": "AWS-Network-Firewall-Multi-AZ-firewall",
	"availability_zone": "us-east-2b",
	"event_timestamp": "<event timestamp>",
	"event": {
	"timestamp": "2021-03-22T04:10:04.214222+0000",
	"flow_id": <flow ID>,
	"event_type": "alert",
	"src_ip": "10.1.3.76",
	"src_port": 22761,
	"dest_ip": "99.86.59.73",
	"dest_port": 443,
	"proto": "TCP",
	"alert": {
	"action": "allowed",
	"signature_id": 2,
	"rev": 0,
	"signature": "",
	"category": "",
	"severity": 3
	},
	"tls": {	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"subject": "CN=aws.amazon.com", "issuerdn": "C=US, O=Amazon, OU=Server CA 1B, CN=Amazon", "serial": "<serial number>", "fingerprint": "<fingerprint ID>", "sni": "aws.amazon.com", "version": "TLS 1.2", "notbefore": "2020-09-30T00:00:00", "notafter": "2021-09-23T12:00:00", "ja3": {}, "ja3s": {} }, "app_proto": "tls" } }	

Verwenden von Terraform zum automatischen Aktivieren von Amazon GuardDuty für eine Organisation

Erstellt von Aarthi Kannan (AWS)

Code-Repository: –amazon-guardduty-for-awsorganizations-with-terraform	Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Cloudnativ; DevOps
Workload: Alle anderen Workloads	AWS-Services: Amazon GuardDuty; AWS Organizations	

Übersicht

Amazon überwacht GuardDuty kontinuierlich Ihre Amazon Web Services (AWS)-Konten und verwendet Bedrohungsinformationen, um unerwartete und potenziell bösartige Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Die manuelle Aktivierung GuardDuty für mehrere Konten oder Organisationen, über mehrere AWS-Regionen oder über die AWS-Managementkonsole kann umständlich sein. Sie können den Prozess automatisieren, indem Sie ein Infrastructure as Code (IaC)-Tool wie Terraform verwenden, das -Services und -Ressourcen mit mehreren Konten und Regionen in der Cloud bereitstellen und verwalten kann.

AWS empfiehlt die Verwendung von AWS Organizations zum Einrichten und Verwalten mehrerer Konten in GuardDuty. Dieses Muster entspricht dieser Empfehlung. Ein Vorteil dieses Ansatzes besteht darin, dass beim Erstellen oder Hinzufügen neuer Konten zur Organisation in diesen Konten für alle unterstützten Regionen automatisch aktiviert GuardDuty wird, ohne dass ein manuelles Eingreifen erforderlich ist.

Dieses Muster zeigt, wie Sie HashiCorp Terraform verwenden, um Amazon GuardDuty für drei oder mehr Amazon Web Services (AWS)-Konten in einer Organisation zu aktivieren. Der mit diesem Muster bereitgestellte Beispielcode führt Folgendes aus:

- Aktiviert GuardDuty für alle AWS-Konten, die aktuelle Mitglieder der Zielorganisation in AWS Organizations sind

- Aktiviert die Auto-Enable-Funktion in GuardDuty, die automatisch GuardDuty für alle Konten aktiviert, die der Zielorganisation zukünftig hinzugefügt werden
- Ermöglicht Ihnen die Auswahl der Regionen, in denen Sie aktivieren möchten GuardDuty
- Verwendet das Sicherheitskonto der Organisation als GuardDuty delegierten Administrator
- Erstellt einen Amazon Simple Storage Service (Amazon S3)-Bucket im Protokollierungskonto und konfiguriert GuardDuty so, dass die aggregierten Ergebnisse aus allen Konten in diesem Bucket veröffentlicht werden
- Weist standardmäßig eine Lebenszyklusrichtlinie zu, die Ergebnisse nach 365 Tagen aus dem S3-Bucket in den Speicher Amazon S3 Glacier Flexible Retrieval überführt

Sie können diesen Beispielcode manuell ausführen oder in Ihre Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) integrieren.

Zielgruppe

Dieses Muster wird für Benutzer empfohlen, die Erfahrung mit Terraform, Python GuardDutyund AWS Organizations haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Organisation ist in AWS Organizations eingerichtet und enthält mindestens die folgenden drei Konten:
  - Ein Verwaltungskonto – Dies ist das Konto, von dem aus Sie den Terraform-Code bereitstellen, entweder eigenständig oder als Teil der CI/CD-Pipeline. Der Terraform-Status wird auch in diesem Konto gespeichert.
  - Ein Sicherheitskonto – Dieses Konto wird als GuardDuty delegierter Administrator verwendet. Weitere Informationen finden Sie unter Wichtige Überlegungen für GuardDuty delegierte Administratoren (GuardDuty Dokumentation).
  - Ein Protokollierungskonto – Dieses Konto enthält den S3-Bucket, in dem die aggregierten Ergebnisse aus allen Mitgliedskonten GuardDuty veröffentlicht.

  Weitere Informationen zum Einrichten der Organisation mit der erforderlichen Konfiguration finden Sie unter Erstellen einer Kontostruktur (AWS Well-Architected Labs).

- Ein Amazon S3-Bucket und eine Amazon-DynamoDB-Tabelle, die als Remote-Backend dienen, um den Status von Terraform im Verwaltungskonto zu speichern. Weitere Informationen zur Verwendung von Remote-Backends für den Terraform-Status finden Sie unter S3-Backends (Terraform-Dokumentation). Ein Codebeispiel, das die Remote-Statusverwaltung mit einem S3-Backend einrichtet, finden Sie unter remote-state-s3-Backend (Terraform Registry). Beachten Sie die folgenden Voraussetzungen:
  - Der S3-Bucket und die DynamoDB-Tabelle müssen sich in derselben Region befinden.
  - Beim Erstellen der DynamoDB-Tabelle muss der Partitionsschlüssel `LockID` (wobei die Groß- und Kleinschreibung beachtet werden muss) und der Partitionsschlüsseltyp muss Zeichenfolge sein. Alle anderen Tabelleneinstellungen müssen ihre Standardwerte haben. Weitere Informationen finden Sie unter Über Primärschlüssel und Erstellen einer Tabelle (DynamoDB-Dokumentation).
- Ein S3-Bucket, der zum Speichern von Zugriffsprotokollen für den S3-Bucket verwendet wird, in dem Ergebnisse GuardDuty veröffentlicht. Weitere Informationen finden Sie unter Aktivieren der Amazon S3-Serverzugriffsprotokollierung (AmazonS3-Dokumentation). Wenn Sie in einer Landing Zone von AWS Control Tower bereitstellen, können Sie den S3-Bucket im Protokollarchivkonto für diesen Zweck wiederverwenden.
- Terraform Version 0.14.6 oder höher ist installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte – AWS (Terraform-Dokumentation).
- Python Version 3.9.6 oder höher ist installiert und konfiguriert. Weitere Informationen finden Sie unter Quellversionen (Python-Website).
- AWS SDK for Python (Boto3) ist installiert. Weitere Informationen finden Sie unter Installation (Boto3-Dokumentation).
- jq ist installiert und konfiguriert. Weitere Informationen finden Sie unter Download jq (jq-Dokumentation).

Einschränkungen

- Dieses Muster unterstützt macOS- und Amazon Linux 2-Betriebssysteme. Dieses Muster wurde nicht für die Verwendung in Windows-Betriebssystemen getestet.
- GuardDuty darf nicht bereits in einem der Konten in einer der Zielregionen aktiviert sein.
- Die IaC-Lösung in diesem Muster erfüllt nicht die Voraussetzungen.
- Dieses Muster ist für eine AWS-Landing Zone konzipiert, die den folgenden bewährten Methoden entspricht:

- Die Landing Zone wurde mit AWS Control Tower erstellt.
- Separate AWS-Konten werden für Sicherheit und Protokollierung verwendet.

Produktversionen

- Terraform Version 0.14.6 oder höher. Der Beispielcode wurde für Version 1.2.8 getestet.
- Python Version 3.9.6 oder höher.

Architektur

Dieser Abschnitt bietet einen allgemeinen Überblick über diese Lösung und die Architektur, die durch den Beispielcode eingerichtet wird. Das folgende Diagramm zeigt die Ressourcen, die über die verschiedenen Konten in der Organisation innerhalb einer einzigen AWS-Region bereitgestellt werden.

1. Terraform erstellt die GuardDutyTerraformOrgRole AWS Identity and Access Management (IAM)-Rolle im Sicherheitskonto und im Protokollierungskonto.
2. Terraform erstellt einen S3-Bucket in der Standard-AWS-Region im Protokollierungskonto. Dieser Bucket wird als Veröffentlichungsziel verwendet, um alle GuardDuty Ergebnisse in allen Regionen und von allen Konten in der Organisation zu aggregieren. Terraform erstellt auch einen AWS Key Management Service (AWS KMS)-Schlüssel im Sicherheitskonto, der zum Verschlüsseln der Ergebnisse im S3-Bucket verwendet wird, und konfiguriert die automatische Archivierung der Ergebnisse aus dem S3-Bucket im Speicher S3 Glacier Flexible Retrieval.
3. Vom Verwaltungskonto aus bestimmt Terraform das Sicherheitskonto als delegierten Administrator für GuardDuty. Das bedeutet, dass das Sicherheitskonto jetzt den GuardDuty Service für alle Mitgliedskonten verwaltet, einschließlich des Verwaltungskontos. Einzelne Mitgliedskonten können sich nicht GuardDuty selbst aussetzen oder deaktivieren.
4. Terraform erstellt den GuardDuty Detektor im Sicherheitskonto für den GuardDuty delegierten Administrator.
5. Wenn es noch nicht aktiviert ist, aktiviert Terraform den S3-Schutz in GuardDuty. Weitere Informationen finden Sie unter Amazon S3-Schutz in Amazon GuardDuty (GuardDuty Dokumentation).

6. Terraform registriert alle aktuellen, aktiven Mitgliedskonten in der Organisation als GuardDuty Mitglieder.
7. Terraform konfiguriert den GuardDuty delegierten Administrator so, dass er die aggregierten Ergebnisse aus allen Mitgliedskonten im S3-Bucket im Protokollierungskonto veröffentlicht.
8. Terraform wiederholt die Schritte 3 bis 7 für jede AWS-Region, die Sie auswählen.

Automatisierung und Skalierung

Der bereitgestellte Beispielcode ist modularisiert, sodass Sie ihn in Ihre CI/CD-Pipeline für die automatisierte Bereitstellung integrieren können.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon GuardDuty ist ein kontinuierlicher Sicherheitsüberwachungsservice, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS-Umgebung zu identifizieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Key Management Service (AWS KMS) unterstützt Sie beim Erstellen und Steuern kryptografischer Schlüssel zum Schutz Ihrer Daten.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS SDK for Python (Boto3) ist ein Software Development Kit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr -Skript in AWS-Services integrieren können.

Andere Tools und Services

- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie Code für die Bereitstellung und Verwaltung von Cloud-Infrastrukturen und -Ressourcen verwenden können.

- Python ist eine allgemeine Programmiersprache.
- jq ist ein Befehlszeilenprozessor, der Sie bei der Arbeit mit JSON-Dateien unterstützt.

Code-Repository

Der Code für dieses Muster ist auf GitHubim amazon-guardduty-for-aws-organizations-with-terraformRepository verfügbar.

Sekunden

Aktivieren von GuardDuty in der Organisation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie in einer Bash-Shell den folgenden Befehl aus. Unter Repository klonen im Abschnitt Zusätzliche Informationen können Sie den vollständigen Befehl kopieren, der die URL des GitHub Repositorys enthält. Dies klont das amazon-guardduty-for-aws-organizations-with-terraformRepository von GitHub. `git clone <github-repository-url>`	DevOps Techniker
Bearbeiten Sie die Terraform-Konfigurationsdatei.	1. Replizieren Sie im `root` Ordner des geklonten Repositorys die Datei configuration.json.sample, indem Sie den folgenden Befehl ausführen.	DevOps Ingenieur, Allgemeines AWS, Terraform, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cp configuration.json .sample configura tion.json` 2. Bearbeiten Sie die neue Datei configuration.json und definieren Sie die Werte für jede der folgenden Variablen: • `management_acc_id` – Konto-ID des Verwaltungskontos. • `delegated_admin_acc_id` – Konto-ID des Sicherheitskontos. • `logging_acc_id` – Konto-ID des Protokollierungskontos. • `target_regions` – Durch Kommata getrennte Liste der AWS-Regionen, in denen Sie aktivieren möchten GuardDuty. • `organization_id` – AWS Organizations-ID der Organisation, in der Sie aktivieren GuardDuty. • `default_region` – Die Region, in der Ihr Terraform-Status im Verwaltungskonto gespeichert ist. Dies	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist dieselbe Region, in der Sie den S3-Bucket und die DynamoDB-Tabelle für das Terraform -Backend bereitgestellt haben. • `role_to_assume_for_role_creation` – Name, den Sie einer neuen IAM-Rolle in den Sicherheits- und Protokollierungskonten zuweisen möchten. Sie erstellen diese neue Rolle in der nächsten Geschichte. Terraform übernimmt diese Rolle, um die `GuardDutyTerraformOrgRole` IAM-Rolle in den Sicherheits- und Protokollierungskonten zu erstellen. • `finding_publishing_frequency` – Häufigkeit, mit der Ergebnisse im S3-Bucket GuardDuty veröffentlicht. • `guardduty_findings_bucket_region` – Bevorzugte Region, in der Sie den S3-Bucket für veröffentlichte Ergebnisse erstellen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `logging_acc_s3_bucket_name` – Bevorzugter Name für den S3-Bucket für veröffentlichte Ergebnisse. • `security_acc_kms_key_alias` – AWS KMS-Alias für den Schlüssel, der zum Verschlüsseln von GuardDuty Ergebnissen verwendet wird. • `s3_access_log_bucket_name` – Name eines bereits vorhandenen S3-Buckets, in dem Sie Zugriffsprotokolle für den S3-Bucket erfassen möchten, der für GuardDuty Ergebnisse verwendet wird. Dieser Bucket sollte sich in derselben AWS-Region wie der GuardDuty Ergebnis-Bucket befinden. • `tfm_state_backend_s3_bucket` – Name des bereits vorhandenen S3-Buckets zum Speichern des Terraform-Remote-Backend-Status. • `tfm_state_backend_dynamodb_table` – Name der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereits vorhandenen DynamoDB-Tabelle zum Sperren des Terraform-Status. 3. Speichern und schließen Sie die -Konfigurationsdatei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie CloudFormation Vorlagen für neue IAM-Rollen.	Dieses Muster enthält eine IaC-Lösung zum Erstellen von zwei CloudFormation Vorlagen. Diese Vorlagen erstellen zwei IAM-Rollen, die Terraform während des Einrichtungsprozesses verwendet. Diese Vorlagen entsprechen der bewährten Sicherheitsmethode der geringsten Berechtigungen . 1. Navigieren Sie in einer Bash-Shell im Repository-`root`Ordner zu `cfn-templates/` . Dieser Ordner enthält CloudFormation Vorlagendateien mit Stubs. 2. Führen Sie den folgenden Befehl aus. Dadurch werden die Stubs durch die Werte ersetzt, die Sie in der Datei configuration.json angegeben haben. `bash scripts/replace_config_stubs.sh` 3. Vergewissern Sie sich, dass die folgenden CloudFormation Vorlagen im `cfn-templates/` Ordner erstellt wurden:	DevOps Ingenieur, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• management-account-role.yaml – Diese Datei enthält die Rollendefinition und die zugehörigen Berechtigungen für die IAM-Rolle im Verwaltungskonto, das über die Mindestberechtigungen verfügt, die zum Abschließen dieses Musters erforderlich sind. • role-to-assume-for-role-creation.yaml – Diese Datei enthält die Rollendefinition und die zugehörigen Berechtigungen für die IAM-Rolle in den Sicherheits- und Protokollierungskonten. Terraform übernimmt diese Rolle, um die GuardDutyTerraformOrgRole Rolle in diesen Konten zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rollen.	Befolgen Sie die Anweisungen unter Erstellen eines Stacks (CloudFormation Dokumentation) wie folgt: 1. Stellen Sie den Stack role-to-assume-for-role-creation.yaml sowohl in den Sicherheits- als auch in den Protokollierungskonten bereit. 2. Stellen Sie den management-account-role.yaml-Stack im Verwaltungskonto bereit. Wenn Sie den Stack erfolgreich erstellen und den `CREATE_COMPLETE` Stack-Status sehen, notieren Sie sich in der Ausgabe den Amazon-Ressourcennamen (ARN) dieser neuen Rolle.	DevOps Ingenieur, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übernehmen Sie die IAM-Rolle im Verwaltungskonto.	Als bewährte Sicherheitsmethode empfehlen wir Ihnen, die neue management-account-role IAM-Rolle zu übernehmen, bevor Sie fortfahren. Geben Sie in der AWS Command Line Interface (AWS CLI) den Befehl unter Übernehmen der IAM-Rolle des Verwaltungskontos im Abschnitt Zusätzliche Informationen ein.	DevOps Ingenieur, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Setup-Skript aus.	Führen Sie im Repositor y-`root`Ordner den folgenden Befehl aus, um das Setup-Skr ipt zu starten. `bash scripts/full-setup .sh` Das full-setup.sh-Skript führt die folgenden Aktionen aus: • Exportiert alle Konfigura tionswerte als Umgebungs variablen • Generiert die Codedateien backend.tf und terraform .tfvars für jedes Terraform-Modul • Aktiviert den vertrauen swürdigen Zugriff für GuardDuty in der Organisat ion über die AWS CLI. • Importiert den Organisat ionsstatus in den Terraform-Status • Erstellt den S3-Bucket zum Veröffentlichen von Ergebnissen im Protokoll ierungskonto • Erstellt den AWS KMS-Schlüssel zum Verschlüs seln von Ergebnissen im Sicherheitskonto	DevOps Ingenieur, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Aktiviert in der GuardDuty gesamten Organisation in allen ausgewählten Regionen, wie im Abschnitt Architektur beschrieben	

(Optional) Deaktivieren von GuardDuty in der Organisation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Bereinigungsskript aus.	Wenn Sie dieses Muster verwendet haben, um GuardDuty für die Organisation zu aktivieren, und deaktivieren möchten GuardDuty, führen Sie im Repository-`root`Ordner den folgenden Befehl aus, um das Skript cleanup-gd.sh zu starten. `bash scripts/cleanup-gd.sh` Dieses Skript wird GuardDuty in der Zielorganisation deaktiviert, entfernt alle bereitgestellten Ressourcen und stellt die Organisation auf den vorherigen Status wieder her, bevor Terraform zum Aktivieren von verwendet wird GuardDuty. Beachten Sie, dass dieses Skript die Terraform-Statusda	DevOps Ingenieur, Allgemeines AWS, Terraform, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	teien oder Sperrdateien nicht aus den lokalen und Remote-Backends entfernt. Wenn Sie dies tun müssen, müssen Sie diese Aktionen manuell ausführen. Außerdem löscht dieses Skript weder die importierte Organisation noch die von ihr verwaltet en Konten. Der vertrauen swürdige Zugriff für GuardDuty ist im Rahmen des Bereinigu ngsskripts nicht deaktiviert.	
Entfernen Sie IAM-Rollen.	Löschen Sie die Stacks, die mit den Vorlagen role-to-a ssume-for-role-creation.yam l und management-account -role.yaml CloudFormation erstellt wurden. Weitere Informationen finden Sie unter Löschen eines Stacks (CloudFormation Dokumenta tion).	DevOps Ingenieur, Allgemein es AWS

Zugehörige Ressourcen

AWS-Dokumentation

- Verwalten mehrerer Konten (GuardDuty Dokumentation)
- Gewähren der geringsten Berechtigung (IAM-Dokumentation)

AWS-Marketing

- Amazon GuardDuty

- AWS Organizations

Sonstige Ressourcen

- Terraform
- Terraform-CLI-Dokumentation

Zusätzliche Informationen

Klonen des Repositorys

Führen Sie den folgenden Befehl aus, um das GitHub Repository zu klonen.

```
git clone https://github.com/aws-samples/amazon-guardduty-for-aws-organizations-with-terraform
```

Übernehmen der IAM-Rolle des Verwaltungskontos

Führen Sie den folgenden Befehl aus, um die IAM-Rolle im Verwaltungskonto zu übernehmen. Ersetzen Sie `<IAM role ARN>` durch den ARN der IAM-Rolle.

```
export ROLE_CREDENTIALS=$(aws sts assume-role --role-arn <IAM role ARN> --role-session-name AWSCLI-Session --output json)
export AWS_ACCESS_KEY_ID=$(echo $ROLE_CREDENTIALS | jq .Credentials.AccessKeyId | sed 's/"//g')
export AWS_SECRET_ACCESS_KEY=$(echo $ROLE_CREDENTIALS | jq .Credentials.SecretAccessKey | sed 's/"//g')
export AWS_SESSION_TOKEN=$(echo $ROLE_CREDENTIALS | jq .Credentials.SessionToken | sed 's/"//g')
```

Stellen Sie sicher, dass neue Amazon-Redshift-Cluster über erforderliche SSL-Endpunkte verfügen

Erstellt von Priyanka Chaudhary (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Analytik; Data Lakes	AWS-Services: AWS CloudTrail; Amazon CloudWatch Events; Amazon Redshift; Amazon SNS ; AWS Lambda

Übersicht

Dieses Muster bietet eine Amazon Web Services (AWS)- CloudFormation Vorlage, die Sie automatisch benachrichtigt, wenn ein neuer Amazon-Redshift-Cluster ohne Secure Sockets Layer (SSL)-Endpunkte gestartet wird.

Amazon Redshift ist ein vollständig verwalteter, cloudbasierter Data-Warehouse-Service im Petabyte-Bereich. Es ist für die groß angelegte Speicherung und Analyse von Datensätzen konzipiert. Es wird auch für umfangreiche Datenbankmigrationen verwendet. Aus Sicherheitsgründen unterstützt Amazon Redshift SSL, um die Verbindung zwischen der SQL Server-Clientanwendung des Benutzers und dem Amazon-Redshift-Cluster zu verschlüsseln. Um Ihren Cluster so zu konfigurieren, dass eine SSL-Verbindung erforderlich ist, legen Sie den `require_SSL` Parameter `true` in der Parametergruppe, die dem Cluster beim Start zugeordnet ist, auf fest.

Die mit diesem Muster bereitgestellte Sicherheitskontrolle überwacht Amazon-Redshift-API-Aufrufe in AWS- CloudTrail Protokollen und initiiert ein Amazon CloudWatch -Events-Ereignis für die ModifyClusterParameterGroup APIs CreateCluster, ModifyCluster, RestoreFromClusterSnapshotCreateClusterParameterGroup, und APIs. Wenn das Ereignis eine dieser APIs erkennt, ruft es AWS Lambda auf, das ein Python-Skript ausführt. Die Python-Funktion analysiert das CloudWatch Ereignis für die aufgelisteten CloudTrail Ereignisse. Wenn ein Amazon-Redshift-Cluster aus einem vorhandenen Snapshot erstellt, geändert oder wiederhergestellt wird, eine neue Parametergruppe für den Cluster erstellt oder eine vorhandene Parametergruppe geändert wird, überprüft die Funktion den `require_SSL` Parameter für den Cluster. Wenn der Parameterwert lautet`false`, sendet die Funktion eine Amazon Simple Notification Service (Amazon

SNS)-Benachrichtigung mit den relevanten Informationen an den Benutzer: den Amazon-Redshift-Clusternamen, die AWS-Region, das AWS-Konto und den Amazon-Ressourcennamen (ARN) für Lambda, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Virtual Private Cloud (VPC) mit einer Cluster-Subnetzgruppe und einer zugehörigen Sicherheitsgruppe.

Einschränkungen

- Diese Sicherheitskontrolle ist regional. Sie müssen sie in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten.

- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.
- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt.
- Amazon Redshift – Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service in Petabytegröße in der Cloud.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `RedshiftSSLEndpointsRequired.zip` – Der Lambda-Code für die Sicherheitskontrolle.
- `RedshiftSSLEndpointsRequired.yml` – Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Polen

Einrichten des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket zum Hosten der ZIP-Datei des Lambda-Co des. Dieser S3-Bucket muss sich in derselben AWS-Regio n befinden wie der Amazon	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Redshift-Cluster, den Sie überwachen möchten. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konte n gemeinsam genutzt. Der Name des S3-Buckets darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie die im Abschnitt Anhänge bereitgestellte ZIP-Datei mit dem Lambda-Code in den S3-Bucket hoch.	Cloud-Architekt

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die AWS-CloudFormation Vorlage.	Öffnen Sie die AWS-CloudFormation Konsole in derselben AWS-Regio n wie Ihr S3-Bucket und stellen Sie die angehängte Vorlage bereit`RedshiftS SLEndpointsRequire d.yml` . Weitere Informati onen zum Bereitstellen von AWS- CloudFormation Vorlagen finden Sie unter Erstellen eines Stacks auf der AWS- CloudFormation Konsole in der - CloudForm ation Dokumentation.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Parameter in der Vorlage ab.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im ersten Epi erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (ZIP-Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. Dateiname .zip oder Steuerelemente/Dateiname .zip). Schließen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, an die Sie Amazon SNS-Benac hrichtigungen erhalten möchten. • Lamba-Protokollier ungsebene : Geben Sie die Protokollierungseb ene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informati	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onsmeldungen zum Fortschritt, Fehler bei Fehlerereignissen, die eine Fortsetzung der Bereitstellung ermöglichen würden, und Warnung bei potenziell schädlichen Situationen zu protokollieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines S3-Buckets (Amazon S3-Dokumentation)
- Hochladen von Dateien in einen S3-Bucket (Amazon S3-Dokumentation)
- Erstellen eines Stacks in der AWS- CloudFormation Konsole (AWS- CloudFormation Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail (AWS- CloudTrail Dokumentation)
- Erstellen eines Amazon-Redshift-Clusters (Amazon-Redshift-Dokumentation)
- Konfigurieren von Sicherheitsoptionen für Verbindungen (Amazon-Redshift-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Überprüfen, ob neue Amazon-Redshift-Cluster in einer VPC gestartet werden

Erstellt von Priyanka Chaudhary (AWS)

Umgebung: Produktion	Technologien: Sicherheit, Identität, Compliance; Analysen; Datenbanken	AWS-Services: Amazon CloudWatch; AWS Lambda ; Amazon Redshift

Übersicht

Dieses Muster bietet eine Amazon Web Services (AWS)- CloudFormation Vorlage, die Sie automatisch benachrichtigt, wenn ein Amazon-Redshift-Cluster außerhalb einer Virtual Private Cloud (VPC) gestartet wird.

Amazon Redshift ist ein vollständig verwaltetes, cloudbasiertes Data-Warehouse-Produkt im Petabyte-Bereich. Es ist für die groß angelegte Speicherung und Analyse von Datensätzen konzipiert. Es wird auch für umfangreiche Datenbankmigrationen verwendet. Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie einen logisch isolierten Abschnitt der AWS Cloud bereitstellen, in dem Sie AWS-Ressourcen wie Amazon Redshift-Cluster in einem von Ihnen definierten virtuellen Netzwerk starten können.

Die mit diesem Muster bereitgestellte Sicherheitskontrolle überwacht Amazon-Redshift-API-Aufrufe in AWS- CloudTrail Protokollen und initiiert ein Amazon- CloudWatch Events-Ereignis für die RestoreFromClusterSnapshot APIs CreateCluster und . APIs Wenn das Ereignis eine dieser APIs erkennt, ruft es AWS Lambda auf, das ein Python-Skript ausführt. Die Python-Funktion analysiert das CloudWatch Ereignis. Wenn ein Amazon-Redshift-Cluster aus einem Snapshot erstellt oder wiederhergestellt wird und außerhalb des Amazon-VPC-Netzwerks erscheint, sendet die Funktion eine Amazon Simple Notification Service (Amazon SNS)-Benachrichtigung mit den relevanten Informationen an den Benutzer: den Amazon-Redshift-Clusternamen, die AWS-Region, das AWS-Konto und den Amazon-Ressourcennamen (ARN) für Lambda, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine VPC mit einer Cluster-Subnetzgruppe und einer zugehörigen Sicherheitsgruppe.

Einschränkungen

- Die AWS- CloudFormation Vorlage unterstützt nur die RestoreFromClusterSnapshot Aktionen CreateCluster und (neue Cluster). Es erkennt keine vorhandenen Amazon-Redshift-Cluster, die außerhalb einer VPC erstellt wurden.
- Diese Sicherheitskontrolle ist regional. Sie müssen sie in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation StackSets verwenden, um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation – AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten.
- AWS CloudTrail – AWS CloudTrail unterstützt Sie bei der Implementierung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos. Aktionen eines Benutzers, einer Rolle oder eines AWS-Services werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events – Amazon CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an AWS-Ressourcen beschreibt.

- AWS Lambda – AWS Lambda ist ein Datenverarbeitungsservice, der das Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern unterstützt. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon Redshift – Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service in Petabytegröße in der Cloud. Amazon Redshift ist in Ihren Data Lake integriert, sodass Sie Ihre Daten verwenden können, um neue Erkenntnisse für Ihr Unternehmen und Ihre Kunden zu gewinnen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `RedshiftMustBeInVPC.zip` – Der Lambda-Code für die Sicherheitskontrolle.
- `RedshiftMustBeInVPC.yml` – Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Um diese Dateien zu verwenden, folgen Sie den Anweisungen im nächsten Abschnitt.

Polen

Einrichten des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3-Konsole einen S3-Bucket zum Hosten der ZIP-Datei des Lambda-Co des. Dieser S3-Bucket muss	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sich in derselben AWS-Regio n befinden wie der Amazon Redshift-Cluster, den Sie überwachen möchten. Ein S3-Bucket-Name ist global eindeutig und der Namespace wird von allen AWS-Konte n gemeinsam genutzt. Der S3-Bucket-Name darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie den Lambda-Co de (`RedshiftMustBeInVP C.zip` -Datei) im Abschnitt Anhänge in den S3-Bucket hoch.	Cloud-Architekt

Bereitstellen der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudForm ation Vorlage.	Öffnen Sie die AWS-CloudFormation Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die angehängte Vorlage bereit (`RedshiftMustBeInVP C.yml`). Weitere Informati onen zum Bereitstellen von AWS- CloudFormation Vorlagen finden Sie unter Erstellen eines Stacks in der AWS- CloudFormation	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole in der - CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Parameter in der Vorlage ab.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im ersten Epi erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (ZIP-Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. Dateiname .zip oder Steuerelemente/Dateiname .zip). Schließen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, an die Sie Amazon SNS-Benac hrichtigungen erhalten möchten. • Lamba-Protokollier ungsebene : Geben Sie die Protokollierungseb ene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informati	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onsmeldungen zum Fortschritt, Fehler bei Fehlerereignissen, die die Bereitstellung weiterhin zulassen würden, und Warnung bei potenziell schädlichen Situationen zu protokollieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines S3-Buckets (Amazon S3-Dokumentation)
- Hochladen von Dateien in einen S3-Bucket (Amazon S3-Dokumentation)
- Erstellen eines Stacks in der AWS- CloudFormation Konsole (AWS- CloudFormation Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail (AWS- CloudTrail Dokumentation)
- Erstellen eines Amazon-Redshift-Clusters (Amazon-Redshift-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Mehr Muster

- Zugreifen auf einen Bastion-Host mithilfe von Session Manager und Amazon EC2 Instance Connect
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- ???
- EC2-Instances Schreibzugriff auf S3-Buckets in AMS-Konten gewähren
- Zuordnen eines AWS- CodeCommit Repositorys in einem AWS-Konto zu SageMaker Studio in einem anderen Konto
- Automatisieren des Hinzufügens oder Aktualisierens von Windows-Registrierungseinträgen mit AWS Systems Manager
- ???
- Automatisches Anfügen einer von AWS verwalteten Richtlinie für Systems Manager an EC2-Instance-Profile mithilfe von Cloud Custodian und AWS CDK
- Automatisches Verschlüsseln vorhandener und neuer Amazon-EBS-Volumes
- Blockieren des öffentlichen Zugriffs auf Amazon RDS mithilfe von Cloud Custodian
- ???
- Überprüfen Sie AWS-CDK-Anwendungen oder - CloudFormation Vorlagen auf bewährte Methoden mithilfe von cdk-nag-Regelpaketen
- EC2-Instances beim Start auf obligatorische Tags überprüfen
- Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren
- Konfigurieren Sie die HTTPS-Verschlüsselung für Oracle JD Edwards EnterpriseOne auf Oracle WebLogic mithilfe eines Application Load Balancer
- Konfigurieren der Protokollierung und Überwachung für Sicherheitsereignisse in Ihrer AWS IoT-Umgebung
- Konfigurieren der gegenseitigen TLS-Authentifizierung für Anwendungen, die auf Amazon EKS ausgeführt werden
- ???
- Erstellen Sie eine React-App mithilfe von AWS Amplify und fügen Sie die Authentifizierung mit Amazon Cognito hinzu

- Erstellen Sie einen Bericht über die Ergebnisse von Network Access Analyzer für eingehenden Internetzugriff in mehreren AWS-Konten
- Anpassen von Amazon- CloudWatch Warnungen für AWS Network Firewall
- Bereitstellen einer Firewall mit AWS Network Firewall und AWS Transit Gateway
- Dokumentieren Ihres AWS-Landing-Zone-Designs
- Aktivieren verschlüsselter Verbindungen für PostgreSQL-DB-Instances in Amazon RDS
- Verschlüsseln einer vorhandenen DB-Instance von Amazon RDS für PostgreSQL
- Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen
- Tagging von Amazon-EMR-Clustern beim Start erzwingen
- Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist
- Suchen Sie AWS-Ressourcen basierend auf ihrem Erstellungsdatum mithilfe von erweiterten AWS Config-Abfragen
- Generieren einer AWS- CloudFormation Vorlage mit verwalteten AWS Config-Regeln mithilfe vonoSphere
- Amazon SNS-Benachrichtigungen abrufen, wenn sich der Schlüsselstatus eines AWS KMS-Schlüssels ändert
- ???
- Identifizieren und warnen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS-Schlüssel verschlüsselt sind
- Verbessern Sie die betriebliche Leistung, indem Sie Amazon DevOps Guru über mehrere AWS-Regionen, Konten und OUs hinweg mit dem AWS-CDK aktivieren
- Aufnehmen und Migrieren von EC2-Windows-Instances in ein AWS Managed Services-Konto
- Migrieren von Amazon RDS für Oracle zu Amazon RDS für PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren eines ELK-Stacks zu Elastic Cloud in AWS
- Migrieren eines F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS Cloud
- Überwachen von Amazon Aurora auf Instances ohne Verschlüsselung
- Rotieren von Datenbankanmeldeinformationen ohne Neustart von Containern
- Sichern und optimieren Sie den Benutzerzugriff in einer Db2-Verbunddatenbank in AWS mithilfe vertrauenswürdiger Kontexte
- ???

- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Einrichten der end-to-end Verschlüsselung für Anwendungen in Amazon EKS mit cert-manager und Let's Encrypt
- Stellen Sie sicher, dass ELB-Load Balancer eine TLS-Beendigung erfordern
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen
- Visualisieren von IAM-Anmeldeinformationsberichten für alle AWS-Konten mit Amazon QuickSight

Serverless

Themen

Erstellen Sie mithilfe von AWS Amplify eine serverlose mobile React Native-App

Erstellt von Deekshitulu Pentakota (AWS)

aws-amplify-react-nativeCode-Repository: - ios-todo-app	Umgebung: Produktion	Quelle: NA
Ziel: AWS Amplify, AWS, Amazon Cognito AppSync, Amazon DynamoDB	R-Typ: Re-Architect	Arbeitsaufwand: Open Source
Technologien: Serverlos; Web- und mobile Apps	AWS-Dienste: AWS Amplify; AWS; Amazon Cognito AppSync; Amazon DynamoDB	

Übersicht

Dieses Muster zeigt, wie Sie mithilfe von AWS Amplify und den folgenden AWS-Services ein serverloses Backend für eine mobile React Native-App erstellen:

- AWS AppSync
- Amazon Cognito
- Amazon-DynamoDB

Nachdem Sie das Backend der App mithilfe von Amplify konfiguriert und bereitgestellt haben, authentifiziert Amazon Cognito App-Benutzer und autorisiert sie für den Zugriff auf die App. AWS interagiert AppSync dann mit der Frontend-App und mit einer DynamoDB-Backend-Tabelle, um Daten zu erstellen und abzurufen.

Hinweis: In diesem Muster wird eine einfache App „ToDoList“ als Beispiel verwendet. Sie können jedoch ein ähnliches Verfahren verwenden, um jede beliebige mobile React Native-App zu erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amplify Command Line Interface (Amplify CLI), installiert und konfiguriert
- XCode (jede Version)
- Microsoft Visual Studio (jede Version, jeder Code-Editor, jeder Texteditor)
- Vertrautheit mit Amplify
- Vertrautheit mit Amazon Cognito
- Vertrautheit mit AWS AppSync
- Vertrautheit mit DynamoDB
- Vertrautheit mit Node.js
- Vertrautheit mit npm
- Vertrautheit mit React und React Native
- Vertrautheit mit JavaScript und ECMAScript 6 (ES6)
- Vertrautheit mit GraphQL

Architektur

Das folgende Diagramm zeigt eine Beispielarchitektur für die Ausführung des Backends einer mobilen React Native-App in der AWS-Cloud:

Das Diagramm zeigt die folgende Architektur:

1. Amazon Cognito authentifiziert App-Benutzer und autorisiert sie, auf die App zuzugreifen.
2. Um Daten zu erstellen und abzurufen, AppSync verwendet AWS eine GraphQL-API, um mit der Frontend-App und einer Backend-DynamoDB-Tabelle zu interagieren.

Tools

AWS-Services

- AWS Amplify ist eine Reihe von speziell entwickelten Tools und Funktionen, mit denen Frontend-Web- und Mobilentwickler schnell Full-Stack-Anwendungen auf AWS erstellen können.

- AWS AppSync bietet eine skalierbare GraphQL-Schnittstelle, mit der Anwendungsentwickler Daten aus mehreren Quellen kombinieren können, darunter Amazon DynamoDB-, AWS Lambda- und HTTP-APIs.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Code

Der Code für die Beispielanwendung, die in diesem Muster verwendet wird, ist im ios-todo-app Repository GitHub aws-amplify-react-native- verfügbar. Um die Beispieldateien zu verwenden, folgen Sie den Anweisungen im Abschnitt Epics dieses Musters.

Epen

Erstelle deine React Native-App und führe sie aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine React Native-Entwicklungsumgebung ein.	Anweisungen finden Sie unter Einrichten der Entwicklungsumgebung in der React Native-Dokumentation.	App-Developer
Erstellen Sie die mobile ToDoList React Native-App und führen Sie sie im iOS-Simulator aus.	1. Erstellen Sie ein neues React Native-Projektverzeichnis für mobile Apps in Ihrer lokalen Umgebung, indem Sie den folgenden Befehl in einem neuen Terminalfenster ausführen: `npx react-native init ToDoListAmplify`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Navigieren Sie zum Stammverzeichnis des Projekts, indem Sie den folgenden Befehl ausführen:
	`cd ToDoListAmplify`
	3. Führen Sie die App aus, indem Sie den folgenden Befehl ausführen:
	`npx react-native run-ios`	

Initialisieren Sie eine neue Backend-Umgebung für die App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Backend-Dienste, die zur Unterstützung der App in Amplify erforderlich sind.	1. Führen Sie in Ihrer lokalen Umgebung den folgenden Befehl im Stammverzeichnis des Projekts aus () ToDoListAmplifyaus: `amplify init` 2. Es wird eine Aufforderung angezeigt, in der Sie aufgefordert werden, Informationen zur App anzugeben. Geben Sie die erforderlichen Informationen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließend die Eingabetaste.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an.
	
	Beispiel für die Konfiguration der React Native Amplify App
	
	`? Name: ToDoListAmplify`
	
	`? Environment: dev`
	
	`? Default editor: Visual Studio Code`
	
	`? App type: javascript`
	
	`? Javascript framework: react-native`
	
	`? Source Directory Path: src`
	
	`? Distribution Directory Path: /`
	
	`? Build Command: npm run-script build`
	
	`? Start Command: npm run-script start`
	
	`? Select the authentication method you want to use: AWS profile`
	
	`? Please choose the profile you want to use: default`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Erstellen eines neuen Amplify-Backends in der Amplify Dev Center-Dokumentation. Hinweis: Der `amplify init` Befehl stellt mithilfe von AWS die folgenden Ressourcen bereit CloudFormation: • AWS Identity and Access Management (IAM) -Rollen für authentifizierte und nicht authentifizierte Benutzer (Auth Role und Unauth Role) • Ein Amazon Simple Storage Service (Amazon S3) - Bucket für die Bereitstellung (für die Beispiel-App dieses Musters, Amplify-Meta.json) • Eine Backend-Umgebung in Amplify Hosting	

Fügen Sie Ihrer Amplify React Native-App die Amazon Cognito Cognito-Authentifizierung hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon Cognito Cognito-Authentifizierungsservice.	1. Führen Sie in Ihrer lokalen Umgebung den folgenden Befehl im Stammverzeichnis des Projekts aus (ToDoListAmplify) aus:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`amplify add auth`
	2. Es wird eine Aufforderung angezeigt, in der Sie aufgefordert werden, Informationen zu den Konfigurationseinstellungen des Authentifizierungsdienstes einzugeben. Geben Sie die erforderlichen Informationen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließend die Eingabetaste.
	
	Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an.
	
	Beispiel für Konfigurationseinstellungen für den Authentifizierungsdienst
	
	`? Do you want to use the default authentication and security configuration? \`
	`Default configuration`
	
	`? How do you want users to be able to sign in? \`
	`Username`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`? Do you want to configure advanced settings? \ No, I am done` Hinweis: Der `amplify add auth` Befehl erstellt die erforderlichen Ordner, Dateien und Abhängigkeitsdateien in einem lokalen Ordner (Amplify) im Stammverz eichnis des Projekts. Für das in diesem Muster verwendet e ToDoList App-Setup wird die Datei aws-exports.js zu diesem Zweck erstellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Amazon Cognito-Service in der AWS-Cloud bereit.	1. Führen Sie im Stammverz eichnis des Projekts den folgenden Amplify CLI-Befehl aus:
	
	`amplify push`
	
	2. Eine Aufforderung zur Bestätigung der Bereitste llung wird angezeigt. Geben Sie Ja ein. Drücken Sie anschließend die Eingabeta ste.
	
	Hinweis: Um die in Ihrem Projekt bereitgestellten Dienste zu sehen, rufen Sie die Amplify-Konsole auf, indem Sie den folgenden Befehl ausführen:
	
	`amplify console`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die erforderlichen Amplify-Bibliotheken für React Native und die CocoaPods Abhängigkeiten für iOS.	1. Installieren Sie die erforderlichen Amplify-Open-Source-Clientbibliotheken, indem Sie den folgenden Befehl im Stammverzeichnis des Projekts ausführen:
	`npm install aws-amplify aws-amplify-react-native \ amazon-cognito-identity-js @react-native-community/netinfo \ @react-native-async-storage/async-storage`
	2. Installieren Sie die erforderlichen CocoaPods Abhängigkeiten für iOS, indem Sie den folgenden Befehl ausführen:
	`npx pod-install`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Importieren und konfigurieren Sie den Amplify-Dienst.	Importieren und laden Sie in der Einstiegspunktdate i der App (z. B. App.js) die Konfigurationsdatei des Amplify-Dienstes, indem Sie die folgenden Codezeilen eingeben:
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	Hinweis: Wenn Sie nach dem Import des Amplify-Dienstes in die Einstiegspunktdate i der App eine Fehlermel dung erhalten, beenden Sie die App. Öffnen Sie dann XCode und wählen Sie den ToDoListAmplify.xcworkspace aus dem iOS-Ordner des Projekts aus und führen Sie die App aus.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die Einstiegspunktdatei Ihrer App, um die WithAuthenticator-Komponente (HOC) zu verwenden.	Hinweis: Der `withAuthenticator` HOC bietet Workflows zum Anmelden, Registrieren und Vergessen von Passwörtern in Ihrer App, wobei nur wenige Codezeilen verwendet werden. Weitere Informationen finden Sie unter Option 1: Verwenden Sie vorgefertigte UI-Komponenten im Amplify Dev Center. Außerdem Komponenten höherer Ordnung in der React-Dokumentation.
	
	1. Importieren Sie den `withAuthenticator` HOC in der Einstiegspunktdatei der App (z. B. App.js), indem Sie die folgenden Codezeilen eingeben:
	
	`import { withAuthenticator } from 'aws-amplify-react-native'`
	
	2. Exportieren Sie den WithAuthenticator-HOC, indem Sie den folgenden Code eingeben:
	
	`export default withAuthenticator(App)`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Beispiel für den WITHAuthenticator HOC-Code
	
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	`import { withAuthenticator } from 'aws-amplify-react-native';`
	
	`const App = () => {`
	`  return null;`
	`};`
	
	`export default withAuthenticator(App);`
	
	Hinweis: In iOS Simulator zeigt die App den Anmeldebildschirm an, der vom Amazon Cognito-Service bereitgestellt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Einrichtung des Authentifizierungsdienstes.	Gehen Sie im iOS-Simulator wie folgt vor: 1. Erstellen Sie ein neues Konto in der App, indem Sie eine echte E-Mail-Adresse verwenden. Ein Bestätigungscode wird dann an die registrierte E-Mail gesendet. 2. Überprüfen Sie das eingerichtete Konto mithilfe des Codes, den Sie in der Bestätigungs-E-Mail erhalten. 3. Geben Sie den Benutzernamen und das Passwort ein, die Sie erstellt haben. Wählen Sie dann Anmelden. Ein Willkommensbildschirm wird angezeigt. Hinweis: Sie können auch die Amazon Cognito Cognito-Konsole öffnen und überprüfen, ob ein neuer Benutzer im Identity Pool erstellt wurde oder nicht.	App-Developer

Eine AppSync AWS-API und eine DynamoDB-Datenbank mit der App Connect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AppSync AWS-API und eine DynamoDB-Datenbank.	1. Fügen Sie Ihrer App eine AppSync AWS-API hinzu und stellen Sie automatisch eine DynamoDB-Datenbank bereit, indem Sie den folgenden Amplify-CLI-Befehl im Stammverz eichnis des Projekts ausführen: `amplify add api` 2. Es wird eine Aufforder ung angezeigt, in der Sie aufgefordert werden, Informationen zu den API- und Datenbank konfigurationseinstellungen anzugeben. Geben Sie die erforderlichen Informati onen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließ end die Eingabetaste. Die Amplify CLI öffnet die GraphQL-Schemadatei in Ihrem Texteditor. Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Beispiel für API- und Datenbankkonfigurationseinstellungen
	
	`? Please select from one of the below mentioned services: \`
	`GraphQL`
	
	`? Provide API name: todolistamplify`
	
	`? Choose the default authorization type for the API \`
	`Amazon Cognito User Pool`
	
	`Do you want to use the default authentication and security configuration`
	
	`? Default configuration How do you want users to be able to sign in? \`
	`Username`
	
	`Do you want to configure advanced settings? \`
	`No, I am done.`
	
	`? Do you want to configure advanced settings for the GraphQL API \`
	`No, I am done.`
	
	`? Do you have an annotated GraphQL schema? \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	No
	
	? Choose a schema
	template: \
	Single object with
	fields (e.g., “Todo”
	with ID, name,
	description)
	
	? Do you want to edit
	the schema now? \
	Yes
	
	Beispiel für ein GraphQL-Schema
	
	type Todo @model {
	id: ID!
	name: String!
	description: String
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AppSync AWS-API bereit.	1. Führen Sie im Stammverzeichnis des Projekts den folgenden Amplify CLI-Befehl aus: `amplify push` 2. Es wird eine Aufforderung angezeigt, in der Sie aufgefordert werden, weitere Informationen zu den API- und Datenbankkonfigurationseinstellungen anzugeben. Geben Sie die erforderlichen Informationen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließend die Eingabetaste. Ihre App kann jetzt mit der AppSync AWS-API interagieren. Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an. Beispiel für AppSync AWS-API-Konfigurationseinstellungen Hinweis: Die folgende Konfiguration erstellt die GraphQL-API in AWS AppSync und eine Todo-Tabelle in Dynamo DB.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ? Are you sure you want to continue? Yes ? Do you want to generate code for your newly created GraphQL API Yes ? Choose the code generation language target javascript ? Enter the file name pattern of graphql queries, mutations and subscriptions src/ graphql/**/*.js ? Do you want to generate/update all possible GraphQL operations - \ queries, mutations and subscriptions Yes ? Enter maximum statement depth \ [increase from default if your schema is deeply nested] 2 ```	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect das Frontend der App mit der AppSync AWS-API.	Um die in diesem Muster bereitgestellte ToDoList Beispiel-App zu verwenden , kopieren Sie den Code aus der Datei App.js im ios-todo-app GitHub Repository aws-amplify-react-native-. Integrieren Sie dann den Beispielcode in Ihre lokale Umgebung. Der in der Datei App.js des Repositorys enthalten e Beispielcode bewirkt Folgendes: • Zeigt das Formular zum Erstellen eines ToDo Elements mit den Feldern Titel und Beschreibung • Zeigt die Liste der zu erledigenden Aufgaben an (Titel und Beschreibung) • Postet Daten mithilfe von Methoden und ruft sie ab `aws-amplify`	App-Developer

Zugehörige Ressourcen

- AWS Amplify
- Amazon Cognito
- AWS AppSync
- Amazon-DynamoDB
- React (React-Dokumentation)

Stellen Sie DynamoDB-Datensätze mithilfe von Kinesis Data Streams und Amazon Data Firehose mit AWS CDK an Amazon S3 bereit

Erstellt von Shashank Shrivastava (AWS) und Daniel Matuki da Cunha (AWS)

Code-Repository: Aufnahme von Amazon DynamoDB in Amazon S3	Umgebung: PoC oder Pilotprojekt	Technologien: Serverlos; Data Lakes; Datenbanken; Speicher und Backup
AWS-Services: AWS CDK; Amazon DynamoDB; Amazon Kinesis Data Firehose; Amazon Kinesis Data Streams; AWS Lambda; Amazon S3		

Übersicht

Dieses Muster enthält Beispielcode und eine Anwendung für die Übermittlung von Datensätzen von Amazon DynamoDB an Amazon Simple Storage Service (Amazon S3) mithilfe von Amazon Kinesis Data Streams und Amazon Data Firehose. Der Ansatz des Musters verwendet L3-Konstrukte des AWS Cloud Development Kit (AWS CDK) und beinhaltet ein Beispiel dafür, wie eine Datentransformation mit AWS Lambda durchgeführt wird, bevor Daten an den Ziel-S3-Bucket in der Amazon Web Services (AWS) -Cloud geliefert werden.

Kinesis Data Streams zeichnet Änderungen auf Elementebene in DynamoDB-Tabellen auf und repliziert sie in den erforderlichen Kinesis-Datenstrom. Ihre Anwendungen können auf den Kinesis Data Stream zugreifen und die Änderungen auf Elementebene nahezu in Echtzeit anzeigen. Kinesis Data Streams bietet auch Zugriff auf andere Amazon Kinesis Kinesis-Services wie Firehose und Amazon Managed Service für Apache Flink. Das bedeutet, dass Sie Anwendungen entwickeln können, die Echtzeit-Dashboards bereitstellen, Warnmeldungen generieren, dynamische Preisgestaltung und Werbung implementieren und anspruchsvolle Datenanalysen durchführen.

Sie können dieses Muster für Ihre Anwendungsfälle zur Datenintegration verwenden. Beispielsweise können Transportfahrzeuge oder Industrieanlagen große Datenmengen an eine DynamoDB-Tabelle senden. Diese Daten können dann transformiert und in einem in Amazon S3 gehosteten Data Lake gespeichert werden. Anschließend können Sie die Daten abfragen und verarbeiten und potenzielle Fehler vorhersagen, indem Sie serverlose Dienste wie Amazon Athena, Amazon Redshift Spectrum, Amazon Rekognition und AWS Glue verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte mit der AWS-CLI in der AWS-CLI-Dokumentation.
- Node.js (18.x+) und npm, installiert und konfiguriert. Weitere Informationen finden Sie in der Dokumentation unter Node.js und npm herunterladen und installieren. `npm`
- aws-cdk (2.x+), installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte mit dem AWS-CDK in der AWS-CDK-Dokumentation.
- Das GitHub aws-dynamodb-kinesisfirehose-s3-ingestion-Repository, geklont und auf Ihrem lokalen Computer konfiguriert.
- Bestehende Beispieldaten für die DynamoDB-Tabelle. Die Daten müssen das folgende Format haben: `{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}`

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Übermittlung von Datensätzen von DynamoDB an Amazon S3 mithilfe von Kinesis Data Streams und Firehose.

Das Diagramm zeigt den folgenden Workflow:

1. Daten werden mit Amazon API Gateway als Proxy für DynamoDB aufgenommen. Sie können auch jede andere Quelle verwenden, um Daten in DynamoDB aufzunehmen.
2. Änderungen auf Artikelebene werden nahezu in Echtzeit in Kinesis Data Streams generiert und an Amazon S3 übermittelt.
3. Kinesis Data Streams sendet die Datensätze zur Transformation und Bereitstellung an Firehose.

4. Eine Lambda-Funktion konvertiert die Datensätze von einem DynamoDB-Datensatzformat in das JSON-Format, das nur die Namen und Werte der Datensatzelementattribute enthält.

Tools

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, mit dem Sie mit Ihrer AWS Cloud Development Kit (AWS CDK) -App interagieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.

Code

Der Code für dieses Muster ist im Repository GitHub aws-dynamodb-kinesisfirehose-s3-ingestion verfügbar.

Epen

Richten Sie den Beispielcode ein und konfigurieren Sie ihn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Abhängigkeiten.	Installieren Sie auf Ihrem lokalen Computer die Abhängigkeiten aus den `package.json` Dateien in den `sample-application` Verzeichnissen `pattern/aws-dynamodb-kinesisstreams-s3` und, indem Sie die folgenden Befehle ausführen:	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd <project_root>/pattern/aws-dynamodb-kinesisstreams-s3`
	
	`npm install && npm run build`
	
	`cd <project_root>/sample-application/`
	
	`npm install && npm run build`	

Generieren Sie die CloudFormation AWS-Vorlage.	1. Führen Sie den Befehl `cd <project_root>/sample-application/` aus. 2. Führen Sie den `cdk synth` Befehl aus, um die CloudFormation AWS-Vorlage zu generieren. 3. Die `AwsDynamodbKinesisfirehoseS3IngestionStack.template.json` Ausgabe wird im `cdk.out` Verzeichnis gespeichert. 4. Verwenden Sie AWS CDK oder die AWS-Managementkonsole, um die Vorlage in AWS CloudFormation zu verarbeiten.	App-Entwickler, General AWS, AWS DevOps

Stellen Sie die Ressourcen bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ressourcen und setzen Sie sie ein.	1. Führen Sie den `cdk diff` Befehl aus, um die Ressourcentypen zu identifizieren, die durch das AWS-CDK-Konstrukt erstellt wurden. 2. Führen Sie den `cdk deploy` Befehl aus, um die Ressourcen bereitzustellen.	App-Entwickler, General AWS, AWS DevOps

Daten in die DynamoDB-Tabelle aufnehmen, um die Lösung zu testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie Ihre Beispieldaten in die DynamoDB-Tabelle auf.	1. Senden Sie eine Anfrage an Ihre DynamoDB-Tabelle, indem Sie den folgenden Befehl in der AWS-CLI ausführen: `aws dynamodb put-item --table-name <your_table_name> --item '{"<table_partition_key>": {"S": "<partition_key_ID>"},"MessageData":{"S": "<data>"}}'` Beispiel:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws dynamodb put-item --table-name SourceData_table --item '{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}'` Standardmäßig `put-item` gibt der keinen Wert als Ausgabe zurück, wenn der Vorgang erfolgreich ist. Wenn der Vorgang fehlschlägt, wird ein Fehler zurückgegeben. Die Daten werden in DynamoDB gespeichert und dann an Kinesis Data Streams und Firehose gesendet. Hinweis: Sie verwenden unterschiedliche Methoden, um Daten zu einer DynamoDB-Tabelle hinzuzufügen. Weitere Informationen finden Sie unter Daten in Tabellen laden in der Amazon DynamoDB DynamoDB-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass ein neues Objekt im S3-Bucket erstellt wurde.	Melden Sie sich bei der AWS-Managementkonsole an und überwachen Sie den S3-Bucket, um sicherzustellen, dass mit den von Ihnen gesendeten Daten ein neues Objekt erstellt wurde. Weitere Informationen finden Sie `get-object` in der Referenzdokumentation zur Amazon S3 S3-API.	App-Entwickler, General AWS

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen bereinigen.	Führen Sie den `cdk destroy` Befehl aus, um alle von diesem Muster verwendeten Ressourcen zu löschen.	App-Entwickler, General AWS

Zugehörige Ressourcen

- s3-static-site-stack.ts (Repository) GitHub
- aws-apigateway-dynamodb Modul (Repositorium) GitHub
- aws-kinesisstreams-kinesisfirehose-S3-Modul (Repository) GitHub
- Erfassung von Änderungsdaten für DynamoDB Streams (Amazon DynamoDB DynamoDB-Dokumentation)
- Verwenden von Kinesis Data Streams zur Erfassung von Änderungen an DynamoDB (Amazon DynamoDB DynamoDB-Dokumentation)

Integrieren Sie Amazon API Gateway mit Amazon SQS, um asynchrone REST-APIs zu handhaben

Erstellt von Natalia Colantonio Favero (AWS) und Gustavo Martim (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Serverlos; Messaging und Kommunikation	AWS-Dienste: Amazon API Gateway; Amazon SQS

Übersicht

Wenn Sie REST-APIs bereitstellen, müssen Sie manchmal eine Nachrichtenwarteschlange bereitstellen, die Client-Anwendungen veröffentlichen können. Möglicherweise haben Sie Probleme mit der Latenz von APIs von Drittanbietern und Verzögerungen bei den Antworten, oder Sie möchten die Antwortzeit von Datenbankabfragen vermeiden oder den Server nicht skalieren, wenn eine große Anzahl gleichzeitiger APIs vorhanden ist. In diesen Szenarien müssen die Client-Anwendungen, die in der Warteschlange veröffentlichen, nur wissen, dass die API die Daten empfangen hat — nicht, was nach dem Empfang der Daten passiert.

Dieses Muster erstellt einen REST-API-Endpunkt, indem Amazon API Gateway verwendet wird, um eine Nachricht an Amazon Simple Queue Service (Amazon SQS) zu senden. Es schafft eine easy-to-implement Integration zwischen den beiden Diensten, wodurch ein direkter Zugriff auf die SQS-Warteschlange vermieden wird.

Voraussetzungen und Einschränkungen

- Ein aktives Konto AWS

Architektur

Das Diagramm veranschaulicht diese Schritte:

1. Fordern Sie einen POST-REST-API-Endpunkt an, indem Sie ein Tool wie Postman, eine andere API oder andere Technologien verwenden.

2. API Gateway stellt eine Nachricht, die im Hauptteil der Anfrage empfangen wird, in die Warteschlange.
3. Amazon SQS empfängt die Nachricht und sendet eine Antwort mit einem Erfolgs- oder Fehlercode an API Gateway.

Tools

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Epen

Erstellen Sie eine SQS-Warteschlange

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Warteschlange.	So erstellen Sie eine SQS-Warteschlange, die die Nachrichten von der REST-API empfängt: 1. Melden Sie sich bei AWS-Konto an. 2. Öffnen Sie die Amazon-SQS-Konsole unter https://console.aws.amazon.com/sqs/.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Create queue (Warteschlange erstellen) aus. 4. Wählen Sie auf der Seite Warteschlange erstellen die richtige Option AWS-Region aus der Dropdownliste Region aus. 5. Behalten Sie für Typ die Standardeinstellung (Standard) bei. 6. Geben Sie einen Namen für die Warteschlange ein. 7. Behalten Sie die Standardwerte für alle anderen Einstellungen bei. 8. Wählen Sie Create queue (Warteschlange erstellen) aus.	

Zugriff auf Amazon SQS bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Diese IAM-Rolle gewährt API Gateway Gateway-Ressourcen vollen Zugriff auf Amazon SQS. 1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.	App-Entwickler, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigationsbereich Roles (Rollen) und Create Role (Rolle erstellen) aus. 3. Wählen Sie für Vertrauenswürdige Entität die Option AWS-Service aus. 4. Wählen Sie unter Anwendungsfall die Option API Gateway aus der Dropdownliste aus und wählen Sie dann Weiter, Weiter aus. 5. Geben Sie als Rollenname eine optionale Beschreibung ein AWSGatewayRoleForSQSund wählen Sie dann Rolle erstellen aus. 6. Suchen Sie im Bereich Rollen nach AWSGatewayRoleForSQSund aktivieren Sie das entsprechende Kontrollkästchen. 7. Unter Berechtigungsrichtlinien im Abschnitt Berechtigungen hinzufügen wählen Sie Richtlinien anfügen aus. 8. Suchen Sie nach AmazonSQS FullAccess und wählen Sie es aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus. 10. Kopieren Sie im Abschnitt Zusammenfassung von AWSGatewayRoleForSQSdie Amazon-Ressourcennummer (ARN). Sie werden diese ID in einem späteren Schritt verwenden.	

Erstellen Sie eine REST-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine REST-API.	Dies ist die REST-API, an die HTTP-Anfragen gesendet werden. 1. Öffnen Sie die API Gateway-Konsole unter https://console.aws.amazon.com/apigateway/. 2. Wählen Sie im Abschnitt REST-API die Option Build aus. 3. Geben Sie als API-Name einen Namen und eine optionale Beschreibung für Ihre API ein, behalten Sie alle anderen Standardeinstellungen bei und wählen Sie dann Create API aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect API Gateway mit Amazon SQS.	Dieser Schritt ermöglicht es, dass die Nachricht aus dem Hauptteil der HTTP-Anfrage an Amazon SQS weitergeleitet wird. 1. Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben. 2. Wählen Sie auf der Seite Ressourcen im Abschnitt Methoden die Option Methode erstellen aus. 3. Wählen Sie in Method type (Methodentyp) POST. 4. Wählen Sie als Integrationstyp AWS-Service. 5. Wählen Sie für die Region aus AWS-Region, in der Sie Ihre SQS-Warteschlange erstellt haben. 6. Wählen Sie für AWS-Service Simple Queue Service (SQS). 7. Wählen Sie als HTTP-Methode POST aus. 8. Wählen Sie als Aktionstyp die Option Pfadüberschreibung verwenden aus. 9. Geben Sie für Path Override den Wert/<AWS	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	account ID>ein<name of SQS queue>. 10. Fügen Sie für die Ausführungsrolle den ARN der Rolle ein, die Sie zuvor erstellt haben. 11. Wählen Sie Methode erstellen aus.	

Testen Sie die REST-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die REST-API.	Führen Sie einen Test durch, um zu überprüfen, ob die Konfiguration fehlt: 1. Wählen Sie in der API Gateway Gateway-Konsole die REST-API aus, die Sie erstellt haben. 2. Wählen Sie im Bereich Ressourcen die POST-Methode aus. 3. Wählen Sie die Registerkarte Test. (Verwenden Sie den Rechtspfeil, wenn die Registerkarte nicht angezeigt wird.) 4. Fügen Sie in das Feld Request body den folgenden JSON-Code ein: `{`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"message":
	"lorem ipsum"
	}</pre>
	5. Wählen Sie Test aus.
	
	Sie erhalten eine Fehlermeldung, die der folgenden ähnelt:
	
	<pre><UnknownOperationException/></pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die API-Integration, um die Anfrage ordnungsgemäß an Amazon SQS weiterzuleiten.	Vervollständigen Sie die Konfiguration, um den Integrationsfehler zu beheben: 1. Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben, und wählen Sie dann POST. 2. Der Abschnitt Method Execution zeigt die visuelle Zuordnung zwischen API Gateway und Amazon SQS. Wählen Sie in diesem Abschnitt Integrationsanfrage und dann Bearbeiten aus. 3. Erweitern Sie den Abschnitt HTTP-Header und wählen Sie dann den Parameter Anforderungsheader hinzufügen aus. • Geben Sie für Name Content-Type an. • Geben Sie für Zugeordnet von den Namen „application/“ ein. x-www-form-urlencoded Achten Sie darauf, die einfachen Anführungszeichen einzuschließen. • Wählen Sie das Kontrollkästchen Caching aus. 4. Erweitern Sie den Abschnitt Mapping-Vorlagen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie Add mapping template. • Geben Sie als Inhaltstyp application/json ein. • Fügen Sie für den Vorlagentext diesen Code ein: `Action=SendMessage&MessageBody=$input.body` • Wählen Sie Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen und validieren Sie die Nachricht in Amazon SQS.	Führen Sie einen Test durch, um zu bestätigen, dass der Test erfolgreich abgeschlossen wurde: 1. Wählen Sie in der API Gateway Gateway-Konsole die REST-API aus, die Sie erstellt haben. 2. Wählen Sie im Bereich Ressourcen die POST-Methode aus. 3. Wählen Sie die Registerkarte Test. (Verwenden Sie den Rechtspfeil, wenn die Registerkarte nicht angezeigt wird.) 4. Fügen Sie in das Feld Request body den folgenden JSON-Code ein: `{ "message": "lorem ipsum" }` 5. Wählen Sie Test aus. 6. Öffnen Sie die Amazon-SQS-Konsole. 7. Wählen Sie im Navigationsbereich Warteschlangen und dann Ihre Warteschlange aus. 8. Wählen Sie Nachrichten senden und empfangen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Abfragen von Nachrichten. 10. Wählen Sie Message (Nachricht)aus. Es sollte Folgendes anzeigen: `Body { "message": "lorem ipsum" }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie API Gateway mit einem Sonderzeichen.	Führen Sie einen Test aus, der Sonderzeichen (wie &) enthält, die in einer Nachricht nicht zulässig sind:
	1. Wählen Sie in der API Gateway Gateway-Konsole Ihre API aus.
	2. Wiederholen Sie den Test aus dem vorherigen Schritt, indem Sie den folgenden JSON-Code verwenden:
	`{ "message": "lorem ipsum &" }`
	3. Wählen Sie Test aus.
	Sie erhalten eine Fehlermeldung wie die folgende:
	`{ "Error": { "Code": "AccessDenied", "Message": "Access to the resource https://sqs.us-east-2.amazonaws.com/976166761794/Apg2 is denied.", "Type": "Sender" }, "RequestId": "e83c9c67-bcf6-5e9`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>a-91e9-c737094b17a
	b"
	}</pre>
	Das liegt daran, dass Sonderzeichen im Nachricht entext standardmäßig nicht unterstützt werden. Im nächsten Schritt konfigurieren Sie API Gateway so, dass es Sonderzeichen unterstüt zt. Weitere Informationen zu Inhaltstypkonvertierungen finden Sie in der API Gateway Gateway-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die API-Konfiguration, sodass Sonderzeichen unterstützt werden.	Passen Sie die Konfiguration so an, dass Sonderzeichen in der Nachricht akzeptiert werden: 1. Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben, und wählen Sie dann POST. 2. Wählen Sie Integrationsanforderung aus und klicken Sie dann auf Bearbeiten. 3. Ändern Sie die Inhaltsverwaltung in In Text konvertieren. 4. Gehen Sie im Abschnitt Mapping-Vorlagen wie folgt vor: • Geben Sie als Inhaltstyp application/json ein. • Geben Sie für Vorlagentext Folgendes an: `Action=SendMessage&MessageBody=$util.urlEncode($input.body)` • Wählen Sie Speichern. 5. Wählen Sie die Registerkarte Test.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie für Request body den JSON-Code von früher ein: `{ " message": "lorem ipsum &" }` 7. Wählen Sie Test aus. 8. Öffnen Sie die Amazon-SQS-Konsole. 9. Wählen Sie Ihre Warteschlange aus und wählen Sie dann Nachrichten senden und empfangen, Nach Nachrichten abfragen, Nachricht wie zuvor aus. Die neue Nachricht sollte das Sonderzeichen enthalten.	

Stellen Sie die REST-API bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die API bereit.	So stellen Sie die REST-API bereit: 1. Öffnen Sie die API Gateway-Konsole. 2. Wählen Sie Ihre API aus. 3. Klicken Sie auf Deploy API. Weitere Informationen zu diesem Schritt finden Sie in	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der API Gateway Gateway-Dokumentation.	
Testen Sie mit einem externen Tool.	Führen Sie einen Test mit einem externen Tool durch, um zu bestätigen, dass die Nachricht erfolgreich empfangen wurde: 1. Öffnen Sie ein Tool wie Postman, Insomnia oder cURL. 2. Führen Sie Ihre API aus. 3. Öffnen Sie die Amazon-SQS-Konsole. 4. Wählen Sie Ihre Warteschlange aus. 5. Laden Sie Nachrichten, um die neue Nachricht zu sehen.	App-Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die API.	Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben, und klicken Sie dann auf Löschen.	App-Developer
Löschen Sie die IAM-Rolle.	Wählen Sie in der IAM-Konsole im Bereich Rollen die Option und AWSGatewa	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	yRoleForSQSanschließend Löschen aus.	
Löschen Sie die SQS-Warteschlange.	Wählen Sie auf der Amazon SQS SQS-Konsole im Bereich Warteschlangen die SQS-Warteschlange aus, die Sie erstellt haben, und klicken Sie dann auf Löschen.	App-Developer

Zugehörige Ressourcen

- SQS- SendMessage (API Gateway Gateway-Dokumentation)
- Inhaltstypkonvertierungen in API Gateway (API Gateway Gateway-Dokumentation)
- $util-Variablen (API Gateway Gateway-Dokumentation)
- Wie integriere ich eine API Gateway Gateway-REST-API in Amazon SQS und behebe häufig auftretende Fehler? (AWS Re:POST-Artikel)

Asynchrone Verarbeitung von Ereignissen mit Amazon API Gateway und AWS Lambda

Erstellt von Andrea Meroni (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) und Michael Wallner (AWS)

Code-Repository: Asynchrone Eventverarbeitung mit API Gateway und Lambda	Umgebung: PoC oder Pilot	Technologien: Serverlos
AWS-Dienste: Amazon API Gateway; Amazon DynamoDB; AWS Lambda		

Übersicht

Amazon API Gateway ist ein vollständig verwalteter Service, den Entwickler zum Erstellen, Veröffentlichen, Verwalten, Überwachen und Sichern von APIs in jeder Größenordnung verwenden können. Es erledigt die Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind, einschließlich der folgenden:

- Verkehrsmanagement
- Unterstützung für Cross-Origin Resource Sharing (CORS)
- Autorisierung und Zugriffskontrolle
- Drosselung
- Überwachen
- API-Versionsverwaltung

Eine wichtige Servicequote von API Gateway ist das Integrations-Timeout. Das Timeout ist die maximale Zeit, in der ein Backend-Dienst eine Antwort zurückgeben muss, bevor die REST-API einen Fehler zurückgibt. Das feste Limit von 29 Sekunden ist für synchrone Workloads im Allgemeinen akzeptabel. Dieses Limit stellt jedoch eine Herausforderung für Entwickler dar, die API Gateway mit asynchronen Workloads verwenden möchten.

Dieses Muster zeigt eine Beispielarchitektur für die asynchrone Verarbeitung von Ereignissen mithilfe von API Gateway und AWS Lambda. Die Architektur unterstützt die Ausführung von Verarbeitungsaufträgen mit einer Dauer von bis zu 15 Minuten und verwendet eine einfache REST-API als Schnittstelle.

Projen wird verwendet, um die lokale Entwicklungsumgebung einzurichten und die Beispielarchitektur in Kombination mit dem AWS Cloud Development Kit (AWS CDK) Toolkit AWS-Konto, Docker und Node.js auf einem Ziel bereitzustellen. Projen richtet automatisch eine virtuelle Python-Umgebung mit Pre-Commit und den Tools ein, die für die Qualitätssicherung des Codes, Sicherheitsscans und Unit-Tests verwendet werden. Weitere Informationen finden Sie im Abschnitt Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Tools sind auf Ihrer Workstation installiert:
  - AWS Cloud Development Kit (AWS CDK) Toolkit-Version 2.85.0
  - Docker-Version 20.10.21
  - Node.js, Version 18.13.0
  - Bewährte Version 0.71.111
  - Python-Version 3.9.16

Einschränkungen

- Die maximale Laufzeit eines Jobs ist durch die maximale Laufzeit für Lambda-Funktionen (15 Minuten) begrenzt.
- Die maximale Anzahl gleichzeitiger Jobanfragen ist durch die reservierte Parallelität der Lambda-Funktion begrenzt.

Architektur

Das folgende Diagramm zeigt die Interaktion der Jobs-API mit den Lambda-Funktionen zur Ereignisverarbeitung und Fehlerbehandlung, wobei Ereignisse in einem Amazon-Ereignisarchiv gespeichert werden. EventBridge

Ein typischer Workflow umfasst die folgenden Schritte:

1. Sie authentifizieren sich bei AWS Identity and Access Management (IAM) und erhalten Sicherheitsanmeldedaten.
2. Sie senden eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt und geben dabei die Jobparameter im Hauptteil der Anfrage an.
3. Die Jobs-API, bei der es sich um eine API-Gateway-REST-API handelt, gibt Ihnen eine HTTP-Antwort zurück, die die Job-ID enthält.
4. Die Jobs-API ruft asynchron die Lambda-Funktion zur Ereignisverarbeitung auf.
5. Die Funktion zur Ereignisverarbeitung verarbeitet das Ereignis und fügt dann die Auftragsergebnisse in die Amazon DynamoDB-Tabelle der Jobs ein.
6. Sie senden eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt mit der Job-ID aus Schritt 3 als. `{jobId}`
7. Die Jobs-API fragt die `jobs` DynamoDB-Tabelle ab, um die Auftragsergebnisse abzurufen.
8. Die Jobs-API gibt eine HTTP-Antwort zurück, die die Auftragsergebnisse enthält.
9. Wenn die Ereignisverarbeitung fehlschlägt, sendet die Ereignisverarbeitungsfunktion das Ereignis an die Fehlerbehandlungsfunktion.
10. Die Fehlerbehandlungsfunktion platziert die Jobparameter in der `jobs` DynamoDB-Tabelle.
11. Sie können die Job-Parameter abrufen, indem Sie eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt senden.
12. Wenn die Fehlerbehandlung fehlschlägt, sendet die Fehlerbehandlungsfunktion das Ereignis an ein EventBridge Ereignisarchiv.

    Sie können die archivierten Ereignisse erneut abspielen, indem Sie. EventBridge

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Andere Tools

- autopep8 formatiert Python-Code automatisch auf der Grundlage des Python Enhancement Proposal (PEP) 8-Styleguides.
- Bandit scannt Python-Code, um häufig auftretende Sicherheitsprobleme zu finden.
- Commitizen ist ein Git-Commit-Checker und -Generator. `CHANGELOG`
- cfn-lint ist ein Linter AWS CloudFormation
- Checkov ist ein statisches Code-Analyse-Tool, das Infrastructure as Code (IaC) auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- jq ist ein Befehlszeilentool zum Parsen von JSON.
- Postman ist eine API-Plattform.
- pre-commit ist ein Git-Hooks-Manager.
- Projen ist ein Projektgenerator.
- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.

Code-Repository

Dieser Beispielarchitekturcode befindet sich im Repository GitHub Asynchronous Event Processing with API Gateway and Lambda.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachung der bereitgestellten Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von CDK Monitoring Constructs oder einer anderen Überwachungslösung in Betracht ziehen.
- Diese Beispielarchitektur verwendet IAM-Berechtigungen, um den Zugriff auf die Jobs-API zu steuern. Jeder, der autorisiert ist, `JobsAPIInvokeRole` dies anzunehmen, kann die Jobs-API aufrufen. Daher ist der Zugriffskontrollmechanismus binär. Wenn Ihr

Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, sollten Sie es mit einem anderen Zugriffskontrollmechanismus testen.

- Wenn ein Benutzer eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt sendet, werden die Eingabedaten auf zwei verschiedenen Ebenen validiert:
  - Amazon API Gateway ist für die erste Anforderungsvalidierung verantwortlich.
  - Die Funktion zur Ereignisverarbeitung führt die zweite Anfrage durch.

  Es wird keine Überprüfung durchgeführt, wenn der Benutzer eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt sendet. Wenn Ihr Anwendungsfall eine zusätzliche Eingabevalidierung und ein höheres Maß an Sicherheit erfordert, sollten Sie die Verwendung von AWS WAF zum Schutz Ihrer API in Betracht ziehen.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository lokal zu klonen: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-lambda-cdk.git`	DevOps Ingenieur
Richten Sie das Projekt ein.	Ändern Sie das Verzeichnis in das Repository-Stammverzeichnis und richten Sie die virtuelle Python-Umgebung und alle Tools mithilfe von Projen ein: `cd asynchronous-event-processing-api-ga`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`teway-api-gateway-lambda-cdk` `npx projen`	

Installieren Sie Pre-Commit-Hooks.	Gehen Sie wie folgt vor, um Pre-Commit-Hooks zu installieren:
	1. Aktivieren Sie die virtuelle Python-Umgebung:
	`source .env/bin/activate`
	2. Installieren Sie die Pre-Commit-Hooks:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps Ingenieur

Stellen Sie die Beispielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	Um AWS CDK in Ihrem zu booten AWS-Konto, führen Sie den folgenden Befehl aus: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Stellen Sie die Beispielarchitektur bereit.	Führen Sie den folgenden Befehl aus AWS-Konto, um	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Beispielarchitektur in Ihrem bereitzustellen: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Testvorau ssetzungen.	Installieren Sie auf Ihrer Workstation the AWS Command Line Interface (AWS CLI), Postman und jq. Die Verwendung von Postman zum Testen dieser Beispiela rchitektur wird empfohlen , ist aber nicht zwingend erforderlich. Wenn Sie sich für ein alternatives API-Testt ool entscheiden, stellen Sie sicher, dass es die Authentif izierung mit AWS Signature Version 4 unterstützt, und beziehen Sie sich auf die exponierten API-Endpunkte, die durch den Export der REST-API überprüft werden können.	DevOps Ingenieur
Gehen Sie von der ausJobsAPIInvokeRole .	Gehen Sie davon ausJobsAPIInvokeRole , dass das als Ausgabe des	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Befehls deploy gedruckt wurde: `CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Postman konfigurieren.	1. Folgen Sie den Anweisungen in der Postman-Dokumentation, um die im Repository enthaltene Postman-Sammlung zu importieren. 2. Stellen Sie die `JobsAPI` Variablen mit den folgenden Werten ein: • `accessKey` – Der Wert des `Credentials.AccessKeyId` Attributs aus dem `assume-role` Befehl • `baseUrl`– Der Wert der `JobsApiJobsAPIEndpoint` Ausgabe des Befehls deploy ohne den abschließenden Schrägstrich • `region`– Der Wert der AWS-Region Stelle, an der Sie die Beispielarchitektur bereitgestellt haben • `seconds`– Der Wert des Eingabeparameters für den Beispieljob. Es muss eine positive Ganzzahl sein • `secretKey` – Der Wert des `Credentials.Secret`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AccessKey` Attributs aus dem `assume-role` Befehl • `sessionToken` – Der Wert des `Credentials.SessionToken` Attributs aus dem `assume-role` Befehl	
Testen Sie die Beispielarchitektur.	Um die Beispielarchitektur zu testen, senden Sie Anfragen an die Jobs-API. Weitere Informationen finden Sie in der Postman-Dokumentation.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Amazon CloudWatch Logs-Protokollgruppe `/aws/apigateway/JobsAPIAccessLogs` bereits existiert.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon S3. 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Stellen Sie die Beispielarchitektur erneut bereit.

Zugehörige Ressourcen

- API-Gateway-Zuordnungsvorlage und Referenz zur Zugriffsprotokollierungsvariablen
- Richten Sie den asynchronen Aufruf der Backend-Lambda-Funktion ein

Ereignisse asynchron mit Amazon API Gateway und Amazon DynamoDB Streams verarbeiten

Erstellt von Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) und Michael Wallner (AWS)

Code-Repository: Asynchrone Verarbeitung mit API Gateway und DynamoDB Streams	Umgebung: PoC oder Pilot	Technologien: Serverlos
AWS-Services: Amazon API Gateway; Amazon DynamoDB; Amazon DynamoDB DynamoDB-Streams; AWS Lambda; Amazon SNS		

Übersicht

Amazon API Gateway ist ein vollständig verwalteter Service, den Entwickler zum Erstellen, Veröffentlichen, Verwalten, Überwachen und Sichern von APIs in jeder Größenordnung verwenden können. Es erledigt die Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind, darunter die folgenden:

- Verkehrsmanagement
- Unterstützung für Cross-Origin Resource Sharing (CORS)
- Autorisierung und Zugriffskontrolle
- Drosselung
- Überwachen
- API-Versionsverwaltung

Eine wichtige Servicequote von API Gateway ist das Integrations-Timeout. Das Timeout ist die maximale Zeit, in der ein Backend-Dienst eine Antwort zurückgeben muss, bevor die REST-API einen

Fehler zurückgibt. Das feste Limit von 29 Sekunden ist für synchrone Workloads im Allgemeinen akzeptabel. Dieses Limit stellt jedoch eine Herausforderung für Entwickler dar, die API Gateway mit asynchronen Workloads verwenden möchten.

Dieses Muster zeigt eine Beispielarchitektur für die asynchrone Verarbeitung von Ereignissen mithilfe von API Gateway, Amazon DynamoDB Streams und. AWS Lambda Die Architektur unterstützt die Ausführung von Parallelverarbeitungsjobs mit denselben Eingabeparametern und verwendet eine grundlegende REST-API als Schnittstelle. In diesem Beispiel begrenzt die Verwendung von Lambda als Backend die Dauer von Jobs auf 15 Minuten. Sie können dieses Limit umgehen, indem Sie einen alternativen Dienst zur Verarbeitung eingehender Ereignisse verwenden (z. B. AWS Fargate).

Projen wird verwendet, um die lokale Entwicklungsumgebung einzurichten und die Beispielarchitektur in Kombination mit dem AWS Cloud Development Kit (AWS CDK) Toolkit AWS-Konto, Docker und Node.js auf einem Ziel bereitzustellen. Projen richtet automatisch eine virtuelle Python-Umgebung mit Pre-Commit und den Tools ein, die für die Qualitätssicherung des Codes, Sicherheitsscans und Unit-Tests verwendet werden. Weitere Informationen finden Sie im Abschnitt Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Tools sind auf Ihrer Workstation installiert:
  - AWS Cloud Development Kit (AWS CDK) Toolkit-Version 2.85.0 oder höher
  - Docker-Version 20.10.21 oder höher
  - Node.js Version 18 oder höher
  - Projen Version 0.71.111 oder höher
  - Python-Version 3.9.16 oder höher

Einschränkungen

- Die empfohlene maximale Anzahl von Lesern für DynamoDB Streams ist zwei, um eine Drosselung zu vermeiden.
- Die maximale Laufzeit eines Jobs ist durch die maximale Laufzeit für Lambda-Funktionen (15 Minuten) begrenzt.
- Die maximale Anzahl gleichzeitiger Jobanfragen ist durch die reservierte Parallelität der Lambda-Funktionen begrenzt.

Architektur

Architektur

Das folgende Diagramm zeigt die Interaktion der Jobs-API mit DynamoDB Streams und den Lambda-Funktionen zur Ereignisverarbeitung und Fehlerbehandlung mit Ereignissen, die in einem Amazon-Ereignisarchiv gespeichert sind. EventBridge

Ein typischer Arbeitsablauf umfasst die folgenden Schritte:

1. Sie authentifizieren sich bei AWS Identity and Access Management (IAM) und erhalten Sicherheitsanmeldedaten.
2. Sie senden eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt und geben dabei die Jobparameter im Hauptteil der Anfrage an.
3. Die Jobs-API gibt Ihnen eine HTTP-Antwort zurück, die die Job-ID enthält.
4. Die Job-API platziert die Job-Parameter in der `jobs_table` Amazon DynamoDB-Tabelle.
5. Der `jobs_table` DynamoDB-Stream der DynamoDB-Tabelle ruft die Lambda-Funktionen zur Ereignisverarbeitung auf.
6. Die Lambda-Funktionen zur Ereignisverarbeitung verarbeiten das Ereignis und fügen dann die Auftragsergebnisse in die `jobs_table` DynamoDB-Tabelle ein. Um konsistente Ergebnisse zu gewährleisten, implementieren die Funktionen zur Ereignisverarbeitung einen optimistischen Sperrmechanismus.
7. Sie senden eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt mit der Job-ID aus Schritt 3 als. `{jobId}`
8. Die Jobs-API fragt die `jobs_table` DynamoDB-Tabelle ab, um die Auftragsergebnisse abzurufen.
9. Die Jobs-API gibt eine HTTP-Antwort zurück, die die Auftragsergebnisse enthält.
10. Wenn die Ereignisverarbeitung fehlschlägt, sendet die Quellenzuordnung der Ereignisverarbeitungsfunktion das Ereignis an das Thema Amazon Simple Notification Service (Amazon SNS) zur Fehlerbehandlung.
11. Das SNS-Thema zur Fehlerbehandlung überträgt das Ereignis asynchron an die Fehlerbehandlungsfunktion.
12. Die Fehlerbehandlungsfunktion platziert die Jobparameter in der `jobs_table` DynamoDB-Tabelle.

Sie können die Job-Parameter abrufen, indem Sie eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt senden.

13. Wenn die Fehlerbehandlung fehlschlägt, sendet die Fehlerbehandlungsfunktion das Ereignis an ein EventBridge Amazon-Archiv.

    Sie können die archivierten Ereignisse erneut abspielen, indem Sie. EventBridge

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS-Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Andere Tools

- autopep8 formatiert Python-Code automatisch auf der Grundlage des Python Enhancement Proposal (PEP) 8-Styleguides.
- Bandit scannt Python-Code, um häufig auftretende Sicherheitsprobleme zu finden.
- Commitizen ist ein Git-Commit-Checker und -Generator. `CHANGELOG`
- cfn-lint ist ein Linter AWS CloudFormation

- Checkov ist ein statisches Code-Analyse-Tool, das Infrastructure as Code (IaC) auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- jq ist ein Befehlszeilentool zum Parsen von JSON.
- Postman ist eine API-Plattform.
- pre-commit ist ein Git-Hooks-Manager.
- Projen ist ein Projektgenerator.
- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.

Code-Repository

Dieser Beispielarchitekturcode befindet sich im Repository GitHub Asynchronous Processing with API Gateway und DynamoDB Streams.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachung der bereitgestellten Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von CDK Monitoring Constructs oder einer anderen Überwachungslösung in Betracht ziehen.
- Diese Beispielarchitektur verwendet IAM-Berechtigungen, um den Zugriff auf die Jobs-API zu steuern. Jeder, der autorisiert ist, `JobsAPIInvokeRole` dies anzunehmen, kann die Jobs-API aufrufen. Daher ist der Zugriffskontrollmechanismus binär. Wenn Ihr Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, sollten Sie es mit einem anderen Zugriffskontrollmechanismus testen.
- Wenn ein Benutzer eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt sendet, werden die Eingabedaten auf zwei verschiedenen Ebenen validiert:
  - API Gateway ist für die erste Anforderungsvalidierung verantwortlich.
  - Die Funktion zur Ereignisverarbeitung führt die zweite Anfrage aus.

    Es wird keine Überprüfung durchgeführt, wenn der Benutzer eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt sendet. Wenn Ihr Anwendungsfall eine zusätzliche Eingabevalidierung und ein erhöhtes Sicherheitsniveau erfordert, sollten Sie den Einsatz AWS WAF zum Schutz Ihrer API in Betracht ziehen.

- Um Drosselung zu vermeiden, rät die DynamoDB Streams-Dokumentation Benutzern davon ab, mit mehr als zwei Verbrauchern vom Shard desselben Streams zu lesen. Um die Anzahl der Verbraucher zu erhöhen, empfehlen wir die Verwendung von Amazon Kinesis Data Streams.
- In diesem Beispiel wurde optimistisches Sperren verwendet, um sicherzustellen, dass Elemente in der `jobs_table` DynamoDB-Tabelle konsistent aktualisiert werden. Je nach Anforderung des Anwendungsfalls müssen Sie möglicherweise zuverlässigere Sperrmechanismen implementieren, z. B. pessimistisches Sperren.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository lokal zu klonen: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-dynamodb-streams-cdk.git`	DevOps Ingenieur

Richten Sie das Projekt ein.	Ändern Sie das Verzeichnis in das Repository-Stammverzeichnis und richten Sie die virtuelle Python-Umgebung und alle Tools mithilfe von Projen ein:
	`cd asynchronous-event-processing-api-gateway-api-gateway-dynamodb-streams-cdk`
	`npx projen`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Pre-Commit-Hooks.	Gehen Sie wie folgt vor, um Pre-Commit-Hooks zu installieren:
	1. Aktivieren Sie die virtuelle Python-Umgebung:
	`source .env/bin/activate`
	2. Installieren Sie die Pre-Commit-Hooks:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps Ingenieur

Stellen Sie die Beispielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	Um AWS CDKin Ihrem zu booten AWS-Konto, führen Sie den folgenden Befehl aus: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Stellen Sie die Beispielarchitektur bereit.	Führen Sie den folgenden Befehl aus AWS-Konto, um die Beispielarchitektur in Ihrem bereitzustellen:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Testvorausetzungen.	Installieren Sie auf Ihrer Workstation the AWS Command Line Interface (AWS CLI), Postman und jq. Die Verwendung von Postman zum Testen dieser Beispielarchitektur wird empfohlen, ist aber nicht zwingend erforderlich. Wenn Sie sich für ein alternatives API-Testtool entscheiden, stellen Sie sicher, dass es die AWS Signature Version 4-Authentifizierung unterstützt, und verweisen Sie auf die exponierten API-Endpunkte, die durch Exportieren der REST-API überprüft werden können.	DevOps Ingenieur
Gehen Sie von der aus`JobsAPIInvokeRole` .	Gehen Sie davon aus`JobsAPIInvokeRole` , dass das als Ausgabe des `deploy` Befehls gedruckt wurde:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Postman konfigurieren.	• Folgen Sie den Anweisungen in der Postman-Dokumentation, um die im Repository enthaltene Postman-Sammlung zu importieren.
	• Stellen Sie die `JobsAPI` Variablen mit den folgenden Werten ein:
	  • `accessKey` – Der Wert des `Credentials.AccessKeyId` Attributs aus dem `assume-role` Befehl.
	  • `baseUrl`– Der Wert der `JobsApiJobsAPIEndpoint` `deploy` Befehlsausgabe ohne den abschließenden Schrägstrich.
	  • `region`– Der Wert der AWS-Region Stelle, an der Sie die Beispielarchitektur bereitgestellt haben.
	  • `seconds`– Der Wert des Eingabeparameters für den Beispieljob. Es muss eine positive Ganzzahl sein.
	  • `secretKey` – Der Wert des `Credentials.Secret`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AccessKey` Attributs aus dem `assume-role` Befehl. • `sessionToken` – Der Wert des `Credentials.SessionToken` Attributs aus dem `assume-role` Befehl.	
Testen Sie die Beispielarchitektur.	Um die Beispielarchitektur zu testen, senden Sie Anfragen an die Jobs-API. Weitere Informationen finden Sie in der Postman-Dokumentation.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Amazon CloudWatch Logs-Protokollgruppe `/aws/apigateway/JobsAPIAccessLogs` bereits existiert.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon Simple Storage Service (Amazon S3). 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Stellen Sie die Beispielarchitektur erneut bereit.

Zugehörige Ressourcen

- API-Gateway-Zuordnungsvorlage und Referenz zur Zugriffsprotokollierungsvariablen
- Erfassung von Änderungsdaten für DynamoDB Streams

- Optimistisches Sperren mit Versionsnummer
- Verwenden von Kinesis Data Streams zur Erfassung von Änderungen an DynamoDB

Ereignisse asynchron mit Amazon API Gateway, Amazon SQS und AWS Fargate verarbeiten

Erstellt von Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) und Michael Wallner (AWS)

Code-Repository: Asynchrone Ereignisverarbeitung mit API Gateway und SQS	Umgebung: PoC oder Pilotprojekt	Technologien: Serverlos
AWS-Dienste: Amazon API Gateway; Amazon DynamoDB; AWS Fargate; Amazon SQS; AWS Lambda		

Übersicht

Amazon API Gateway ist ein vollständig verwalteter Service, den Entwickler zum Erstellen, Veröffentlichen, Verwalten, Überwachen und Sichern von APIs in jeder Größenordnung verwenden können. Es erledigt die Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind, darunter die folgenden:

- Verkehrsmanagement
- Unterstützung für Cross-Origin Resource Sharing (CORS)
- Autorisierung und Zugriffskontrolle
- Drosselung
- Überwachen
- API-Versionsverwaltung

Eine wichtige Servicequote von API Gateway ist das Integrations-Timeout. Das Timeout ist die maximale Zeit, in der ein Backend-Dienst eine Antwort zurückgeben muss, bevor die REST-API einen Fehler zurückgibt. Das feste Limit von 29 Sekunden ist für synchrone Workloads im Allgemeinen akzeptabel. Dieses Limit stellt jedoch eine Herausforderung für Entwickler dar, die API Gateway mit asynchronen Workloads verwenden möchten.

Dieses Muster zeigt eine Beispielarchitektur für die asynchrone Verarbeitung von Ereignissen mithilfe von API Gateway, Amazon Simple Queue Service (Amazon SQS) und. AWS Fargate Die Architektur unterstützt die Ausführung von Verarbeitungsaufträgen ohne zeitliche Einschränkungen und verwendet eine einfache REST-API als Schnittstelle.

Projen wird verwendet, um die lokale Entwicklungsumgebung einzurichten und die Beispielarchitektur in Kombination mit Docker und Node.js AWS Cloud Development Kit (AWS CDK)auf einem Ziel AWS-Konto bereitzustellen. Projen richtet automatisch eine virtuelle Python-Umgebung mit Pre-Commit und den Tools ein, die für die Qualitätssicherung des Codes, Sicherheitsscans und Unit-Tests verwendet werden. Weitere Informationen finden Sie im Abschnitt Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Tools sind auf Ihrer Workstation installiert:
  - AWS Cloud Development Kit (AWS CDK) Toolkit-Version 2.85.0 oder höher
  - Docker-Version 20.10.21 oder höher
  - Node.js Version 18 oder höher
  - Projen Version 0.71.111 oder höher
  - Python-Version 3.9.16 oder höher

Einschränkungen

- Gleichzeitige Jobs sind auf 500 Aufgaben pro Minute begrenzt. Dies ist die maximale Anzahl von Aufgaben, die Fargate bereitstellen kann.

Architektur

Das folgende Diagramm zeigt die Interaktion der Jobs-API mit der `jobs` Amazon DynamoDB-Tabelle, dem Fargate-Dienst zur Ereignisverarbeitung und der Fehlerbehandlungsfunktion. AWS Lambda Ereignisse werden in einem EventBridge Amazon-Eventarchiv gespeichert.

Ein typischer Arbeitsablauf umfasst die folgenden Schritte:

1. Sie authentifizieren sich bei AWS Identity and Access Management (IAM) und erhalten Sicherheitsanmeldedaten.
2. Sie senden eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt und geben dabei die Jobparameter im Hauptteil der Anfrage an.
3. Die Jobs-API, bei der es sich um eine API-Gateway-REST-API handelt, gibt Ihnen eine HTTP-Antwort zurück, die die Job-ID enthält.
4. Die Jobs-API sendet eine Nachricht an die SQS-Warteschlange.
5. Fargate ruft die Nachricht aus der SQS-Warteschlange ab, verarbeitet das Ereignis und fügt dann die Auftragsergebnisse in die `jobs` DynamoDB-Tabelle ein.
6. Sie senden eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt mit der Job-ID aus Schritt 3 als. `{jobId}`
7. Die Jobs-API fragt die `jobs` DynamoDB-Tabelle ab, um die Auftragsergebnisse abzurufen.
8. Die Jobs-API gibt eine HTTP-Antwort zurück, die die Auftragsergebnisse enthält.
9. Wenn die Ereignisverarbeitung fehlschlägt, sendet die SQS-Warteschlange das Ereignis an die Dead-Letter-Warteschlange (DLQ).
10. Ein EventBridge Ereignis initiiert die Fehlerbehandlungsfunktion.
11. Die Fehlerbehandlungsfunktion platziert die Jobparameter in der `jobs` DynamoDB-Tabelle.
12. Sie können die Job-Parameter abrufen, indem Sie eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt senden.
13. Wenn die Fehlerbehandlung fehlschlägt, sendet die Fehlerbehandlungsfunktion das Ereignis an ein EventBridge Archiv.

    Sie können die archivierten Ereignisse erneut abspielen, indem Sie EventBridge

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung von AWS Cloud Infrastruktur im Code unterstützt.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

- AWS Fargatehilft Ihnen dabei, Container auszuführen, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Andere Tools

- autopep8 formatiert Python-Code automatisch auf der Grundlage des Python Enhancement Proposal (PEP) 8-Styleguides.
- Bandit scannt Python-Code, um häufig auftretende Sicherheitsprobleme zu finden.
- Commitizen ist ein Git-Commit-Checker und -Generator. `CHANGELOG`
- cfn-lint ist ein Linter AWS CloudFormation
- Checkov ist ein statisches Code-Analyse-Tool, das Infrastructure as Code (IaC) auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- jq ist ein Befehlszeilentool zum Parsen von JSON.
- Postman ist eine API-Plattform.
- pre-commit ist ein Git-Hooks-Manager.
- Projen ist ein Projektgenerator.
- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.

Code-Repository

Dieser Beispielarchitekturcode befindet sich im Repository GitHub Asynchronous Processing with API Gateway und SQS.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachung der bereitgestellten Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von CDK Monitoring Constructs oder einer anderen Überwachungslösung in Betracht ziehen.
- Diese Beispielarchitektur verwendet IAM-Berechtigungen, um den Zugriff auf die Jobs-API zu steuern. Jeder, der autorisiert ist, `JobsAPIInvokeRole` dies anzunehmen, kann die Jobs-API aufrufen. Daher ist der Zugriffskontrollmechanismus binär. Wenn Ihr Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, sollten Sie es mit einem anderen Zugriffskontrollmechanismus testen.
- Wenn ein Benutzer eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt sendet, werden die Eingabedaten auf zwei verschiedenen Ebenen validiert:
  - API Gateway ist für die erste Anforderungsvalidierung verantwortlich.
  - Die Funktion zur Ereignisverarbeitung führt die zweite Anfrage aus.

    Es wird keine Überprüfung durchgeführt, wenn der Benutzer eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt sendet. Wenn Ihr Anwendungsfall eine zusätzliche Eingabevalidierung und ein erhöhtes Sicherheitsniveau erfordert, sollten Sie den Einsatz AWS WAF zum Schutz Ihrer API in Betracht ziehen.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository lokal zu klonen: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-sqs-cdk.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das Projekt ein.	Ändern Sie das Verzeichnis in das Repository-Stammverzeichnis und richten Sie die virtuelle Python-Umgebung und alle Tools mithilfe von Projen ein:
	`cd asynchronous-event-processing-api-gateway-api-gateway-sqs-cdk`
	`npx projen`
		DevOps Ingenieur

Installieren Sie Pre-Commit-Hooks.	Gehen Sie wie folgt vor, um Pre-Commit-Hooks zu installieren:
	1. Aktivieren Sie die virtuelle Python-Umgebung:
	`source .env/bin/activate`
	2. Installieren Sie die Pre-Commit-Hooks:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps Ingenieur

Stellen Sie die Beispielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	Um AWS CDKin Ihrem zu booten AWS-Konto, führen Sie den folgenden Befehl aus: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen bootstrap`	AWS DevOps
Stellen Sie die Beispiela rchitektur bereit.	Führen Sie den folgenden Befehl aus AWS-Konto, um die Beispielarchitektur in Ihrem bereitzustellen: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	AWS DevOps

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Testvorau ssetzungen.	Installieren Sie auf Ihrer Workstation the AWS Command Line Interface (AWS CLI), Postman und jq. Die Verwendung von Postman zum Testen dieser Beispiela rchitektur wird empfohlen , ist aber nicht zwingend erforderlich. Wenn Sie sich für ein alternatives API-Testt ool entscheiden, stellen Sie	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sicher, dass es die Authentifizierung mit AWS Signature Version 4 unterstützt, und beziehen Sie sich auf die exponierten API-Endpunkte, die durch den Export der REST-API überprüft werden können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie von der aus`JobsAPIInvokeRole` .	Gehen Sie davon aus`JobsAPIInvokeRole` , dass das als Ausgabe des `deploy` Befehls gedruckt wurde: `CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Postman konfigurieren.	• Folgen Sie den Anweisungen in der Postman-Dokumentation, um die im Repository enthaltene Postman-Sammlung zu importieren.
	• Stellen Sie die `JobsAPI` Variablen mit den folgenden Werten ein:
	  • `accessKey` – Der Wert des `Credentials.AccessKeyId` Attributs aus dem `assume-role` Befehl.
	  • `baseUrl`– Der Wert der `JobsApiJobsAPIEndpoint` `deploy` Befehlsausgabe ohne den abschließenden Schrägstrich.
	  • `region`– Der Wert der AWS-Region Stelle, an der Sie die Beispielarchitektur bereitgestellt haben.
	  • `seconds`– Der Wert des Eingabeparameters für den Beispieljob. Es muss eine positive Ganzzahl sein.
	  • `secretKey` – Der Wert des `Credentials.Secret`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AccessKey` Attributs aus dem `assume-role` Befehl. • `sessionToken` – Der Wert des `Credentials.SessionToken` Attributs aus dem `assume-role` Befehl.	
Testen Sie die Beispielarchitektur.	Um die Beispielarchitektur zu testen, senden Sie Anfragen an die Jobs-API. Weitere Informationen finden Sie in der Postman-Dokumentation.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Amazon CloudWatch Logs-Protokollgruppe `/aws/apigateway/JobsAPIAccessLogs` bereits existiert.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon Simple Storage Service (Amazon S3). 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Stellen Sie die Beispielarchitektur erneut bereit.
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Protokollgruppe CloudWatch Logs `/aws/ecs/EventProcessingServiceLogs` bereits vorhanden ist.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon S3. 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/ecs/EventProcessingServiceLogs.`

Problem	Lösung
	3. Stellen Sie die Beispielarchitektur erneut bereit.

Zugehörige Ressourcen

- API-Gateway-Zuordnungsvorlage und Referenz zur Zugriffsprotokollierungsvariablen
- Wie integriere ich eine API Gateway Gateway-REST-API in Amazon SQS und behebe häufig auftretende Fehler?

Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus

Erstellt von Elie El khoury (AWS)

Code-Repository: amazon-stepfunctions-ssm-waitfortasktoken	Umgebung: Produktion	Technologien: Serverlos DevOps; Datenverarbeitung für Endbenutzer; Betrieb
AWS-Services: AWS Step Functions; AWS Systems Manager		

Übersicht

Dieses Muster erklärt die Integration AWS Step Functions mit AWS Systems Manager. Es verwendet AWS SDK-Dienstintegrationen, um die Systems Manager startAutomationExecutionManager-API mit einem Task-Token aus einem State-Machine-Workflow aufzurufen, und pausiert, bis das Token mit einem erfolgreichen oder fehlerhaften Aufruf zurückkehrt. Um die Integration zu demonstrieren, implementiert dieses Muster einen Wrapper für Automatisierungsdokumente (Runbook) um das `AWS-RunPowerShellScript` OR-Dokument und wird verwendet`.waitForTaskToken`, um `AWS-RunShellScript` oder synchron aufzurufen. `AWS-RunShellScript` `AWS-RunPowerShellScript` Weitere Informationen zu AWS SDK-Dienstintegrationen in Step Functions finden Sie im AWS Step Functions Entwicklerhandbuch.

Step Functions ist ein visueller Workflow-Dienst mit geringem Programmieraufwand, mit dem Sie mithilfe von Diensten verteilte Anwendungen erstellen, IT- und Geschäftsprozesse automatisieren und Daten- und Machine-Learning-Pipelines erstellen können. AWS Workflows verwalten Fehler, Wiederholungen, Parallelisierung, Serviceintegrationen und Beobachtbarkeit, sodass Sie sich auf die wertvollere Geschäftslogik konzentrieren können.

Automatisierung, eine Funktion von AWS Systems Manager, vereinfacht allgemeine Wartungs-, Bereitstellungs- und Problembehebungsaufgaben für AWS-Services Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift und Amazon Simple Storage Service (Amazon S3). Durch die Automatisierung haben Sie eine detaillierte Kontrolle

über die Parallelität Ihrer Automatisierungen. Sie können beispielsweise angeben, auf wie viele Ressourcen gleichzeitig zugegriffen werden soll und wie viele Fehler auftreten können, bevor eine Automatisierung gestoppt wird.

Einzelheiten zur Implementierung, einschließlich Runbook-Schritten, Parametern und Beispielen, finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Konto AWS
- AWS Identity and Access Management (IAM) -Berechtigungen für den Zugriff auf Step Functions und Systems Manager
- Eine EC2-Instanz, auf der Systems Manager Agent (SSM Agent) installiert ist
- Ein IAM-Instanzprofil für Systems Manager, das an die Instance angehängt ist, auf der Sie das Runbook ausführen möchten
- Eine Step Functions Functions-Rolle mit den folgenden IAM-Berechtigungen (die dem Prinzip der geringsten Rechte folgen):

```
{
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "*"
 }
```

Produktversionen

- SSM-Dokumentschema Version 0.3 oder höher
- SSM Agent Version 2.3.672.0 oder höher

Architektur

Zieltechnologie-Stack

- AWS Step Functions
- AWS Systems Manager -Automatisierung

Zielarchitektur

Automatisierung und Skalierung

- Dieses Muster bietet eine AWS CloudFormation Vorlage, mit der Sie die Runbooks auf mehreren Instanzen bereitstellen können. (Weitere Informationen finden Sie im Implementierungs-Repository von GitHub Step Functions und Systems Manager.)

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, sie zu verwenden.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt werden. AWS Cloud Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.

Code

Der Code für dieses Muster ist im Implementierungs-Repository von GitHub Step Functions und Systems Manager verfügbar.

Epen

Runbooks erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie die `ssm-automation-documents.cfn.json` Vorlage aus dem `cloudformation` Ordner des GitHub Repositorys herunter.	AWS DevOps
Runbooks erstellen.	Melden Sie sich bei der an AWS Management Console, öffnen Sie die AWS CloudFormation Konsole und stellen Sie die Vorlage bereit. Weitere Informationen zum Bereitstellen von CloudFormation Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der AWS CloudFormation Konsole. Die CloudFormation Vorlage stellt drei Ressourcen bereit: • `SfnRunCommandByInstanceIds` — Runbook, mit dem Sie `AWS-RunShellScript` Instanz-IDs ausführen oder `AWS-RunPowerShellScript` verwenden können.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `SfnRunCommandByTargets` — Runbook, mit dem Sie Ziele ausführen `AWS-RunShellScript` oder `AWS-RunPowerShellScript` verwenden können. • `SSMSyncRole` — Die von den Runbooks übernommene IAM-Rolle.	

Erstellen Sie eine Beispiel-Zustandsmaschine

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Teststatus-Maschine.	Folgen Sie den Anweisungen im AWS Step Functions Entwicklerhandbuch, um einen State Machine zu erstellen und auszuführen. Verwenden Sie für die Definition den folgenden Code. Achten Sie darauf, den `InstanceIds` Wert mit der ID einer gültigen Systems Manager-fähigen Instanz in Ihrem Konto zu aktualisieren. `{ "Comment": "A description of my state machine", "StartAt": "StartAutomationWaitForCallBack", "States": {`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"StartAutomationWaitForCallBack": {
	"Type": "Task",
	"Resource": "arn:aws:states:::aws-sdk:ssm:startAutomationExecution.waitForTaskToken",
	"Parameters": {
	"DocumentName": "SfnRunCommandByInstanceIds",
	"Parameters": {
	"InstanceIds": [
	"i-1234567890abcdef0"
	],
	"taskToken.$": "States.Array($$.Task.Token)",
	"workingDirectory": [
	"/home/ssm-user/"
	],
	"Commands": [
	"echo \"This is a test running automation waitForTaskToken\" >> automation.log",
	"sleep 100"
	],
	"executionTimeout": [
	"10800"
	],
	"deliveryTimeout": [
	"30"
	],</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"shell": [
	"Shell"
	]
	}
	},
	"End": true
	}
	}
	}</pre>
	Dieser Code ruft das Runbook auf, um zwei Befehle auszuführen, die den `waitForTaskToken` Aufruf von Systems Manager Automation demonstrieren.
	
	Der `shell` Parameterwert (`Shell`oder`PowerShell`) bestimmt, ob das Automatisierungsdokument ausgeführt wird `AWS-RunShellScript` oder`AWS-RunPowerShellScript`.
	
	Die Aufgabe schreibt „Dies ist ein waitForTask Automatisierungstoken für die Testausführung“ in die `/home/ssm-user/automation.log` Datei und ruht dann 100 Sekunden lang, bevor sie mit dem Aufgabentoken antwortet und die nächste Aufgabe im Workflow freigibt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie stattdessen das `SfnRunCommandByTargets` Runbook aufrufen möchten, ersetzen Sie den `Parameters` Abschnitt des vorherigen Codes durch den folgenden: `"Parameters": { "Targets": [ { "Key": "InstanceIds", "Values": [ "i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE" ] } ],`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die IAM-Rolle für den State Machine.	Im vorherigen Schritt wird automatisch eine dediziert e IAM-Rolle für den State Machine erstellt. Es gewährt jedoch keine Berechtigungen zum Aufrufen des Runbooks. Aktualisieren Sie die Rolle, indem Sie die folgenden Berechtigungen hinzufügen: `{ "Effect": "Allow", "Action": "ssm:StartAutomationExecution", "Resource": "*" }`	AWS DevOps
Validieren Sie die synchronen Aufrufe.	Führen Sie die Zustandsmaschine aus, um den synchronen Aufruf zwischen Step Functions und Systems Manager Automation zu validieren. Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen.	AWS DevOps

Zugehörige Ressourcen

- Erste Schritte mit AWS Step Functions (AWS Step Functions Entwicklerhandbuch)
- Warten Sie auf einen Rückruf mit dem Task-Token (AWS Step Functions Developer Guide, Service Integration Patterns)
- API-Aufrufe send_task_success und send_task_failure (Boto3-Dokumentation)

- AWS Systems Manager Automatisierung AWS Systems Manager (Benutzerhandbuch)

Zusätzliche Informationen

Implementierungsinformationen

Dieses Muster stellt eine CloudFormation Vorlage bereit, die zwei Systems Manager Manager-Runbooks bereitstellt:

- `SfnRunCommandByInstanceIds`führt den `AWS-RunPowerShellScript` Befehl `AWS-RunShellScript` or mithilfe von Instanz-IDs aus.
- `SfnRunCommandByTargets`führt den `AWS-RunPowerShellScript` Befehl `AWS-RunShellScript` or mithilfe von Zielen aus.

Jedes Runbook implementiert vier Schritte, um einen synchronen Aufruf zu erreichen, wenn die `.waitForTaskToken` Option in Step Functions verwendet wird.

Schritt	Action (Aktion)	Beschreibung
1	`Branch`	Prüft den `shell` Parameter wert (`Shell`oder`PowerShell`), um zu entscheiden, ob die Ausführung `AWS-RunShellScript` für Linux oder `AWS-RunPowerShellScript` für Windows erfolgen soll.
2	`RunCommand_Shell` oder `RunCommand_PowerShell`	Nimmt mehrere Eingaben entgegen und führt den `RunPowerShellScript` Befehl `RunShellScript` oder aus. Weitere Informationen finden Sie auf der Registerkarte Details für das Dokument `RunCommand_Shell` oder `RunComman`

		d_PowerShell Automation in der Systems Manager Manager-Konsole.
3	SendTaskFailure	Wird ausgeführt, wenn Schritt 2 abgebrochen oder abgebrochen wird. Es ruft die Step Functions send_task_failure API auf, die drei Parameter als Eingabe akzeptiert: das von der Zustandsmaschine übergebene Token, den Fehlerfehler und eine Beschreibung der Fehlerursache.
4	SendTaskSuccess	Wird ausgeführt, wenn Schritt 2 erfolgreich ist. Es ruft die Step Functions send_task_success API auf, die das von der Zustandsmaschine übergebene Token als Eingabe akzeptiert.

Runbook-Parameter

SfnRunCommandByInstanceIdsRunbook:

Parametername	Typ	Optional oder erforderlich	Beschreibung
shell	String	Erforderlich	Die Instanz-Shell, um zu entscheiden, ob sie AWS-RunShellScript für Linux oder AWS-RunPowerShellS

			`cript` für Windows ausgeführt werden sollen.
`deliveryTimeout`	Ganzzahl	Optional	Die Wartezeit in Sekunden, bis ein Befehl an den SSM-Agenten auf einer Instance übermitte lt wird. Dieser Parameter hat einen Mindestwert von 30 (0,5 Minuten) und einen Höchstwert von 2592000 (720 Stunden).
`execution Timeout`	String	Optional	Die Zeit in Sekunden, die ein Befehl bis zum Abschluss benötigt, bevor er als fehlgesch lagen betrachtet wird. Der Standardwert ist 3600 (1 Stunde). Der Höchstwert ist 172800 (48 Stunden).
`workingDi rectory`	String	Optional	Der Pfad zum Arbeitsverzeichnis auf der Instance.
`Commands`	StringList	Erforderlich	Das auszuführende Shell-Skript oder der auszuführende Befehl.

`InstanceIds`	StringList	Erforderlich	Die IDs der Instanzen, auf denen Sie den Befehl ausführen möchten.
`taskToken`	String	Erforderlich	Das Task-Token, das für Rückrufantworten verwendet werden soll.

`SfnRunCommandByTargets`Runbook:

Name	Typ	Optional oder erforderlich	Beschreibung
`shell`	String	Erforderlich	Die Instanz-Shell, um zu entscheiden, ob sie `AWS-RunShellScript` für Linux oder `AWS-RunPowerShellScript` für Windows ausgeführt werden sollen.
`deliveryTimeout`	Ganzzahl	Optional	Die Wartezeit in Sekunden, bis ein Befehl an den SSM-Agenten auf einer Instance übermittelt wird. Dieser Parameter hat einen Mindestwert von 30 (0,5 Minuten) und einen Höchstwert

			von 2592000 (720 Stunden).
`executionTimeout`	Ganzzahl	Optional	Die Zeit in Sekunden, die ein Befehl bis zum Abschluss benötigt, bevor er als fehlgesch lagen betrachtet wird. Der Standardwert ist 3600 (1 Stunde). Der Höchstwert ist 172800 (48 Stunden).
`workingDirectory`	String	Optional	Der Pfad zum Arbeitsverzeichnis auf der Instance.
`Commands`	StringList	Erforderlich	Das auszuführende Shell-Skript oder der auszuführende Befehl.
`Targets`	MapList	Erforderlich	Eine Reihe von Suchkriterien, die Instanzen anhand von Schlüssel-Wert-Paaren identifizieren, die Sie angeben. Beispiel: `[{"Key":"InstanceIds","Values":["i-02573cafcfEXAMPLE","i-0471e04240EXAMPLE"]}]`

`taskToken`	String	Erforderlich	Das Task-Token, das für Rückrufantworten verwendet werden soll.

Beispielausgabe

Die folgende Tabelle enthält ein Beispiel für die Ausgabe der Step-Funktion. Sie zeigt, dass die Gesamtlaufzeit zwischen Schritt 5 (`TaskSubmitted`) und Schritt 6 (`TaskSucceeded`) über 100 Sekunden beträgt. Dies zeigt, dass die Step-Funktion auf die Beendigung des `sleep 100` Befehls gewartet hat, bevor sie zur nächsten Aufgabe im Workflow überging.

ID (ID)	Typ	Schritt	Ressource	Verstrichene Zeit (ms)	Zeitstempel
1	`ExecutionStarted`		-	0	11. März 2022 14:50:34.303 Uhr
2	`TaskStateEntered`	`StartAutomationWaitForCallBack`	-	40	11. März 2022 14:50:34,343 Uhr
3	`TaskScheduled`	`StartAutomationWaitForCallBack`	-	40	11. März 2022 14:50:34,343 Uhr
4	`TaskStarted`	`StartAutomationWaitForCallBack`	-	154	11. März 2022 14:50:34.457 Uhr
5	`TaskSubmitted`	`StartAutomationWai`	-	657	11. März 2022

		tForCallBack			14:50:34.960 Uhr
6	TaskSucceeded	StartAutomationWaitForCallBack	-	10:3835	11. März 2022 14:52:18.138 Uhr
7	TaskStateExited	StartAutomationWaitForCallBack	-	1038 60	11. März 2022 14:52:18.163 Uhr
8	ExecutionSucceeded		-	103 897	11. März 2022 14:52:18.200 Uhr

Ausführen paralleler Lesevorgänge von S3-Objekten mithilfe von Python in einer AWS Lambda-Funktion

Erstellt von Eduardo Bortoluzzi

Code-Repository: aws-lambda-parallel-download	Umgebung: PoC oder Pilotprojekt	Technologien: Serverless
AWS-Services: AWS Lambda ;Amazon S3; AWS Step Functions		

Übersicht

Sie können dieses Muster verwenden, um eine Liste von Dokumenten aus Amazon Simple Storage Service (Amazon S3)-Buckets in Echtzeit abzurufen und zusammenzufassen. Das Muster bietet Beispielcode zum parallelen Lesen von Objekten aus S3-Buckets auf Amazon Web Services (AWS). Das Muster zeigt, wie I/O-gebundene Aufgaben mit AWS Lambda-Funktionen mithilfe von Python effizient ausgeführt werden.

Ein Finanzunternehmen hat dieses Muster in einer interaktiven Lösung verwendet, um korrelierte Finanztransaktionen in Echtzeit manuell zu genehmigen oder abzulehnen. Die Dokumente zu Finanztransaktionen wurden in einem S3-Bucket gespeichert, der sich auf den Markt bezieht. Ein Operator hat eine Liste von Dokumenten aus dem S3-Bucket ausgewählt, den Gesamtwert der von der Lösung berechneten Transaktionen analysiert und sich entschieden, den ausgewählten Batch zu genehmigen oder abzulehnen.

E/A-gebundene Aufgaben unterstützen mehrere Threads. In diesem Beispielcode wird die Datei concurrent. futures.ThreadPoolExecutor mit maximal 1 000 gleichzeitigen Threads verwendet. Lambda-Funktionen unterstützen bis zu 1 024 Threads, und einer dieser Threads ist Ihr Hauptprozess. Sie müssen auch die maximalen Poolverbindungen in erhöhen, `botocore` damit alle Threads den S3-Objekt-Download gleichzeitig durchführen können.

Der Beispielcode verwendet ein 8,3-KB-Objekt mit JSON-Daten in einem S3-Bucket. Das Objekt wird mehrmals gelesen. Nachdem die Lambda-Funktion das Objekt gelesen hat, werden die JSON-

Daten in ein Python-Objekt dekodiert. Das Ergebnis nach der Ausführung dieses Beispiels waren 1 000 Lesevorgänge, die in 2,3 Sekunden verarbeitet wurden, und 10 000 Lesevorgänge, die in 26 Sekunden mit einer Lambda-Funktion verarbeitet wurden, die mit 2 048 MB Speicher konfiguriert ist. Das Erhöhen des Lambda-Speichers war nicht hilfreich, um die Zeit für die Ausführung der Aufgabe zu verkürzen.

Das AWS Lambda Power Tuning-Tool wurde verwendet, um verschiedene Lambda-Speicherkonfigurationen zu testen und das beste performance-to-cost Verhältnis für die Aufgabe zu überprüfen. Die Testergebnisse finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Besorgnis bei der Python-Entwicklung

Einschränkungen

- Eine Lambda-Funktion kann maximal 1 024 Ausführungsprozesse oder Threads haben.
- Neue AWS-Konten haben ein Lambda-Speicherlimit von 3 008 MB. Passen Sie das AWS Lambda Power Tuning-Tool entsprechend an. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung.
- Python Version 3.8 ist die empfohlene Mindestversion, da sie die Thread-Wiederverwendung aus dem Thread-Ausführungspool eingeführt hat.
- Amazon S3 hat ein Limit von 5 500 GET/HEAD-Anforderungen pro Sekunde pro partitioniertem Präfix .

Produktversionen

- Python 3.8 oder höher
- AWS Cloud Development Kit (AWS CDK) v2
- Version 2 AWS Command Line Interface (AWS CLI)
- AWS Lambda Power Tuning 4.3.3 (optional)

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon S3
- AWS Step Functions (wenn AWS Lambda Power Tuning bereitgestellt wird)

Zielarchitektur

Das folgende Diagramm zeigt eine Lambda-Funktion, die Objekte parallel aus einem S3-Bucket liest. Das Diagramm enthält auch einen Step Functions-Workflow für das AWS Lambda Power Tuning-Tool zur Feinabstimmung des Lambda-Funktionsspeichers. Diese Feinabstimmung trägt dazu bei, ein gutes Gleichgewicht zwischen Kosten und Leistung zu erreichen.

Automatisierung und Skalierung

Die Lambda-Funktionen skalieren bei Bedarf schnell. Um 503 Slow Down-Fehler von Amazon S3 bei hoher Nachfrage zu vermeiden, empfehlen wir, einige Beschränkungen für die Skalierung festzulegen.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) v2 ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS Cloud-Infrastruktur im Code unterstützt. Die Beispielinfrastruktur wurde für die Bereitstellung mit AWS CDK erstellt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können. In diesem Muster wird AWS CLI Version 2 verwendet, um eine JSON-Beispieldatei hochzuladen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- AWS Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie AWS Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Andere Tools

- Python ist eine universelle Computer-Programmiersprache. Die Wiederverwendung von inaktiven Worker-Threads wurde in Python Version 3.8 eingeführt und der Lambda-Funktionscode in diesem Muster wurde für diese Version erstellt.

Code-Repository

Der Code für dieses Muster ist im aws-lambda-parallel-download GitHub Repository verfügbar.

Bewährte Methoden

- Dieses AWS-CDK-Konstrukt benötigt die Benutzerberechtigungen Ihres AWS-Kontos, um die Infrastruktur bereitzustellen. Wenn Sie AWS-CDK-Pipelines oder kontoübergreifende Bereitstellungen verwenden möchten, finden Sie weitere Informationen unter Stack-Synthesizer.
- In dieser Beispielanwendung sind die Zugriffsprotokolle im S3-Bucket nicht aktiviert. Es hat sich bewährt, Zugriffsprotokolle im Produktionscode zu aktivieren.

Sekunden

Vorbereiten der Entwicklungsumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die installierte Python-Version.	Der bereitgestellte Code wurde unter Python 3.8 und höher erstellt und getestet. Um Ihre installierte Python-Version zu überprüfen, führen Sie aus`python3 -V`. Laden Sie bei Bedarf eine neuere Version herunter und installieren Sie sie.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um zu überprüfen, ob die erforderlichen Module installiert sind, führen Sie aus`python3 -c "import pip, venv"`. Wenn die Module installiert sind, wird kein Fehler zurückgegeben.	
Installieren und konfigurieren Sie AWS CDK.	Um das AWS-CDK zu installieren und es zu booten, falls es noch nicht konfiguriert ist, folgen Sie den Anweisungen unter Erste Schritte mit dem AWS-CDK. Um zu bestätigen, dass die installierte AWS-CDK-Version 2.0 oder höher ist, führen Sie aus`cdk --version`: Übergeben Sie beim Bootstrapping den `--cloudformation-execution-policies "arn:aws:iam::aws:policy/job-function/ViewOnlyAccess"` Parameter an `cdk bootstrap` . In diesem Beispiel wird nicht die definierte Rolle verwendet, um den Stack bereitzustellen, und dieser Parameter macht Ihre Bereitstellung sicherer.	Cloud-Architekt

Klonen des Beispiel-Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um die neueste Version des Repositorys zu klonen: `git clone --depth 1 --branch v1.1.2 \ git@github.com:aws-samples/aws-lambda-parallel-download.git`	Cloud-Architekt
Ändern Sie das Arbeitsverzeichnis in das geklonte Repository.	Führen Sie den folgenden Befehl aus: `cd aws-lambda-parallel-download`	Cloud-Architekt
Erstellen Sie die virtuelle Python-Umgebung.	Führen Sie den folgenden Befehl aus, um eine virtuelle Python-Umgebung zu erstellen: `python3 -m venv .venv`	Cloud-Architekt
Aktivieren Sie die virtuelle Umgebung.	Führen Sie den folgenden Befehl aus, um die virtuelle Umgebung zu aktivieren: `source .venv/bin/activate`	Cloud-Architekt
Installieren Sie die Abhängigkeiten.	Um die Python-Abhängigkeiten zu installieren, führen Sie den `pip` Befehl aus:	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pip install -r requirements.txt`	
Durchsuchen Sie den Code.	(Optional) Der Beispielcode, der ein Objekt aus dem S3-Bucket herunterlädt, befindet sich unter `resources/parallel.py` . Der Infrastrukturcode befindet sich im `parallel_download` Ordner .	Cloud-Architekt

Bereitstellen und Testen der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung bereit.	Führen Sie `cdk deploy`. Schreiben Sie die AWS-CDK-Ausgaben auf: • `ParallelDownloadStack.LambdaFunctionARN` • `ParallelDownloadStack.SampleS3BucketName` • `ParallelDownloadStack.StateMachineARN`	Cloud-Architekt
Laden Sie eine JSON-Beispieldatei hoch.	Das Repository enthält eine JSON-Beispieldatei von etwa 9 KB. Führen Sie den	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgenden Befehl aus, um die Datei in den S3-Bucket des erstellten Stacks hochzuladen: `aws s3 cp sample.json s3://<ParallelDownloadStack.SampleS3BucketName>` Ersetzen Sie durch `<ParallelDownloadStack.SampleS3BucketName>` den entsprechenden Wert aus der AWS-CDK-Ausgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die App aus.	1. Melden Sie sich bei der AWS-Managementkonsole an, navigieren Sie zur Lambda-Konsole und suchen Sie die Lambda-Funktion, die den ARN aus der AWS-CDK-Ausgabe enthält `ParallelDownloadStack.LambdaFunctionARN` . 2. Ändern Sie auf der Registerkarte Test den Ereignis-JSON-Code wie folgt: `{"objectKey": "sample.json"}` 3. Wählen Sie Test aus. 4. Um das Ergebnis anzuzeigen, wählen Sie Details aus. Die Details zeigen die Statistiken des parallelen Downloads, die Informationen der Ausführung und die Protokolle.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Anzahl der Downloads hinzu.	(Optional) Um 1 500 Get Object-Aufrufe auszuführen, verwenden Sie den folgenden JSON-Code in Event JSON des `Test` Parameters : `{"repeat": 1500, "objectKey": "sample.json"}`	Cloud-Architekt

Optional: Ausführen von AWS Lambda Power Tuning

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Tool AWS Lambda Power Tuning aus.	1. Melden Sie sich bei der -Konsole an und navigieren Sie zu Step Functions . 2. Suchen Sie den Zustandsautomaten mit dem ARN aus der AWS-CDK-Ausgabe `ParallelDownloadStack.StateMachineARN` . 3. Wählen Sie Ausführung starten und fügen Sie das folgende JSON ein: `{ "lambdaARN": "<ParallelDownloadStack.LambdaFunctionARN>", "num": 5, "payload": {"repeat": 2000,`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"objectKey":
	"sample.json"}
	}</pre>
	Denken Sie daran, `<ParallelDownloadStack.LambdaFunctionARN>` durch den Wert aus der CDK-Ausgabe zu ersetzen.
	
	Am Ende der Ausführung befindet sich das Ergebnis auf der Registerkarte Eingabe und Ausgabe der Ausführung.	

Sehen Sie sich die Ergebnisse der AWS Lambda Power Tuning in einem Diagramm an.	Kopieren Sie auf der Registerkarte Ein- und Ausgabe der Ausführung den `visualization` Eigenschaftslink und fügen Sie ihn in eine neue Browser-Registerkarte ein.	Cloud-Architekt

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Objekte aus dem S3-Bucket.	Bevor Sie die bereitgestellten Ressourcen löschen, entfernen Sie alle Objekte aus dem S3-Bucket: <pre>aws s3 rm s3://<ParallelDownloadStack</pre>	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`.SampleS3BucketName> \ --recursive` Denken Sie daran, `<ParallelDownloadStack.SampleS3BucketName>` durch den Wert aus den AWS-CDK-Ausgaben zu ersetzen.	
Zerstören Sie die Ressourcen.	Führen Sie den folgenden Befehl aus, um alle Ressourcen zu löschen, die für dieses Pilotprojekt erstellt wurden: `cdk destroy`	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
`'MemorySize' value failed to satisfy constraint: Member must have value less than or equal to 3008`	Bei neuen Konten können Sie möglicherweise nicht mehr als 3 008 MB in Ihren Lambda-Funktionen konfigurieren. Um mit AWS Lambda Power Tuning zu testen, fügen Sie die folgende Eigenschaft am Eingabe-JSON hinzu, wenn Sie die Step Functions-Ausführung starten: `"powerValues": [ 512, 1024, 1536, 2048, 2560,`

Problem	Lösung

	<pre>3008
	]</pre>

Zugehörige Ressourcen

- Python – gleichzeitig.Zugänge.ThreadPoolExecutor
- Lambda-Kontingente – Funktionskonfiguration, Bereitstellung und Ausführung
- Arbeiten mit dem AWS-CDK in Python
- Profiling-Funktionen mit AWS Lambda Power Tuning

Zusätzliche Informationen

Code

Der folgende Codeausschnitt führt die parallele E/A-Verarbeitung durch:

```
with ThreadPoolExecutor(max_workers=MAX_WORKERS) as executor:
  for result in executor.map(a_function, (the_arguments)):
    ...
```

Die verwendet die Threads `ThreadPoolExecutor` wieder, sobald sie verfügbar sind.

Tests und Ergebnisse

Beim ersten Test wurden 2 500 Objektlesevorgänge verarbeitet, mit dem folgenden Ergebnis.

Ab 3 009 MB bleibt die Verarbeitungszeit für jede Speichererhöhung gleich, aber die Kosten stiegen mit zunehmender Speichergröße.

Ein weiterer Test untersuchte den Bereich zwischen 1 536 MB und 3 072 MB Arbeitsspeicher. Dabei wurden Werte verwendet, die Vielfaches von 256 MB waren und 10 000 Objektlesevorgänge verarbeiten, mit den folgenden Ergebnissen.

Das beste performance-to-cost Verhältnis war mit der Lambda-Konfiguration mit 2.048 MB Speicher.

Zum Vergleich dauerte ein sequenzieller Prozess von 2 500 Objektlesevorgängen 40 Sekunden. Der parallele Prozess mit der Lambda-Konfiguration von 2 048 MB dauerte 5,8 Sekunden, was 85 Prozent weniger entspricht.

Richten Sie den privaten Zugriff auf einen Amazon S3 S3-Bucket über einen VPC-Endpunkt ein

Erstellt von Martin Maritsch (AWS), Gabriel Rodriguez Garcia (AWS), Shukhrat Khodjaev (AWS), Nicolas Jacob Baer (AWS), Mohan Gowda Purushothama (AWS) und Joaquin Rinaudo (AWS)

Code-Repository: Private S3 VPCE	Umgebung: Produktion	Technologien: Serverlos
AWS-Services: Amazon API Gateway; Amazon S3; Amazon VPC; Elastic Load Balancing (ELB)		

Übersicht

In Amazon Simple Storage Service (Amazon S3) ermöglichen Ihnen vorsignierte URLs, Dateien beliebiger Größe für Zielbenutzer freizugeben. Standardmäßig sind vorsignierte Amazon S3 S3-URLs innerhalb eines Ablaufzeitfensters vom Internet aus zugänglich, sodass sie bequem zu verwenden sind. In Unternehmensumgebungen muss der Zugriff auf vorsignierte Amazon S3 S3-URLs jedoch häufig nur auf ein privates Netzwerk beschränkt sein.

Dieses Muster stellt eine serverlose Lösung für die sichere Interaktion mit S3-Objekten dar, indem vorsignierte URLs aus einem privaten Netzwerk ohne Internetdurchquerung verwendet werden. In der Architektur greifen Benutzer über einen internen Domainnamen auf einen Application Load Balancer zu. Der Datenverkehr wird intern über Amazon API Gateway und einen Virtual Private Cloud (VPC) -Endpunkt für den S3-Bucket geleitet. Die AWS Lambda Funktion generiert vorsignierte URLs für Dateidownloads über den privaten VPC-Endpunkt, wodurch die Sicherheit und der Datenschutz für sensible Daten verbessert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine VPC, die ein Subnetz umfasst AWS-Konto , das in einem mit dem Unternehmensnetzwerk verbunden ist (z. B. über AWS Direct Connect).

Einschränkungen

- Der S3-Bucket muss denselben Namen wie die Domain haben. Wir empfehlen daher, die Amazon S3 S3-Bucket-Namensregeln zu überprüfen.
- Diese Beispielarchitektur beinhaltet keine Überwachungsfunktionen für die bereitgestellte Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von AWS Überwachungsdiensten in Betracht ziehen.
- Diese Beispielarchitektur beinhaltet keine Eingabevalidierung. Wenn Ihr Anwendungsfall eine Eingabevalidierung und ein erhöhtes Sicherheitsniveau erfordert, sollten Sie dies AWS WAF zum Schutz Ihrer API in Betracht ziehen.
- Diese Beispielarchitektur beinhaltet keine Zugriffsprotokollierung mit dem Application Load Balancer. Wenn Ihr Anwendungsfall eine Zugriffsprotokollierung erfordert, sollten Sie die Aktivierung der Load Balancer-Zugriffsprotokolle in Betracht ziehen.

Versionen

- Python-Version 3.11 oder höher
- Terraform Version 1.6 oder höher

Architektur

Zieltechnologie-Stack

Die folgenden AWS-Services werden im Zieltechnologie-Stack verwendet:

- Amazon S3 ist der zentrale Speicherservice, der für das sichere Hochladen, Herunterladen und Speichern von Dateien verwendet wird.
- Amazon API Gateway stellt Ressourcen und Endpunkte für die Interaktion mit dem S3-Bucket zur Verfügung. Dieser Service spielt eine Rolle bei der Generierung vorsignierter URLs für das Herunterladen oder Hochladen von Daten.
- AWS Lambdageneriert vorsignierte URLs für das Herunterladen von Dateien von Amazon S3. Die Lambda-Funktion wird von API Gateway aufgerufen.
- Amazon VPC stellt Ressourcen innerhalb einer VPC bereit, um das Netzwerk zu isolieren. Die VPC umfasst Subnetze und Routingtabellen zur Steuerung des Datenverkehrs.

- Der Application Load Balancer leitet eingehenden Datenverkehr entweder an API Gateway oder an den VPC-Endpunkt des S3-Buckets weiter. Es ermöglicht Benutzern aus dem Unternehmensnetzwerk den internen Zugriff auf Ressourcen.
- Der VPC-Endpunkt für Amazon S3 ermöglicht die direkte, private Kommunikation zwischen Ressourcen in der VPC und Amazon S3, ohne das öffentliche Internet zu durchqueren.
- AWS Identity and Access Management (IAM) steuert den Zugriff auf Ressourcen. AWS Berechtigungen werden eingerichtet, um sichere Interaktionen mit der API und anderen Diensten zu gewährleisten.

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Benutzer aus dem Unternehmensnetzwerk können über einen internen Domainnamen auf den Application Load Balancer zugreifen. Wir gehen davon aus, dass eine Verbindung zwischen dem Unternehmensnetzwerk und dem Intranet-Subnetz im besteht AWS-Konto (z. B. über eine AWS Direct Connect Verbindung).
2. Der Application Load Balancer leitet eingehenden Datenverkehr entweder an API Gateway weiter, um vorsignierte URLs zum Herunterladen oder Hochladen von Daten auf Amazon S3 zu generieren, oder an den VPC-Endpunkt des S3-Buckets. In beiden Szenarien werden Anfragen intern weitergeleitet und müssen nicht über das Internet geleitet werden.
3. API Gateway stellt Ressourcen und Endpunkte für die Interaktion mit dem S3-Bucket zur Verfügung. In diesem Beispiel stellen wir einen Endpunkt zum Herunterladen von Dateien aus dem S3-Bucket bereit. Dieser könnte jedoch erweitert werden, um auch Upload-Funktionen bereitzustellen.
4. Die Lambda-Funktion generiert die vorsignierte URL zum Herunterladen einer Datei von Amazon S3, indem sie den Domainnamen des Application Load Balancer anstelle der öffentlichen Amazon S3 S3-Domain verwendet.
5. Der Benutzer erhält die vorsignierte URL und verwendet sie, um die Datei mithilfe des Application Load Balancer von Amazon S3 herunterzuladen. Der Load Balancer enthält eine Standardroute, um Traffic, der nicht für die API bestimmt ist, an den VPC-Endpunkt des S3-Buckets zu senden.
6. Der VPC-Endpunkt leitet die vorsignierte URL mit dem benutzerdefinierten Domainnamen an den S3-Bucket weiter. Der S3-Bucket muss denselben Namen wie die Domain haben.

Automatisierung und Skalierung

Dieses Muster verwendet Terraform, um die Infrastruktur aus dem Code-Repository in einem bereitzustellen. AWS-Konto

Tools

Tools

- Python ist eine Allzweck-Computerprogrammiersprache.
- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer AWS Befehlszeilen-Shell mit Diensten interagieren können.

Code-Repository

Der Code für dieses Muster ist in einem GitHub Repository unter https://github.com/aws-samples/private-s3-vpce verfügbar.

Bewährte Methoden

Die Beispielarchitektur für dieses Muster verwendet IAM-Berechtigungen, um den Zugriff auf die API zu steuern. Jeder, der über gültige IAM-Anmeldeinformationen verfügt, kann die API aufrufen. Wenn Ihr Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, möchten Sie möglicherweise einen anderen Zugriffskontrollmechanismus verwenden.

Epen

Stellen Sie die Lösung in einem bereit AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich AWS Anmeldeinformationen.	Überprüfen Sie Ihre AWS Anmeldeinformationen und Ihren Zugang zu Ihrem Konto. Anweisungen finden Sie in der AWS CLI Dokumentation unter	AWS DevOps, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konfiguration und Einstellungen für die Anmeldeinformationsdatei.	
Klonen Sie das Repository	Klonen Sie das mit diesem Muster bereitgestellte GitHub Repository: `git clone https://github.com/aws-samples/private-s3-vpce`	AWS DevOps, Allgemeines AWS
Variablen konfigurieren.	1. Öffnen Sie auf Ihrem Computer im GitHub Repository den `terraform` Ordner: `cd terraform` 2. Öffnen Sie die `example.tfvars` Datei und passen Sie die Parameter an Ihre Bedürfnisse an.	AWS DevOps, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lösung bereitstellen.	1. Führen Sie im `terraform` Ordner Terraform aus und übergeben Sie die Variablen, die Sie angepasst haben: `terraform apply -var-file="example.tfvars"` 2. Vergewissern Sie sich, dass die im Architekturdiagramm angezeigten Ressourcen erfolgreich bereitgestellt wurden.	AWS DevOps, Allgemeines AWS

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Testdatei.	Laden Sie eine Datei auf Amazon S3 hoch, um ein Testszenario für den Dateidownload zu erstellen. Sie können die Amazon S3 S3-Konsole oder den folgenden AWS CLI Befehl verwenden: `aws s3 cp /path/to/testfile s3://your-bucket-name/testfile`	AWS DevOps, Allgemeines AWS
Testen Sie die Funktionalität vordefinierter URLs.	1. Senden Sie mithilfe von awscurl eine Anfrage an	AWS DevOps, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Application Load Balancer, um eine vorsignierte URL für die Testdatei zu erstellen: `awscurl https://your-domain-name/api/get_url?key=testfile` In diesem Schritt wird aus Ihren Anmeldeinformationen eine gültige Signatur erstellt, die von API Gateway validiert wird. 2. Analysieren Sie den Link aus der Antwort, die Sie im vorherigen Schritt erhalten haben, und öffnen Sie die vorsignierte URL, um die Datei herunterzuladen.	
Bereinigen Sie.	Stellen Sie sicher, dass Sie die Ressourcen entfernen, wenn sie nicht mehr benötigt werden: `terraform destroy`	AWS DevOps, Allgemeines AWS

Fehlerbehebung

Problem	Lösung
S3-Objektschlüsselnamen mit Sonderzeichen wie Nummernzeichen (#) unterbrechen URL-Parameter und führen zu Fehlern.	Codieren Sie die URL-Parameter ordnungsgemäß und stellen Sie sicher, dass der Name des S3-Objektschlüssels den Amazon S3 S3-Richtlinien entspricht.

Zugehörige Ressourcen

Amazon S3:

- Objekte mit vorsignierten URLs teilen
- Steuern des Zugriffs von VPC-Endpunkten aus mit Bucket-Richtlinien

Amazon API Gateway:

- Verwenden Sie VPC-Endpunktrichtlinien für private APIs in API Gateway

Application Load Balancer:

- Hosten interner statischer HTTPS-Websites mit ALB, S3 und PrivateLink (AWS Blogbeitrag)

Verketten von AWS-Services mithilfe eines Serverless-Ansatzes

Erstellt von Aniket Brasilien (AWS)

Umgebung: Produktion	Technologien: Serverless; Cloudnativ; Softwareentwicklung und -tests DevOps; Modernisierung; Infrastruktur	AWS-Services: Amazon S3; Amazon SNS ;Amazon SQS ;AWS Lambda

Übersicht

Dieses Muster zeigt einen skalierbaren Serverless-Ansatz für die Verarbeitung einer hochgeladenen Datei durch Verkettung von Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) und AWS Lambda . Das Beispiel für die hochgeladene Datei dient zu Demonstrationszwecken. Sie können einen Serverless-Ansatz verwenden, um andere Aufgaben zu erledigen, indem Sie die Kombination der AWS-Services miteinander verketten, die zur Erfüllung Ihrer Geschäftsziele erforderlich sind. Der Serverless-Ansatz verwendet einen asynchronen Workflow, der auf ereignisgesteuerten Benachrichtigungen, belastbarem Speicher und FaaS-Computing (Function as a Service) basiert, um Anfragen zu verarbeiten. Sie können den Serverless-Ansatz verwenden, um zu skalieren, um die Nachfrage zu decken und gleichzeitig die Kosten zu minimieren.

Hinweis: Es gibt mehrere Möglichkeiten, AWS-Services über einen Serverless-Ansatz miteinander zu verketten. Sie können beispielsweise einen Ansatz verwenden, der Lambda mit Amazon S3 anstelle von Amazon SNS und Amazon SQS kombiniert. Dieses Muster verwendet jedoch Amazon SNS und Amazon SQS, da dieser Ansatz es ermöglicht, während einer Ereignisbenachrichtigung mehrere Integrationspunkte zum Lambda-Aufrufprozess hinzuzufügen und die Implementierung zu erweitern, um mehrere Listener in eine Serverless-Orchestrierung aufzunehmen und gleichzeitig den Verarbeitungsaufwand zu minimieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Programmgesteuerter Zugriff auf das AWS-Konto. Weitere Informationen finden Sie hier:

  - Voraussetzungen in der AWS Cloud Development Kit (AWS CDK)-Dokumentation
  - Voraussetzungen in der AWS Command Line Interface (AWS CLI)-Dokumentation
- AWS-CDK, installiert
- AWS CLI, installiert und konfiguriert
- Python 3.9

Produktversionen

- AWS-CDK 2.x
- Python 3.9

Architektur

Das folgende Diagramm zeigt, wie verkettete AWS-Services es einem Benutzer ermöglichen können, eine Datei zur Verarbeitung in einen S3-Bucket hochzuladen:

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer lädt eine Datei in den S3-Bucket hoch.
2. Der Upload initiiert ein S3-Ereignis, das eine Nachricht in einem SNS-Thema veröffentlicht. Die Nachricht enthält die Details des S3-Ereignisses.
3. Die im SNS-Thema veröffentlichte Nachricht wird in eine SQS-Warteschlange eingefügt, die abonniert ist und Benachrichtigungen für dieses Thema erhält.
4. Eine Lambda-Funktion fragt die SQS-Warteschlange (als Ereignisquelle) ab und wartet, bis Nachrichten verarbeitet werden.
5. Wenn die Lambda-Funktion Nachrichten von der SQS-Warteschlange empfängt, verarbeitet sie sie und bestätigt den Empfang dieser Nachrichten.
6. Wenn eine Nachricht nicht von Lambda verarbeitet wird, wird diese Nachricht an die SQS-Warteschlange zurückgegeben und schließlich an eine SQS-Warteschlange für unzustellbare Nachrichten weitergeleitet.

Technologie-Stack

- Amazon S3
- Amazon SNS
- Amazon SQS
- AWS Lambda

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Notification Service (Amazon SNS) hilft Ihnen, den Nachrichtenaustausch zwischen Publishern und Clients, einschließlich Webservern und E-Mail-Adressen, zu koordinieren und zu verwalten.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die genutzte Rechenzeit bezahlen.

Andere Tools

- AWS Cloud Development Kit (AWS CDK) ist das primäre Tool für die Interaktion mit Ihrer AWS CDK-App. Es führt Ihre App aus, fragt das von Ihnen definierte Anwendungsmodell ab und erstellt und stellt die vom AWS-CDK generierten AWS- CloudFormation Vorlagen bereit.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Python ist eine allgemeine, interpretierte Allzweck-Programmiersprache.

Code

Der Code für dieses Muster ist im Repository GitHub Verketten von S3 zu SNS zu SQS zu Lambda verfügbar.

Polen

Entwickeln Ihrer Serverless-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository und navigieren Sie zum `python/s3-sns-sqs-lambda-chain` Ordner .	App-Developer
Richten Sie eine virtuelle Umgebung ein.	1. Führen Sie im AWS-CDK den `python3 -m venv .venv` Befehl aus. 2. Führen Sie den `source .venv/bin/activate` Befehl unter MacOS /Linux oder unter Windows `.venv\Scripts\activate.bat` aus.	App-Developer
Installieren Sie die Abhängigkeiten.	Führen Sie den Befehl `pip install -r requirements.txt` aus.	App-Developer

Testen des CloudFormation Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Einheitentests durch.	1. Führen Sie den Befehl `pip install -r requirements-dev.txt` aus. 2. (Optional) Führen Sie den `cdk synth --no-staging > template.`	App-Entwickler, Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`yml` Befehl aus, um den CloudFormation Stack zu generieren. Wichtig: Sie können den Stack überprüfen, aber vermeiden , die bereitgestellten Ressourcen und Artefakte zu generieren. 3. Führen Sie den `pytest` Befehl aus, um alle Komponententests auszuführen. 4. (Optional) Führen Sie den `pytest tests/unit/<test_filename>` Befehl aus, um Tests für eine bestimmte Datei auszuführen.	

Bereitstellen des CloudFormation Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Bootstrap-Umgebung ein.	Folgen Sie den Anweisungen unter Bootstrapping in der AWS-Dokumentation, um die Umgebung für die AWS-CDK-Bereitstellung in jeder AWS-Region zu booten, in der der CloudFormation Stack bereitgestellt wird. Hinweis: Dieser Schritt erfordert, dass Sie über	App-Entwickler, DevOps Techniker, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anmeldeinformationen mit programmatischem Zugriff verfügen.	
Stellen Sie den CloudFormation Stack bereit.	Führen Sie den `cdk deploy` Befehl aus, um den Stack zu erstellen und für das AWS-Konto bereitzustellen.	App-Entwickler, DevOps Techniker, AWS DevOps

Bereinigen der Ressourcen Ihrer Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den CloudFormation Stack und entfernen Sie die zugehörigen Ressourcen.	Um den erstellten CloudFormation Stack zu löschen und alle zugehörigen Ressourcen zu entfernen, führen Sie den Befehl `run cdk` „Detroy“ aus.	App-Developer

Mehr Muster

- Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden
- Aggregieren von Daten in Amazon DynamoDB für ML-Prognosen in Athena
- Automatisieren der AWS-Ressourcenbewertung
- Automatisieren der Bereitstellung verschachtelter Anwendungen mit AWS SAM
- Automatisieren der Replikation von Amazon RDS-Instances über AWS-Konten hinweg
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatisches Erkennen von Änderungen und Initiieren verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit
- Erstellen Sie mithilfe von DevOps Praktiken und AWS Cloud9 eine lose gekoppelte Architektur mit Microservices
- Erstellen einer Serverless-Architektur mit mehreren Mandanten in Amazon OpenSearch Service
- Erstellen eines erweiterten Mainframe-Datei-Viewers in der AWS Cloud
- Berechnen des Risikowerts (VaR) mithilfe von AWS-Services
- AWS Service Catalog-Produkte über verschiedene AWS-Konten und AWS-Regionen hinweg kopieren
- Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte
- Zerlegen von Monolithen in Microservices mithilfe von CQRS und Event Sourcing
- Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Bereitstellen und Debuggen von Amazon-EKS-Clustern
- Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden
- Bereitstellen von Lambda-Funktionen mit Container-Images
- Entwickeln Sie mithilfe von Amazon Bedrock-Agenten und Wissensdatenbanken einen vollautomatischen Chat-basierten Assistenten
- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct
- Generieren Sie dynamisch eine IAM-Richtlinie mit IAM Access Analyzer mithilfe von Step Functions
- Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist

- Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität
- Generieren Sie personalisierte und neu eingestufte Empfehlungen mit Amazon Personalize
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Implementieren Sie das Serverless-Saga-Muster mithilfe von AWS Step Functions
- Verbessern Sie die betriebliche Leistung, indem Sie Amazon DevOps Guru über mehrere AWS-Regionen, Konten und OUs hinweg mit dem AWS-CDK aktivieren
- Starten eines CodeBuild Projekts über AWS-Konten hinweg mithilfe von Step Functions und einer Lambda-Proxy-Funktion
- Migrieren von Apache Cassandra-Workloads zu Amazon Keyspaces mithilfe von AWS Glue
- Überwachen der Verwendung eines freigegebenen Amazon Machine Image über mehrere AWS-Konten hinweg
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Strukturieren eines Python-Projekts in hexaffinaler Architektur mit AWS Lambda
- Deaktivieren von Sicherheitsstandardkontrollen für alle Security Hub-Mitgliedskonten in einer Umgebung mit mehreren Konten

Softwareentwicklung und Testen

Themen

Automatisches Generieren eines PynamoDB-Modells und von CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung

Erstellt von Vijit Vashishtha (AWS), Dheeraj Alimchandani (AWS) und Dhananjay Karanjkar (AWS)

Code-Repository: amazon-reverse-engineer-dynamodb	Umgebung: PoC oder Pilotprojekt	Technologien: Softwareentwicklung und -tests; Datenbanken; DevOps
Workload: Open-Source	AWS-Services: Amazon DynamoDB	

Übersicht

Es ist üblich, Entitäten und CRUD-Operationsfunktionen (Create, Read, Update, Delete) zu verlangen, um Amazon-DynamoDB-Datenbankoperationen effizient auszuführen. PynamoDB ist eine Python-basierte Schnittstelle, die Python 3 unterstützt. Sie bietet auch Funktionen wie Unterstützung für Amazon-DynamoDB-Transaktionen, automatische Attributwertserialisierung und Deserialisierung und Kompatibilität mit gängigen Python-Frameworks wie Flask und Django. Dieses Muster hilft Entwicklern bei der Arbeit mit Python und DynamoDB, indem es eine Bibliothek bereitstellt, die die automatische Erstellung von PynamoDB-Modellen und CRUD-Operationsfunktionen optimiert. Es generiert zwar wichtige CRUD-Funktionen für Datenbanktabellen, kann aber auch PynamoDB-Modelle und CRUD-Funktionen aus Amazon-DynamoDB-Tabellen zurückentwerfen. Dieses Muster soll den Datenbankbetrieb mithilfe einer Python-basierten Anwendung vereinfachen.

Im Folgenden sind die wichtigsten Features dieser Lösung aufgeführt:

- JSON-Schema in PynamoDB-Modell – Generieren Sie PynamoDB-Modelle automatisch in Python, indem Sie eine JSON-Schemadatei importieren.
- CRUD-Funktionsgenerierung – Generieren Sie automatisch Funktionen, um CRUD-Operationen für DynamoDB-Tabellen auszuführen.
- Reverse-Engineering von DynamoDB – Verwenden Sie PynamoDB Object-relational Mapping (ORM), um PynamoDB-Modelle und CRUD-Funktionen für vorhandene Amazon-DynamoDB-Tabellen zurückzuentwickeln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Python Version 3.8 oder höher, heruntergeladen und installiert
- Jinja2 Version 3.1.2 oder höher, heruntergeladen und installiert
- Amazon-DynamoDB-Tabellen, für die Sie ORM generieren möchten
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- PynamoDB Version 5.4.1 oder höher, installiert

Architektur

Zieltechnologie-Stack

- JSON-Skript
- Python-Anwendung
- PynamoDB-Modell
- Amazon-DynamoDB-Datenbank-Instance

Zielarchitektur

1. Sie erstellen eine JSON-Eingabeschemadatei. Diese JSON-Schemadatei stellt die Attribute der jeweiligen DynamoDB-Tabellen dar, aus denen Sie PynamoDB-Modelle erstellen möchten, und CRUD-Funktionen. Es enthält die folgenden drei wichtigen Schlüssel:
   - `name` – Der Name der DynamoDB-Zieltabelle.
   - `region` – Die AWS-Region, in der die Tabelle gehostet wird
   - `attributes` – Die Attribute, die Teil der Zieltabelle sind, z. B. der Partitionsschlüssel (auch als Hash-Attribut bezeichnet), Sortierschlüssel , lokale sekundäre Indizes, globale sekundäre Indizes und alle Nicht-Schlüsselattribute . https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.CoreComponents.html#HowItWorks.CoreComponents.TablesItemsAttributes Dieses Tool erwartet, dass das Eingabeschema nur die Nicht-Schlüsselattribute bereitstellt,

wenn die Anwendung die Schlüsselattribute direkt aus der Zieltabelle abruft. Ein Beispiel für die Angabe von Attributen in der JSON-Schemadatei finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

2. Führen Sie die Python-Anwendung aus und stellen Sie die JSON-Schemadatei als Eingabe bereit.
3. Die Python-Anwendung liest die JSON-Schemadatei.
4. Die Python-Anwendung stellt eine Verbindung zu den DynamoDB-Tabellen her, um das Schema und die Datentypen abzuleiten. Die Anwendung führt den Vorgang describe_table aus und ruft die Schlüssel- und Indexattribute für die Tabelle ab.
5. Die Python-Anwendung kombiniert die Attribute aus der JSON-Schemadatei und der DynamoDB-Tabelle. Es verwendet die Jinja-Vorlagen-Engine, um ein PynamoDB-Modell und entsprechende CRUD-Funktionen zu generieren.
6. Sie greifen auf das PynamoDB-Modell zu, um CRUD-Operationen für die DynamoDB-Tabelle auszuführen.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Andere Tools

- Jinja ist eine erweiterbare Vorlagen-Engine, die Vorlagen in optimiertem Python-Code kompiliert. Dieses Muster verwendet Jinja, um dynamische Inhalte zu generieren, indem Platzhalter und Logik in Vorlagen eingebettet werden.
- PynamoDB ist eine Python-basierte Schnittstelle für Amazon DynamoDB .
- Python ist eine Allzweck-Computer-Programmiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub PynamoDB-Modelle und CRUD-Funktionen automatisch generieren verfügbar. Das Repository ist in zwei Hauptteile unterteilt: das Controller-Paket und die Vorlagen.

Controller-Paket

Das Controller-Python-Paket enthält die Hauptanwendungslogik, die bei der Generierung des PynamoDB-Modells und der CRUD-Funktionen hilft. Sie enthält Folgendes:

- `input_json_validator.py` – Diese Python-Skripte validieren die JSON-Eingabeschemadatei und erstellen die Python-Objekte, die die Liste der DynamoDB-Zieltabellen und die jeweils erforderlichen Attribute enthalten.
- `dynamo_connection.py` – Dieses Skript stellt eine Verbindung zur DynamoDB-Tabelle her und verwendet die -`describe_table`Operation, um die Attribute zu extrahieren, die zum Erstellen des PynamoDB-Modells erforderlich sind.
- `generate_model.py` – Dieses Skript enthält eine Python-Klasse`GenerateModel`, die das PynamoDB-Modell basierend auf der JSON-Eingabeschemadatei und der -`describe_table`Operation erstellt.
- `generate_crud.py` – Für die DynamoDB-Tabellen, die in der JSON-Schemadatei definiert sind, verwendet dieses Skript die `GenerateCrud` Operation , um die Python-Klassen zu erstellen.

Vorlagen

Dieses Python-Verzeichnis enthält die folgenden Jinja-Vorlagen:

- `model.jinja` – Diese Jinja-Vorlage enthält den Vorlagenausdruck zum Generieren des PynamoDB-Modellskripts.
- `crud.jinja` – Diese Jinja-Vorlage enthält den Vorlagenausdruck zum Generieren des CRUD-Funktionsskripts.

Polen

Einrichten der Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um das Repository PynamoDB-Modelle und CRUD-Funktionen automatisch zu klonen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/amazon-reverse-engineer-dynamodb.git`	

Richten Sie die Python-Umgebung ein.	1. Navigieren Sie im geklonten Repository zum Verzeichnis der obersten Ebene.
	`cd amazon-reverse-engineer-dynamodb`
	2. Geben Sie den folgenden Befehl ein, um die erforderlichen Bibliotheken und Pakete zu installieren.
	`pip install -r requirements.txt`
		App-Developer

Generieren des PynamoDB-Modells und der CRUD-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die JSON-Schemadatei.	1. Navigieren Sie im geklonten Repository zum Verzeichnis der obersten Ebene. `cd amazon-reverse-engineer-dynamodb` 2. Öffnen Sie die `test.json` Datei in Ihrem bevorzugten Editor. Sie können diese Datei als Referenz	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, um Ihre eigene JSON-Schemadatei zu erstellen, oder Sie können die Werte in dieser Datei entsprechend Ihrer Umgebung aktualisieren. 3. Ändern Sie die Werte für Name AWS-Regio nund Attribute für Ihre DynamoDB-Zieltabellen. Hinweis: Wenn Sie eine Tabelle definieren, die in der JSON-Schemadatei nicht vorhanden ist, generiert diese Lösung keine Modelle oder CRUD-Funktionen für diese Tabelle. 4. Speichern und schließen Sie die Datei `test.json` . Wir empfehlen, diese Datei mit einem neuen Namen zu speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Python-Anwendung aus.	Geben Sie den folgenden Befehl ein, um die PynamoDB-Modelle und CRUD-Funktionen zu generieren, wobei der Name Ihrer JSON-Schemadatei `<input_schema.json>` ist. `python main.py --file <input_schema.json>`	App-Developer

Überprüfen des PynamoDB-Modells und der CRUD-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das generierte PynamoDB-Modell.	1. Geben Sie im Verzeichnis der obersten Ebene des geklonten Repositorys den folgenden Befehl ein, um zum `models`Repository zu navigieren. `cd models` 2. Standardmäßig benennt diese Lösung die PynamoDB-Modelldatei `demo_model.py` . Überprüfen Sie, ob diese Datei vorhanden ist.	App-Developer
Überprüfen Sie die generierten CRUD-Funktionen.	1. Geben Sie im Verzeichnis der obersten Ebene des geklonten Repositorys den folgenden Befehl ein, um	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zum `crud`Repository zu navigieren. `cd crud` 2. Standardmäßig benennt diese Lösung das Skript `demo_crud.py` . Überprüfen Sie, ob diese Datei vorhanden ist. 3. Verwenden Sie die Python-Klassen in der -`demo_crud.py` Datei, um eine CRUD-Operation für die DynamoDB-Zieltabelle auszuführen. Bestätige n Sie, dass der Vorgang erfolgreich abgeschlossen wurde.	

Zugehörige Ressourcen

- Kernkomponenten von Amazon DynamoDB (DynamoDB-Dokumentation)
- Verbesserung des Datenzugriffs mit sekundären Indizes (DynamoDB-Dokumentation)

Zusätzliche Informationen

Beispielattribute für die JSON-Schemadatei

```
[
{
"name": "test_table",
"region": "ap-south-1",
"attributes": [
{
```

```
"name": "id",
"type": "UnicodeAttribute"
},
{
"name": "name",
"type": "UnicodeAttribute"
},
{
"name": "age",
"type": "NumberAttribute"
}
]
}
]
```

Entdecken Sie die Full-Stack-Entwicklung von cloudnativen Webanwendungen mit Green Boost

Erstellt von Ben Stickley (AWS) und Amiin Samatar (AWS)

Umgebung: PoC oder Pilot	Technologien: Softwaree ntwicklung und -tests; Web- und mobile Apps; Cloud-native	Arbeitslast: Open Source
AWS-Dienste: Amazon Aurora; AWS CDK; Amazon CloudFront; AWS Lambda; AWS WAF		

Übersicht

Als Reaktion auf die sich wandelnden Bedürfnisse von Entwicklern ist sich Amazon Web Services (AWS) der dringenden Nachfrage nach einem effizienten Ansatz für die Entwicklung cloudnativer Webanwendungen bewusst. Der Schwerpunkt von AWS liegt darauf, Sie bei der Überwindung häufiger Hindernisse im Zusammenhang mit der Bereitstellung von Web-Apps in der AWS-Cloud zu unterstützen. Durch die Nutzung der Funktionen moderner Technologien wie AWS Cloud Development Kit (AWS CDK) TypeScript, React und Node.js zielt dieses Muster darauf ab, den Entwicklungsprozess zu rationalisieren und zu beschleunigen.

Das Muster basiert auf dem Green Boost (GB) -Toolkit und bietet einen praktischen Leitfaden für die Erstellung von Webanwendungen, die die umfangreichen Funktionen von AWS in vollem Umfang nutzen. Es dient als umfassende Roadmap, die Sie durch den Prozess der Bereitstellung einer grundlegenden CRUD-Webanwendung (Create, Read, Update, Delete) führt, die in die Amazon Aurora PostgreSQL-Compatible Edition integriert ist. Dies wird durch die Verwendung der Green Boost-Befehlszeilenschnittstelle (Green Boost CLI) und die Einrichtung einer lokalen Entwicklungsumgebung erreicht.

Nach der erfolgreichen Bereitstellung der Anwendung befasst sich das Pattern mit den wichtigsten Komponenten der Web-App, einschließlich Infrastrukturdesign, Backend- und Frontend-Entwicklung sowie mit wichtigen Tools wie cdk-dia für die Visualisierung, die ein effizientes Projektmanagement ermöglichen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git installiert
- Visual Studio Code (VS Code) installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI) installiert
- Das AWS CDK Toolkit ist installiert
- Node.js 18 installiert oder Node.js 18 mit aktiviertem pnpm
- pnpm ist installiert, falls es nicht Teil Ihrer Node.js Installation ist
- Grundkenntnisse in AWS CDK TypeScript, Node.js und React
- Ein aktives AWS-Konto
- Ein AWS-Konto, das mithilfe von AWS CDK in gestartet wurde. `us-east-1` Die `us-east-1` AWS-Region ist für die Unterstützung der Amazon CloudFront Lambda @Edge -Funktionen erforderlich.
- AWS-SicherheitsanmeldedatenAWS_ACCESS_KEY_ID, einschließlich korrekt konfigurierter Anmeldeinformationen in Ihrer Terminalumgebung
- Für Windows-Benutzer ein Terminal im Administratormodus (um der Art und Weise Rechnung zu tragen, wie pnpm mit Knotenmodulen umgeht)

Versionen der Produkte

- AWS-SDK für JavaScript Version 3
- AWS CDK Version 2
- AWS-CLI Version 2.2
- Node.js, Version 18
- React-Version 18

Architektur

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-Compatible Edition
- Amazon CloudFront
- Amazon CloudWatch

- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Lambda
- AWS Secrets Manager
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon-Simple-Storage-Service (Amazon-S3)
- AWS WAF

Zielarchitektur

Das folgende Diagramm zeigt, dass Benutzeranfragen Amazon CloudFront, AWS WAF und AWS Lambda durchlaufen, bevor sie mit einem S3-Bucket, einer Aurora-Datenbank, einer EC2-Instance interagieren und letztendlich Entwickler erreichen. Administratoren hingegen verwenden Amazon SNS und Amazon CloudWatch für Benachrichtigungen und Überwachungszwecke.

Um nach der Bereitstellung einen tieferen Einblick in die Anwendung zu erhalten, können Sie mithilfe von cdk-dia ein Diagramm erstellen, wie im folgenden Beispiel gezeigt.

Diese Diagramme zeigen die Architektur der Webanwendung aus zwei unterschiedlichen Blickwinkeln. Das cdk-dia-Diagramm bietet einen detaillierten technischen Überblick über die AWS-CDK-Infrastruktur und hebt bestimmte AWS-Services wie Amazon Aurora PostgreSQL-Compatible und AWS Lambda hervor. Im Gegensatz dazu nimmt das andere Diagramm eine breitere Perspektive ein und betont den logischen Datenfluss und die Benutzerinteraktionen. Der Hauptunterschied liegt im Detaillierungsgrad: Das cdk-dia befasst sich mit technischen Feinheiten, während das erste Diagramm eine eher benutzerorientierte Ansicht bietet.

Die Erstellung des cdk-dia-Diagramms wird im Epos Verstehen der App-Infrastruktur mithilfe von AWS CDK behandelt.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten. Dieses Muster verwendet AWS Systems Manager Session Manager.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, mit dem Sie beliebige Datenmengen speichern, schützen und abrufen können. Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- AWS WAF ist eine Webanwendungs-Firewall, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem.
- Green Boost ist ein Toolkit für die Erstellung von Web-Apps auf AWS.

- Next.js ist ein React-Framework zum Hinzufügen von Funktionen und Optimierungen.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.
- pnpm ist ein Paketmanager für Node.js Projektabhängigkeiten.

Bewährte Methoden

Weitere Informationen zu den folgenden Empfehlungen finden Sie im Abschnitt Epics:

- Überwachen Sie die Infrastruktur mithilfe von Amazon CloudWatch Dashboards und Alarmen.
- Setzen Sie bewährte AWS-Verfahren durch, indem Sie cdk-nag verwenden, um statische Infrastructure-as-Code-Analysen (IaC) durchzuführen.
- Richten Sie die DB-Portweiterleitung über SSH-Tunneling (Secure Shell) mit Systems Manager Session Manager ein. Dies ist sicherer als eine öffentlich zugängliche IP-Adresse.
- Verwalten Sie Sicherheitslücken, indem Sie Folgendes ausführen: `pnpm audit`
- Setzen Sie bewährte Verfahren durch, indem Sie ESLint zur Durchführung statischer TypeScript Codeanalysen und Prettier zur Standardisierung der Codeformatierung verwenden.

Epen

Stellen Sie eine CRUD-Web-App mit Aurora PostgreSQL-kompatibel bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Green Boost CLI.	Führen Sie den folgenden Befehl aus, um Green Boost CLI zu installieren. `pnpm add -g gboost`	App-Developer
Erstellen Sie eine GB-App.	1. Führen Sie den Befehl aus, um eine App mit Green	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Boost zu erstellengboost create. 2. Wählen Sie als Vorlage CRUD App with Aurora PostgreSQL aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Abhängigkeiten und stellen Sie die App bereit.	1. Navigieren Sie zum Projektverzeichnis:`cd <your directory>` . 2. Führen Sie den Befehl aus, um Abhängigkeiten zu installieren`pnpm i`. 3. Navigieren Sie zum Infra-Verzeichnis:`cd infra`. 4. Führen Sie den Befehl `pnpm deploy:local` aus, um die App lokal bereitzustellen. Dies ist ein Alias für einen `cdk deploy ...` Befehl, der in definiert ist`infra/package.json` . Warten Sie, bis die Bereitstellung abgeschlossen ist (ca. 20 Minuten). Überwachen Sie die CloudFormation AWS-Stacks in der CloudFormation Konsole, während Sie warten. Beachten Sie, wie die im Code definierten Konstrukte der bereitgestellten Ressource zugeordnet sind. Sehen Sie sich die CDK Construct-Strukturansicht in der CloudFormation Konsole an.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die App zu.	Nachdem Sie Ihre GB-App lokal bereitgestellt haben, können Sie über die CloudFront URL darauf zugreifen. Die URL wird in der Terminalausgabe gedruckt, aber es kann etwas überwältigend sein, sie zu finden. Gehen Sie wie folgt vor, um sie schneller zu finden: 1. Öffnen Sie das Terminal, in dem Sie den `pnpm deploy:local` Befehl ausgeführt haben. 2. Suchen Sie in der Terminalausgabe nach einem Abschnitt, der dem folgenden Text ähnelt. `myapp5stickbui9C39A55A.CloudFrontDomainName = d1q16n5pof924c.cloudfront.net` Die URL wird für Ihre Bereitstellung eindeutig sein. Alternativ können Sie die CloudFront URL finden, indem Sie auf die CloudFront Amazon-Konsole zugreifen:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zum CloudFront Service. 2. Suchen Sie in der Liste nach der zuletzt bereitgestellten Distribution. Kopieren Sie den Domainnamen, der der Distribution zugeordnet ist. Es wird ähnlich aussehen wie `your-unique-id.cloudfront.net` .	

Überwachen Sie mithilfe von Amazon CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich das CloudWatch Dashboard an.	1. Öffnen Sie die CloudWatch Konsole und wählen Sie Dashboards. 2. Wählen Sie das Dashboard mit dem Namen - - Dashboard <appId><stageName>aus. 3. Überprüfen Sie das Dashboard. Welche Ressourcen werden überwacht? Welche Metriken werden aufgezeichnet? Dieses Dashboard wird durch das Open-Sour	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ce-Konstrukt cdk-monitoring-constructsermöglicht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Alarme aktivieren.	Ein CloudWatch Dashboard hilft Ihnen dabei, Ihre Web-App aktiv zu überwachen. Um Ihre Web-App passiv zu überwachen, können Sie Warnmeldungen aktivieren.
	1. Navigieren Sie zu `/infra/src/app/stateless/monitor-stack.ts` , was den Monitor-Stack definiert.
	2. Kommentieren Sie die folgende Zeile aus und `admin@example.com` ersetzen Sie sie durch Ihre E-Mail-Adresse.
	`onAlarmTopic.addSubscription(new EmailSubscription("admin@example.com"));`
	3. Fügen Sie die folgenden Importinformationen am Anfang der Datei hinzu.
	`import { EmailSubscription } from "aws-cdk-lib/aws-sns-subscriptions";`
	4. Führen Sie darin den folgenden Befehl aus. `infra/`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk deploy "*/monitor" --exclusively.` 5. Um Ihr Abonnement für das SNS-Thema zu bestätigen, das ausgelöst wird, wenn ein Überwachungsalarm ausgelöst wird, klicken Sie auf den Link in der E-Mail-Nachricht.	

Verstehen Sie die App-Infrastruktur mithilfe von AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Architektdiagramm.	Generieren Sie mithilfe von cdk-dia ein Architekturdiagramm Ihrer Web-App. Die Visualisierung der Architektur trägt dazu bei, das Verständnis und die Kommunikation zwischen den Teammitgliedern zu verbessern. Es bietet einen klaren Überblick über die Komponenten des Systems und ihre Beziehungen. 1. Installieren Sie Graphviz. 2. Führen Sie `infra/` darin den Befehl aus. `pnpm cdk-dia` 3. Sehen Sie sich Ihre `aninfra/diagram.png` .	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie cdk-nag, um bewährte Verfahren durchzuse tzen.	Verwenden Sie cdk-nag, um eine sichere und regelkonf orme Infrastruktur aufrechtz uerhalten, indem Sie bewährte Verfahren durchsetzen und so das Risiko von Sicherhei tslücken und Fehlkonfi gurationen verringern. 1. Erfahren Sie im Abschnitt Regeln, wie cdk-nag bewährte Verfahren durchsetzt, einschließlich der Prüfungen aus dem Regelpaket der AWS Solutions Library. 2. Um zu sehen, wie cdk-nag Regeln durchsetzt, nehmen Sie eine Änderung im Code vor. Zum Beispiel in, ändern Sie `zuinfra/src/app/stateful/data-stacks.ts` . `storageEncrypted: true` `storageEncrypted: false` 3. Führen Sie darin den Befehl aus `cdk synth "*/data"`. `infra/` Während der Synthese wird ein Build-Fehler auftreten, der auf einen Regelverstoß hinweist.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`AwsSolutions-RDS2: The RDS instance or Aurora DB cluster does not have storage encryption enabled.`
	
	Dieser Fehler zeigt, dass cdk-nag ein Sicherhei tsmechanismus ist, der bewährte Methoden für die Infrastruktur durchsetzt und Sicherheitsfehlkonfiguratio nen verhindert.
	4. Bei Bedarf können Sie auch Regeln in unterschiedlichen Bereichen unterdrüc ken. Um beispielsweise AwsSolutions -RDS2 zu unterdrücken, fügen Sie den folgenden Code unter der Instanziierung von hinzu. `DbIamCluster`
	
	`NagSuppressions.addResourceSuppressions( cluster.node.findChild("Resource"), [ { id: "AwsSolutions-RDS2", reason: "Customer requirement necessitates`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`having unencrypted DB storage", }, ], );` 5. Führen Sie den Vorgang nach der Unterdrückung erneut aus. `cdk synth "*/data"` Ihre AWS CDK-App sollte jetzt erfolgreich synthetisiert werden. Sie finden alle unterdrückten Regeln unter. `infra/cdk.out/assembly-<appId>-<stageName>/AwsSolutions-<appId>-<stageName>-${stackId}-NagReport.csv`	

Evaluieren Sie die Datenbankkonfiguration und das Schema

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erwerben Sie Umgebungsvariablen.	Gehen Sie wie folgt vor, um die erforderlichen Umgebungsvariablen abzurufen: 1. Um die zu findenDB_BASTION_ID , melden Sie sich bei der Konsole an und navigieren Sie zur EC2-Konsole. Wählen Sie Instances (running) und suchen Sie	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Zeile, die - ssm-db-bastion Name <stageName>enthält. Die Instanz-ID beginnt mit i-. 2. Um das zu findenDB_ENDPOINT , wählen Sie in der Amazon Relational Database Service (Amazon RDS) -Konsole DB Instances und dann den regionalen Cluster aus, dessen DB-ID mit - -data <appId><stageName>- beginnt. Suchen Sie den Writer-Instance-Endpunkt, der auf rds.amazonaws.com endet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Portweiterleitung ein.	Gehen Sie wie folgt vor, um die Portweiterleitung einzurichten: 1. Installieren Sie das AWS Systems Manager Session Manager-Plug-In. 2. Starten Sie die Portweiterleitung, indem `core/` Sie `pnpm db:connect` within ausführen, um eine sichere Verbindung über den Bastion-Host herzustellen. 3. Nachdem Sie den Text `Waiting for connections...,` in Ihrem Terminal sehen, wurde erfolgreich ein SSH-Tunnel zwischen Ihrem lokalen Computer und dem Aurora-Server über den EC2-Bastion-Host eingerichtet.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Timeout für den Systems Manager Session Manager an.	(Optional) Wenn das standardmäßige Sitzungstimeout von 20 Minuten zu kurz ist, können Sie es in der Systems Manager Manager-Konsole auf bis zu 60 Minuten erhöhen, indem Sie Sitzungsmanager, Einstellungen, Bearbeiten, Timeout für Leerlaufsitzungen wählen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Visualisieren Sie die Datenbank.	pgAdmin ist ein benutzerf reundliches Open-Source-Tool zur Verwaltung von PostgreSQL-Datenbanken. Es vereinfacht Datenbank aufgaben und ermöglicht es Ihnen, Datenbanken effizient zu erstellen, zu verwalten und zu optimieren. Dieser Abschnitt führt Sie durch die Installation von pgAdmin und die Verwendung seiner Funktionen für die PostgreSQ L-Datenbankverwaltung. 1. Öffnen Sie im Objekt-Ex plorer das Kontextmenü (Rechtsklick) für Server und wählen Sie dann Register, Server. 2. Geben Sie auf der Registerkarte Allgemein - <appId><stageName>für das Feld Name ein. 3. Um das DB-Passwort abzurufen, öffnen Sie die AWS Secrets Manager Manager-Konsole, wählen Sie das Geheimnis mit der vom CDK generiert en Beschreibung für den Stack: - -data <appId><s tageName>aus und wählen Sie die Secret Value-Karte	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus. Wählen Sie Retrieve Secret Value und kopieren Sie den Secret-Wert mit einem Passwortschlüssel. 4. Geben Sie auf der Registerkarte Verbindung 0.0.0.0 für das Feld Hostname/Adresse und _admin für das Feld Benutzername ein. <appId> Verwenden Sie für das Feld Passwort das Geheimnis, das Sie zuvor abgerufen haben. Wählen Sie Ja für das Feld Passwort speichern? Feld. 5. Wählen Sie Speichern. 6. Um die Tabellen anzuzeigen, navigieren Sie zu -, Datenbanken, _db, Schemas,, Tabellen. <appId><stageName> <appId><appId> 7. Öffnen Sie das Kontextmenü (Rechtsklick) für die Elementtabelle und wählen Sie dann Daten anzeigen/bearbeiten, Alle Zeilen aus. 8. Erkunden Sie die Tabelle.	

Debuggen Sie mit Node.js

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Debuggen Sie den Anwendungsfall „Objekt erstellen“.	Gehen Sie wie folgt vor, um den Anwendungsfall „Element erstellen“ zu debuggen:
	1. Öffnen Sie die `core/src/modules/item/create-item.use-case.ts` Datei und fügen Sie den folgenden Code ein.
	`import { fileURLToPath } from "node:url";`
	
	`// existing create-item.use-case.ts code here`
	
	`if (process.argv[1] === fileURLToPath(import.meta.url)) {`
	`  createItemUseCase({`
	`  description: "Item 1's Description",`
	`  name: "Item 1",`
	`  });`
	`}`
	2. Der im vorherigen Schritt hinzugefügte Code stellt sicher, dass die `createItemUseCase` Funktion aufgerufen wird, wenn dieses Modul direkt
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausgeführt wird. Setzen Sie Haltepunkte in den Zeilen innerhalb dieses Codeblocks, in denen Sie das line-by-line Debugging einleiten möchten. 1. Öffnen Sie das VS Code JavaScript Debug Terminal und führen Sie es dann aus, `pnpm tsx core/src/modules/item/create-item.use-case.ts` um den Code mit Debugging auszuführen. line-by-line Sie können auch `console.log` Anweisungen verwenden, aber Print-Anweisungen können unzureichend sein, wenn Sie mit komplexer Geschäftslogik arbeiten. ine-by-line L-Debugging bietet Ihnen mehr Kontext.	

Entwickeln Sie das Frontend

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Entwicklungsserver ein.	1. Navigieren Sie zum `ui/` Entwicklungsserver Next.js und führen Sie ihn aus, `pnpm dev` um ihn zu starten.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Greifen Sie lokal auf Ihre Web-App zu unter `http://localhost:3000` . Der Entwicklungsserver Next.js ist mit sofortigem Fast Refresh-Feedback zu Änderungen an Ihren React-Komponenten eingerichtet. 3. Experimentieren Sie mit der Anpassung der Farbe der App-Leiste. Öffnen Sie die `ui/src/components/theme/theme.tsx` Datei und suchen Sie den Abschnitt, der das Thema für die App-Leiste definiert. Aktualisieren Sie in dem `colorSchemes.light.palette.primary` Abschnitt den Hauptwert von `colors.lagoon` `biscolors.carrot` . Nachdem Sie diese Änderung vorgenommen haben, speichern Sie die Datei und beobachten Sie das Update in Ihrem Browser. 4. Experimentieren Sie, indem Sie Text und Komponenten ändern und neue Seiten hinzufügen.	

Tooling mit Green Boost

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Monorepo und den pnpm-Paketmanager ein.	1. Sehen Sie `pnpm-workspace.yaml` im Stammverzeichnis Ihres GB-Repositorys nach und achten Sie darauf, wie Workspaces definiert sind. Weitere Informationen zu Workspaces finden Sie in der pnpm-Dokumentation. 2. Lesen Sie `ui/package.json` sich durch und achten Sie darauf, wie es `core/` mit dem Paketnamen auf den Workspace verweist. `"<appId>/core": "workspace:^",` 3. Beobachten Sie, wie TypeScript die ESLint-Konfiguration in den darin definierten `packages/` Utility-Paketen zentralisiert ist. Diese Konfiguration wird dann von Anwendungspaketen wie `core/infra/`, und `ui/` verwendet. Dies ist hilfreich, wenn Ihre App skaliert und Sie mehr Anwendungspakete definieren, die auf die Dienstprogrammpakete verweisen können, ohne	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Konfigurationscode zu duplizieren.	
Führen Sie pnpm-Skripte aus.	Führen Sie die folgenden Befehle im Stammverzeichnis Ihres Repositorys aus: 1. Führen Sie `pnpm lint`. Dieser Befehl führt eine statische Codeanalyse mit ESLint aus. 2. Führen Sie `pnpm typecheck .` Dieser Befehl führt den TypeScript Compiler aus, um die Typen Ihres Codes zu überprüfen. 3. Führen Sie `pnpm test`. Dieser Befehl führt Vitest aus, um Komponententests auszuführen. Beachten Sie, wie diese Befehle in allen Arbeitsbereichen ausgeführt werden. Die Befehle sind in den Feldern der einzelnen Workspaces definiert. `package.json#scripts`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie ESLint für die statische Codeanalyse.	Gehen Sie wie folgt vor, um die Fähigkeit von ESLint zur statischen Codeanalyse zu testen: 1. Stellen Sie zunächst sicher, dass die VS Code ESLint-Erweiterung (ID:`dbaeumer.vscode-eslint`) installiert ist. Wir empfehlen, auch VS Code Error Lens (ID:`usernamehw.errorlens`) zu installieren, um Fehler direkt anzuzeigen. 2. Fügen Sie Ihrem Code bewusst eine Codezeile hinzu, die die `eval()` Funktion verwendet, wie im folgenden Beispiel gezeigt. `const userInput = "import("fs").then((fs) => console.log(fs.readFileSync("/etc/passwd", { encoding: "utf8" })))"; eval(userInput);` Wichtig: Dies dient nur zu Testzwecken. `eval()`Die Verwendung gilt als potenziell gefährlich und sollte aufgrund	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von Sicherheitsrisiken vermieden werden. 3. Nachdem Sie die `eval()` Zeile eingefügt haben, öffnen Sie Ihren Code-Editor, um anhand roter Schnörkel zu überprüfen, ob ESLint den Codegeruch angezeigt hat. 4. Weitere Informationen zu den ESLint-Plugins und der Konfiguration finden Sie unter. `packages/eslint-config-{node,next}/.eslintrc.cjs`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abhängigkeiten und Sicherheitslücken verwalten.	1. Führen `pnpm audit` Sie das Programm im Stammverzeichnis Ihres Repositorys aus, um allgemeine Sicherheitslücken und Risiken (Common Vulnerabilities and Exposures, CVEs) zu identifizieren. Dort sollte die Meldung Keine bekannten Sicherheitslücken gefunden angezeigt werden. 2. Installieren Sie ein absichtlich anfälliges Paket darin`pnpm add minimist@0.2.3` , `core/` indem Sie es ausführen und dann ausführen`pnpm audit`. Beachten Sie die gemeldete Sicherheitslücke. 3. Deinstallieren Sie das darin enthaltene anfällige Paket, `core/` indem Sie Folgendes ausführen`pnpm remove minimist`.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hooks mit Husky vor dem Commit.	1. Nehmen Sie ein paar kleine Änderungen an den TypeScript Dateien im gesamten Repository vor. Die Änderungen können so einfach sein wie das Hinzufügen von Kommentaren. 2. Stellen Sie diese Änderungen bereit und übernehmen Sie sie, indem Sie `git add -A` und then verwenden`git commit -m "test husky"`. Der Husky-Pre-Commit-Hook-Trigger, der in definiert ist`.husky/pre-commit` , führt den Befehl aus. `pnpm lint-staged` 3. Beobachten Sie, wie lint-staged Befehle, die in `*/.lintstagedrc.js` Dateien angegeben sind, im gesamten Repository auf Dateien ausführt, die von Git bereitgestellt wurden. Diese Tools sind Mechanismen, die verhindern sollen, dass böser Code in Ihre Anwendung gelangt.	App-Developer

Reißen Sie die Infrastruktur nieder

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Bereitstellung aus Ihrem Konto.	1. Um die Infrastruktur, die Sie im ersten Epic bereitgestellt haben, durch Run `pnpm destroy:local` In `infra/` abzubauen. 2. Warten Sie 15 Minuten, bis der `pnpm destroy:local` Vorgang abgeschlossen ist, und löschen Sie dann die beibehaltene Lambda @Edge -Funktion , indem Sie in der Lambda-Konsole nach Ihrer App-ID suchen. Lambda @Edge -Funktionen werden repliziert, was es schwierig macht, sie zu löschen. Weitere Informationen zum Löschen von Lambda @Edge -Funktionen finden Sie in der CloudFront Dokumentation.	App-Developer

Fehlerbehebung

Problem	Lösung
Die Portweiterleitung konnte nicht eingerichtet werden	Stellen Sie sicher, dass Ihre AWS-Anmeldeinformationen ordnungsgemäß konfiguriert sind und über die erforderlichen Berechtigungen verfügen.

Problem	Lösung
	Vergewissern Sie sich, dass die Umgebungsvariablen Bastion-Host-ID (`DB_BASTION_ID`) und Datenbank-Endpunkt (`DB_ENDPOINT`) korrekt gesetzt sind. Falls weiterhin Probleme auftreten, finden Sie in der AWS-Dokumentation Informationen zur Fehlerbehebung bei SSH-Verbindungen und im Session Manager.
Die Website wird nicht geladen `localhost:3000`	Vergewissern Sie sich, dass die Terminalausgabe eine erfolgreiche Portweiterleitung anzeigt, einschließlich der Weiterleitungsadresse. Stellen Sie sicher, dass es keine widersprüchlichen Prozesse gibt, die Port 3000 auf Ihrem lokalen Computer verwenden. Stellen Sie sicher, dass die Green Boost-Anwendung ordnungsgemäß konfiguriert ist und auf dem erwarteten Port (3000) ausgeführt wird. Überprüfen Sie Ihren Webbrowser auf Sicherheitserweiterungen oder Einstellungen, die lokale Verbindungen blockieren könnten.
Fehlermeldungen bei der lokalen Bereitstellung (`pnpm deploy:local`)	Überprüfen Sie die Fehlermeldungen sorgfältig, um die Ursache des Problems zu ermitteln. Stellen Sie sicher, dass die erforderlichen Umgebungsvariablen und Konfigurationsdateien korrekt eingestellt sind.

Zugehörige Ressourcen

- AWS-CDK-Dokumentation
- Green Boost-Dokumentation
- Dokumentation zu Next.js
- Dokumentation zu Node.js
- React-Dokumentation
- TypeScript Dokumentation

Ausführen von Einheitentests für eine Node.js-Anwendung von mithilfe GitHub von AWS CodeBuild

Erstellt von Bol Bol Bol Bol (AWS) und-Baptiste Guis (AWS)

Code-Repository: Beispiel für Knoten-JS-Tests	Umgebung: Produktion	Technologien: Softwaree ntwicklung und -tests
AWS-Services: AWS CodeBuild		

Übersicht

Dieses Muster bietet Beispiel-Quellcode und Testkomponenten für Schlüsseleinheiten für eine Node.js-Spiel-API. Es enthält auch Anweisungen zum Ausführen dieser Einheitentests aus einem GitHub Repository mithilfe von AWS CodeBuildals Teil Ihres CI/CD-Workflows (Continuous Integration and Continuous Delivery).

Komponententests sind ein Softwareentwicklungsprozess, bei dem verschiedene Teile einer Anwendung, die als Einheiten bezeichnet wird, einzeln und unabhängig auf korrekte Funktionsweise getestet werden. Tests überprüfen die Qualität des Codes und bestätigen, dass er wie erwartet funktioniert. Andere Entwickler können sich auch leicht mit Ihrer Codebasis vertraut machen, indem sie die Tests konsultieren. Einheitentests reduzieren die zukünftige Faktorwechselzeit, helfen Technikern dabei, Ihre Codebasis schneller zu erreichen und Vertrauen in das erwartete Verhalten zu schaffen.

Komponententests beinhalten das Testen einzelner Funktionen, einschließlich AWS Lambda-Funktionen. Um Komponententests zu erstellen, benötigen Sie ein Test-Framework und eine Möglichkeit, Tests (Zusicherungen) zu validieren. Die Codebeispiele in diesem Muster verwenden dasMocha-Test-Framework und dieChai-Assertion-Bibliothek .

Weitere Informationen zu Komponententests und Beispiele für Testkomponenten finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto mit korrekten CodeBuild Berechtigungen

- Ein - GitHub Konto (siehe Anweisungen zur Registrierung von)
- Git (siehe Installationsanweisungen)
- Ein Code-Editor, um Änderungen vorzunehmen und Ihren Code an zu übertragen GitHub (Sie können beispielsweise AWS Cloud9 verwenden)

Architektur

Dieses Muster implementiert die Architektur, die im folgenden Diagramm dargestellt ist.

Tools

Tools

- Git Bol Git ist ein Versionsverwaltungssystem, das Sie für die Codeentwicklung verwenden können.
- AWS Cloud9 ist AWS Cloud9 eine integrierte Entwicklungsumgebung (IDE), die eine umfassende Codebearbeitungserfahrung mit Unterstützung für mehrere Programmiersprachen und Laufzeit-Debugger sowie ein integriertes Terminal bietet. Es enthält eine Sammlung von Tools, die Sie verwenden, um Software zu codieren, zu erstellen, auszuführen, zu testen und zu debuggen, und Ihnen hilft, Software in der Cloud zu veröffentlichen. Sie greifen über einen Webbrowser auf die AWS Cloud9-IDE zu.
- AWS CodeBuild AWS CodeBuild ist ein vollständig verwalteter kontinuierlicher Integrationsservice, der Quellcode kompiliert, Tests ausführt und Softwarepakete erstellt, die bereitgestellt werden können. Mit müssen CodeBuildSie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht mehr in einer Warteschlange warten. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen. Mit werden CodeBuildIhnen die von Ihnen verwendeten Rechenressourcen nach Minuten berechnet.

Code

Der Quellcode für dieses Muster ist auf verfügbar GitHub, im Beispielanwendungs-Repository für Spieleinheitentests. Sie können Ihr eigenes GitHub Repository aus diesem Beispiel erstellen (Option 1) oder das Beispiel-Repository direkt (Option 2) für dieses Muster verwenden. Folgen Sie den

Anweisungen für jede Option im nächsten Abschnitt. Welche Option Sie befolgen, hängt von Ihrem Anwendungsfall ab.

Sekunden

Option 1 – Ausführen von Einheitentests in Ihrem persönlichen GitHub Repository mit CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihr eigenes GitHub Repository basierend auf dem Beispielprojekt.	1. Melden Sie sich bei an GitHub. 2. Erstellen Sie ein neues Repository. Anweisungen finden Sie in der GitHub - Dokumentation. 3. Klonen Sie das Beispiel-Repository und übertragen Sie es in das neue Repository in Ihrem Konto.	App-Entwickler, AWS-Administrator, AWS DevOps
Erstellen Sie ein neues CodeBuild Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CodeBuild Konsole unter https://console.aws.amazon.com/codesuite/codebuild/home. 2. Wählen Sie Create build project (Build-Projekt erstellen) aus. 3. Geben Sie im Abschnitt Projektkonfiguration für Projektname aws-tests-sample-node-js ein. 4. Wählen Sie im Abschnitt Quelle für Quellanbieter ausGitHub.	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie für Repository die Option Repository in meinem GitHub Konto aus und fügen Sie dann die URL in Ihr neu erstelltes GitHub Repository ein. 6. Wählen Sie im Abschnitt Webhook-Ereignisse der primären Quelle jedes Mal, wenn eine Codeänderung in dieses Repository übertragen wird, die Option Neu erstellen aus. 7. Wählen Sie als Ereignistyp PUSH aus. 8. Wählen Sie im Abschnitt Umgebung die Option Verwaltetes Image , Amazon Linux 2 und das neueste Image aus. 9. Behalten Sie die Standardeinstellungen für alle anderen Optionen bei und wählen Sie dann Build-Projekt erstellen aus.	
Starten Sie den Build.	Klicken Sie auf der Seite Review (Überprüfen) auf Start build (Build starten), um den Build auszuführen.	App-Entwickler, AWS-Administrator, AWS DevOps

Option 2 – Ausführen von Einheitentests in einem öffentlichen Repository mit CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein neues CodeBuild Build-Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CodeBuild Konsole unter https://console.aws.amazon.com/codesuite/codebuild/home. 2. Wählen Sie Create build project (Build-Projekt erstellen) aus. 3. Geben Sie im Abschnitt Projektkonfiguration für Projektname aws-tests-sample-node-js ein. 4. Wählen Sie im Abschnitt Quelle für Quellanbieter ausGitHub. 5. Wählen Sie für Repository die Option Öffentliches Repository aus und fügen Sie dann die URL ein: https://github.com/aws-samples/node-js-tests-sample. 6. Wählen Sie im Abschnitt Umgebung die Option Verwaltetes Image , Amazon Linux 2 und das neueste Image aus. 7. Behalten Sie die Standardeinstellungen für alle anderen Optionen bei und	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Build-Pro jekt erstellen aus.	
Starten Sie den Build.	Klicken Sie auf der Seite Review (Überprüfen) auf Start build (Build starten), um den Build auszuführen.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Analysieren der Komponententests

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Testergeb nisse an.	Überprüfen Sie in der - CodeBuild Konsole die Einheitentestergebnisse des CodeBuild Auftrags. Sie sollten mit den Ergebniss en übereinstimmen, die im Abschnitt Zusätzliche Informati onen angezeigt werden. Diese Ergebnisse validieren die GitHub Repository-Integra tion mit CodeBuild.	App-Entwickler, AWS-Admin istrator, AWS DevOps
Wenden Sie einen Webhook an.	Sie können jetzt einen Webhook anwenden, sodass Sie einen Build automatis ch starten können, wenn Sie Codeänderungen an den Hauptzweig Ihres Repositor ys übertragen. Anweisungen finden Sie in der CodeBuild Dokumentation .	App-Entwickler, AWS-Admin istrator, AWS DevOps

Zugehörige Ressourcen

- Beispiel für eine Testanwendung für Spieleinheiten (GitHub Repository mit Beispielcode)
- AWS- CodeBuild Dokumentation
- GitHub Webhook-Ereignisse (CodeBuild Dokumentation)
- Erstellen eines neuen Repositorys (GitHub Dokumentation)

Zusätzliche Informationen

Einheiten-Testergebnisse

In der CodeBuild Konsole sollten Sie die folgenden Testergebnisse sehen, nachdem das Projekt erfolgreich erstellt wurde.

Beispielkomponenten für Komponententests

In diesem Abschnitt werden die vier Arten von Testkomponenten beschrieben, die beim Komponententest verwendet werden: Assertionen, Spies, Stubs und Mocks. Es enthält eine kurze Erklärung und ein Codebeispiel für jede Komponente.

Assertionen

Eine Assertion wird verwendet, um ein erwartetes Ergebnis zu überprüfen. Dies ist eine wichtige Testkomponente, da sie die erwartete Antwort einer bestimmten Funktion validiert. Die folgende Beispiel-Assertion überprüft, ob die zurückgegebene ID bei der Initialisierung eines neuen Spiels zwischen 0 und 1000 liegt.

```
const { expect }  = require('chai');
const { Game } = require('../src/index');

describe('Game Function Group', () => {
 it('Check that the Game ID is between 0 and 1000', function() {
      const game = new Game();
      expect(game.id).is.above(0).but.below(1000)
 });
});
```

Spies

Ein Spy wird verwendet, um zu beobachten, was passiert, wenn eine Funktion ausgeführt wird. Sie können beispielsweise überprüfen, ob die Funktion korrekt aufgerufen wurde. Das folgende Beispiel zeigt, dass Start- und Stoppmethoden für ein Spielklassenobjekt aufgerufen werden.

```
const { expect }  = require('chai');
const { spy } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () => {
   it('should verify that the correct function is called', () => {
      const spyStart = spy(Game.prototype, "start");
      const spyStop = spy(Game.prototype, "stop");

      const game = new Game();
      game.start();
      game.stop();

      expect(spyStart.called).to.be.true
      expect(spyStop.called).to.be.true
    });
});
```

Stubs

Ein Stub wird verwendet, um die Standardantwort einer Funktion zu überschreiben. Dies ist besonders nützlich, wenn die Funktion eine externe Anforderung stellt, da Sie vermeiden möchten, dass externe Anforderungen aus Einheitentests stammen. (Externe Anforderungen eignen sich besser für Integrationstests, die Anforderungen zwischen verschiedenen Komponenten physisch testen können.) Im folgenden Beispiel erzwingt ein Stub eine Rückgabe-ID von der getId-Funktion.

```
const { expect }  = require('chai');
const {.stub } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let generateIdStub = stub(Game.prototype, 'getId').returns(999999);

      const game = new Game();
```

```
      expect(game.getId).is.equal(999999);

      generateIdStub.restore();
    });
});
```

Mocks

Ein Mock ist eine gefälschte Methode, die ein vorprogrammiertes Verhalten zum Testen verschiedener Szenarien aufweist. Ein Mock kann als erweiterte Form eines Stubs betrachtet werden und mehrere Aufgaben gleichzeitig ausführen. Im folgenden Beispiel wird ein Mock verwendet, um drei Szenarien zu validieren:

- Funktion wird aufgerufen
- Die Funktion wird mit Argumenten aufgerufen
- Funktion gibt die Ganzzahl 9 zurück

```
const { expect }  = require('chai');
const {.mock } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let mock = mock(Game.prototype).expects('getId').withArgs().returns(9);

      const game = new Game();
      const id = get.getId();

      mock.verify();
      expect(id).is.equal(9);
    });
});
```

Strukturieren eines Python-Projekts in hexaffinaler Architektur mit AWS Lambda

Erstellt vonkan Oruc (AWS), Dominik Goby (AWS), Dar Kunce (AWS) und Mi Ploski (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Softwaree ntwicklung und -tests; Cloudnativ; Container und Microservices; Serverless; Modernisierung	AWS-Services: Amazon DynamoDB ;AWS Lambda ;Amazon API Gateway

Übersicht

Dieses Muster zeigt, wie Sie ein Python-Projekt in der hexaffinalen Architektur mithilfe von AWS Lambda strukturieren. Das Muster verwendet das AWS Cloud Development Kit (AWS CDK) als Infrastructure as Code (IaC)-Tool, Amazon API Gateway als REST-API und Amazon DynamoDB als Persistenzschicht. Die hexoriale Architektur folgt domänengesteuerten Gestaltungsprinzipien. In der hexhexhexhexitionalen Architektur besteht die Software aus drei Komponenten: Domain, Ports und Adapter. Ausführliche Informationen zu Hexhexhex-Architekturen und ihren Vorteilen finden Sie im HandbuchHex-Integritätsarchitekturen auf AWS erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Erfahrung mit Python
- Vertrautheit mit AWS Lambda , AWS CDK, Amazon API Gateway und DynamoDB
- Ein GitHub Konto (siehe Anweisungen zur Registrierung von)
- Git (siehe Installationsanweisungen)
- Ein Code-Editor zum Vornehmen von Änderungen und Übertragen Ihres Codes an GitHub (z. B. AWS Cloud9, Visual Studio Code oder JetBrains PyCharm)
- Docker installiert und der Docker-Daemon betriebsbereit

Produktversionen

- Git Version 2.24.3 oder höher
- Python Version 3.7 oder höher
- AWS CDK v2
- Poetry Version 1.1.13 oder höher
- AWS Lambda Powertools für Python Version 1.25.6 oder höher
- pyteste Version 7.1.1 oder höher
- Moto-Version 3.1.9 oder höher
- pydantische Version 1.9.0 oder höher
- Boto3 Version 1.22.4 oder höher
- mypy-boto3-dynamodb Version 1.24.0 oder höher

Architektur

Zieltechnologie-Stack

Der Zieltechnologie-Stack besteht aus einem Python-Service, der API Gateway, Lambda und DynamoDB verwendet. Der Service verwendet einen DynamoDB-Adapter, um Daten beizubehalten. Es bietet eine Funktion, die Lambda als Eintrittspunkt verwendet. Der Service verwendet Amazon API Gateway, um eine REST-API bereitzustellen. Die API verwendet AWS Identity and Access Management (IAM) für die Authentifizierung von Clients.

Zielarchitektur

Zur Veranschaulichung der Implementierung stellt dieses Muster eine Serverless-Zielarchitektur bereit. Clients können Anfragen an einen API Gateway-Endpunkt senden. API Gateway leitet die Anforderung an die Lambda-Zielfunktion weiter, die das hexhexhexaffinale Architekturmuster implementiert. Die Lambda-Funktion führt CRUD-Operationen (Erstellen, Lesen, Aktualisieren und Löschen) für eine DynamoDB-Tabelle aus.

> Wichtig: Dieses Muster wurde in einer PoC-Umgebung getestet. Sie müssen eine Sicherhei tsüberprüfung durchführen, um das Bedrohungsmodell zu identifizieren und eine sichere Codebasis zu erstellen, bevor Sie eine Architektur in einer Produktionsumgebung bereitstellen.

Die API unterstützt fünf Operationen für eine Produktentität:

- `GET /products` gibt alle Produkte zurück.
- `POST /products` erstellt ein neues Produkt.
- `GET /products/{id}` gibt ein bestimmtes Produkt zurück.
- `PUT /products/{id}` aktualisiert ein bestimmtes Produkt.
- `DELETE /products/{id}` löscht ein bestimmtes Produkt.

Sie können die folgende Ordnerstruktur verwenden, um Ihr Projekt so zu organisieren, dass es dem hexaffinalen Architekturmuster folgt:

```
app/  # application code
|--- adapters/  # implementation of the ports defined in the domain
     |--- tests/  # adapter unit tests
|--- entrypoints/  # primary adapters, entry points
     |--- api/  # api entry point
          |--- model/  # api model
          |--- tests/  # end to end api tests
|--- domain/  # domain to implement business logic using hexagonal architecture
     |--- command_handlers/  # handlers used to execute commands on the domain
     |--- commands/  # commands on the domain
     |--- events/  # events triggered via the domain
     |--- exceptions/  # exceptions defined on the domain
     |--- model/  # domain model
     |--- ports/  # abstractions used for external communication
     |--- tests/  # domain tests
|--- libraries/  # List of 3rd party libraries used by the Lambda function
infra/  # infrastructure code
simple-crud-app.py  # AWS CDK v2 app
```

Tools

AWS-Services

- Amazon API Gateway ist ein vollständig verwalteter Service, der es Entwicklern erleichtert, APIs in jeder Größenordnung zu erstellen, zu veröffentlichen, zu warten, zu überwachen und zu sichern.

- Amazon DynamoDB ist eine vollständig verwaltete, serverlose NoSQL-Schlüsselwertdatenbank, die für die Ausführung von Hochleistungsanwendungen in jeder Größenordnung entwickelt wurde.
- AWS Lambda ist ein serverloser, ereignisgesteuerter Datenverarbeitungsservice, mit dem Sie Code für praktisch jeden Anwendungs- oder Backend-Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Sie können Lambda-Funktionen von über 200 AWS-Services und Software-as-a-Service (SaaS)-Anwendungen starten und nur für das bezahlen, was Sie tatsächlich nutzen.

Tools

- Git wird als Versionsverwaltungssystem für die Codeentwicklung in diesem Muster verwendet.
- Python wird als Programmiersprache für dieses Muster verwendet. Python bietet allgemeine Datenstrukturen und einen Ansatz für die objektorientierte Programmierung. AWS Lambda bietet eine integrierte Python-Laufzeit, die den Betrieb von Python-Services vereinfacht.
- Visual Studio Code wird als IDE für die Entwicklung und das Testen dieses Musters verwendet. Sie können jede IDE verwenden, die Python-Entwicklung unterstützt (z. B. AWS Cloud9 oder PyCharm).
- AWS Cloud Development Kit (AWS CDK) ist ein Open-Source-Softwareentwicklungs-Framework, mit dem Sie Ihre Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen definieren können. Dieses Muster verwendet das CDK, um die Cloud-Infrastruktur als Code zu schreiben und bereitzustellen.
- Poetry wird verwendet, um Abhängigkeiten im Muster zu verwalten.
- Docker wird vom AWS-CDK verwendet, um das Lambda-Paket und die Ebene zu erstellen.

Code

Der Code für dieses Muster ist im GitHub Lambda-Beispiel-Repository für die hexaffinale Architektur verfügbar.

Bewährte Methoden

Um dieses Muster in einer Produktionsumgebung zu verwenden, befolgen Sie diese bewährten Methoden:

- Verwenden Sie vom Kunden verwaltete Schlüssel in AWS Key Management Service (AWS KMS), um Amazon- CloudWatch Protokollgruppen und Amazon DynamoDB-Tabellen zu verschlüsseln.

- Konfigurieren Sie AWS WAF für Amazon API Gateway so, dass der Zugriff nur über das Netzwerk Ihrer Organisation möglich ist.
- Erwägen Sie andere Optionen für die API Gateway-Autorisierung, wenn IAM Ihre Anforderungen nicht erfüllt. Sie können beispielsweise Amazon Cognito-Benutzerpools oder API-Gateway-Lambda-Genehmiger verwenden.
- Verwenden Sie DynamoDB-Backups .
- Konfigurieren Sie Lambda-Funktionen mit einer Virtual Private Cloud (VPC)-Bereitstellung, um den Netzwerkverkehr innerhalb der Cloud zu halten.
- Aktualisieren Sie die zulässige Ursprungskonfiguration für CORS-Preflight (Cross-Origin Resource Sharing), um den Zugriff auf die anfordernde Ursprungsdomäne zu beschränken.
- Verwenden Sie cdk-nag, um den AWS-CDK-Code auf bewährte Sicherheitsmethoden zu überprüfen.
- Erwägen Sie, Code-Scan-Tools zu verwenden, um häufige Sicherheitsprobleme im Code zu finden. Bandit ist beispielsweise ein Tool, das darauf ausgelegt ist, häufige Sicherheitsprobleme im Python-Code zu finden. Pip-audit scannt Python-Umgebungen auf Pakete mit bekannten Schwachstellen.

Dieses Muster verwendet AWS X-Ray, um Anfragen über den Einstiegspunkt, die Domain und die Adapter der Anwendung nachzuverfolgen. AWS X-Ray hilft Entwicklern dabei, Engpässe zu identifizieren und hohe Latenzen zu ermitteln, um die Anwendungsleistung zu verbessern.

Polen

Initialisieren des Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihr eigenes Repository.	1. Melden Sie sich bei an GitHub. 2. Erstellen Sie ein neues Repository. Anweisungen finden Sie in der GitHub Dokumentation . 3. Klonen Sie das Beispiel-Repository für dieses	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Muster und übertragen Sie es in das neue Repository in Ihrem Konto.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Abhängigkeiten.	1. Installieren Sie Poetry.
	`pip install poetry`
	2. Installieren Sie Pakete aus dem Stammverzeichnis. Mit dem folgenden Befehl werden die Anwendung und AWS-CDK-Pakete installiert. Außerdem werden Entwicklungspakete installiert, die für die Ausführung von Einheitentests erforderlich sind. Alle installierten Pakete werden in einer neuen virtuellen Umgebung platziert.
	`poetry install`
	3. Führen Sie den folgenden Befehl aus, um eine grafische Darstellung der installierten Pakete anzuzeigen.
	`poetry show --tree`
	4. Aktualisieren Sie alle Abhängigkeiten.
	`poetry update`
	5. Öffnen Sie eine neue Shell in der neu erstellten virtuellen Umgebung. Sie enthält
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	alle installierten Abhängigkeiten. `poetry shell`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihre IDE.	Wir empfehlen Visual Studio Code, aber Sie können eine beliebige IDE Ihrer Wahl verwenden, die Python unterstützt. Die folgenden Schritte beziehen sich auf Visual Studio Code. 1. Aktualisieren Sie die `-.vscode/settings` Datei. `{ "python.testing.pytestArgs": [ "app/adapters/tests", "app/entrypoints/api/tests", "app/domain/tests" ], "python.testing.unittestEnabled": false, "python.testing.pytestEnabled": true, "python.envFile": "${workspaceFolder}/.env", }` 2. Erstellen Sie eine `-.env`Datei im Stammverzeichnis des Projekts. Dadurch wird sichergestellt, dass das Stammverz	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eichnis des Projekts in der enthalten ist, PYTHONPAT H damit es finden und alle Pakete ordnungsgemäß erkennen `pytest` kann. `PYTHONPATH=.`	
Führen Sie Einheitentests aus, Option 1: Visual Studio Code verwenden.	1. Wählen Sie den Python-Interpreter der virtuellen Umgebung aus, die von Poetry verwaltet wird. 2. Führen Sie Tests von Test Explorer aus.	App-Developer

Führen Sie Einheitentests aus, Option 2: Verwenden von Shell-Befehlen.	1. Starten Sie eine neue Shell in der virtuellen Umgebung.
	`poetry shell`
	2. Führen Sie den `pytest` Befehl aus dem Stammverz eichnis aus.
	`python -m pytest`
	Alternativ können Sie den Befehl auch direkt von Poetry aus ausführen.
	`poetry run python -m pytest`
		App-Developer

Bereitstellen und Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fordern Sie temporäre Anmeldeinformationen an.	Um AWS-Anmeldeinformationen auf der Shell zu haben, wenn Sie ausführen `cdk deploy`, erstellen Sie temporäre Anmeldeinformationen mithilfe von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On). Anweisungen finden Sie im Blogbeitrag So rufen Sie kurzfristige Anmeldeinformationen für die Verwendung mit AWS IAM Identity Center ab.	App-Entwickler, AWS DevOps

Stellen Sie die Anwendung bereit.	1. Installieren Sie AWS CDK v2.
	`npm install -g aws-cdk`
	Weitere Informationen finden Sie in der AWS-CDK-Dokumentation.
	2. Bootstrappen Sie das AWS-CDK in Ihr Konto und Ihre Region.
	`cdk bootstrap aws://12345678900/us-east-1 --profile aws-profile-name`
	3. Stellen Sie die Anwendung mithilfe eines AWS-Profils
		App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als AWS- CloudFormation Stack bereit. `cdk deploy --profile aws-profile-name`	
Testen Sie die API, Option 1: Verwenden Sie die -Konsole.	Verwenden Sie die API Gateway-Konsole, um die API zu testen. Weitere Informationen zu API-Operationen und Anforderungs-/Antwortnachrichten finden Sie im Abschnitt API-Nutzung der Readme-Datei im GitHub Repository.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die API, Option 2: Verwenden Sie Postman.	Wenn Sie ein Tool wie Postman verwenden möchten: 1. Installieren Sie Postman als eigenständige Anwendung oder Browsererweiterung. 2. Kopieren Sie die Endpunkt-URL für das API Gateway. Es wird das folgende Format haben. `https://{api-id}.execute-api.{region}.amazonaws.com/{stage}/{path}` 3. Konfigurieren Sie die AWS-Signatur auf der Registerkarte Autorisierung. Anweisungen finden Sie im AWS re:Post-Artikel zur Aktivierung der IAM-Authentifizierung für API Gateway-REST-APIs. 4. Verwenden Sie Postman, um Anfragen an Ihren API-Endpunkt zu senden.	App-Entwickler, AWS DevOps

Entwickeln des -Services

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie Einheitentests für die Geschäftsdomäne.	1. Erstellen Sie eine Python-Datei im `app/domain/`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`tests` Ordner mit dem `test_` Dateinamenpräfix .
	2. Erstellen Sie eine neue Testmethode, um die neue Geschäftslogik anhand des folgenden Beispiels zu testen.
	`def test_create_product_should_store_in_repository():`
	`    # Arrange`
	`    command = create_product_command.CreateProductCommand(`
	`        name="Test Product",`
	`        description="Test Description",`
	`    )`
	`    # Act`
	`    create_product_command_handler.handle_create_product_command(`
	`        command=command, unit_of_work=mock_unit_of_work`
	`    )`
	`# Assert`
	3. Erstellen Sie eine Befehlsklasse im `app/domain/commands` Ordner .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wenn die Funktionalität neu ist, erstellen Sie einen Stub für den Befehlshandler im `app/domain/command_handlers` Ordner . 5. Führen Sie den Komponententest aus, um zu sehen, dass er fehlschlägt, da immer noch keine Geschäftslogik vorhanden ist. `python -m pytest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Implementieren Sie Befehle und Befehlshandler.	1. Implementieren Sie die Geschäftslogik in der neu erstellten Befehlshandlerdatei.
	2. Deklarieren Sie für jede Abhängigkeit, die mit externen Systemen interagiert, eine abstrakte Klasse im `app/domain/ports` Ordner .
	
	`class ProductsRepository(ABC):`
	`  @abstractmethod`
	`  def add(self, product: product.Product) -> None:`
	`  ...`
	
	`class UnitOfWork(ABC):`
	`  products: ProductsRepository`
	
	`  @abstractmethod`
	`  def commit(self) -> None:`
	`  ...`
	
	`  @abstractmethod`
	`  def __enter__(self) -> typing.Any:`
	`  ...`
	
	`  @abstractmethod`
	`  def __exit__(self, *args) -> None:`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	...
	3. Aktualisieren Sie die Befehlshandlersignatur, um die neu deklarierten Abhängigkeiten zu akzeptieren, indem Sie die abstrakte Portklasse als Typanmerkung verwenden.
	`def handle_create_product_command(`
	`command: create_product_command.CreateProductCommand,`
	`unit_of_work: unit_of_work.UnitOfWork,`
	`) -> str:`
	`...`
	4. Aktualisieren Sie den Komponententest, um das Verhalten aller deklarierten Abhängigkeiten für den Befehlshandler zu simulieren.
	`# Arrange`
	`mock_unit_of_work = unittest.mock.create_autospec(`
	`spec=unit_of_work.UnitOfWork, instance=True`
	`)`
	`mock_unit_of_work.products =`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>unittest.mock.create_autospec(
	spec=unit_of_work.ProductsRepository, instance=True
	)</pre>
	5. Aktualisieren Sie die Assertion-Logik im Test, um nach den erwarteten Abhängigkeitsaufrufen zu suchen.
	<pre># Assert
	mock_unit_of_work.commit.assert_called_once()
	product = mock_unit_of_work.products.add.call_args.args[0]
	
	assertpy.assert_that(product.name).is_equal_to("Test Product")
	assertpy.assert_that(product.description).is_equal_to("Test Description")</pre>
	6. Führen Sie den Komponententest aus, um zu sehen, dass er erfolgreich war.
	<pre>python -m pytest</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie Integrationstests für sekundäre Adapter.	1. Erstellen Sie eine Testdatei im `app/adapters/tests` Ordner , indem Sie `test_` als Dateinamenpräfix verwenden. 2. Verwenden Sie die Moto-Bibliothek, um AWS-Services zu simulieren. 3. Erstellen Sie eine neue Testmethode für einen Integrationstest des Adapters.	App-Developer

```
@pytest.fixture
def mock_dynamodb():
   with moto.mock_dynamodb():
    yield boto3.resource("dynamodb", region_name="eu-central-1")
```

```
def test_add_and_commit_should_store_product(mock_dynamodb):
    # Arrange
    unit_of_work = dynamodb_unit_of_work.DynamoDBUnitOfWork(
        table_name=TEST_TABLE_NAME, dynamodb_client=mock_dynamodb.meta.client
    )
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
    current_time =
 datetime.datetime.
now(datetime.timez
one.utc).isoformat
()

    new_product_id =
 str(uuid.uuid4())
    new_product =
 product.Product(
        id=new_pr
oduct_id,
        name="test-
name",
        descripti
on="test-descripti
on",
        createDat
e=current_time,
        lastUpdat
eDate=current_time,
    )

    # Act
    with unit_of_w
ork:
        unit_of_w
ork.products.add(n
ew_product)
        unit_of_w
ork.commit()

    # Assert
```

4. Erstellen Sie eine Adapterklasse im `app/adapters` Ordner . Verwenden Sie die abstrakte Klasse aus dem Ports-Ordner als Basisklasse.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Führen Sie den Komponent entest aus, um zu sehen, dass er fehlschlägt, da immer noch keine Logik vorhanden ist. `python -m pytest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Implementieren Sie sekundäre Adapter.	1. Implementieren Sie Logik in der neu erstellten Adapterdatei.
	2. Aktualisieren Sie die Testzusicherungen.
	
	`# Assert`
	`    with unit_of_work_readonly:`
	`        product_from_db = unit_of_work_readonly.products.get(new_product_id)`
	
	`    assertpy.assert_that(product_from_db).is_not_none()`
	`    assertpy.assert_that(product_from_db.dict()).is_equal_to(`
	`        {`
	`            "id": new_product_id,`
	`            "name": "test-name",`
	`            "description": "test-description",`
	`            "createDate": current_time,`
	`            "lastUpdateDate": current_time,`
	`        }`
	`    )`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Führen Sie den Komponent entest aus, um zu sehen, dass er erfolgreich war. `python -m pytest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie end-to-end Tests.	1. Erstellen Sie eine Testdatei im `app/entrypoints/api/tests` Ordner , indem Sie `test_` als Dateinamenpräfix verwenden. 2. Erstellen Sie eine Lambda-Kontextumgebung, die vom Test zum Aufrufen von Lambda verwendet wird. 3. Erstellen Sie eine Testmethode für den API-Aufruf.	App-Developer

```
@pytest.fixture
def lambda_co
ntext():
    @dataclass
    class LambdaCon
text:
        function_
name: str = "test"
        memory_li
mit_in_mb: int = 128
        invoked_f
unction_arn: str =
 "arn:aws:lambda:eu
-west-1:809313241:
function:test"
        aws_reque
st_id: str =
 "52fdfc07-2182-154
f-163f-5f0f9a621d7
2"

 return LambdaCon
text()
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`def test_crea te_product(lambda_ context):`
	`    # Arrange`
	`    name = "TestName"`
	`    description =  "Test description"`
	`    request =  api_model.CreatePr oductRequest(name= name, descripti on=description)`
	
	`    minimal_event =  api_gateway_proxy_ event.APIGatewayPr oxyEvent(`
	`        {`
	`            "path": "/ products",`
	`            "httpMeth od": "POST",`
	`            "requestC ontext": {  #  correlation ID`
	
	`  "requestId":  "c6af9ac6-7b61-11e 6-9a41-93e8deadbee f"`
	`            },`
	`            "body":  json.dumps(request .dict()),`
	`        }`
	`    )`
	
	`    create_pr oduct_func_mock =  unittest.mock.crea te_autospec(`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>spec=crea
	te_product_command
	_handler.handle_cr
	eate_product_comma
	nd
	)
	handler.c
	reate_product_comm
	and_handler.handle
	_create_product_co
	mmand = (
	create_pr
	oduct_func_mock
	)
	
	# Act
	handler.h
	andler(minimal_eve
	nt, lambda_context)</pre>	

	4. Führen Sie den Komponententest aus, um zu sehen, dass er fehlschlägt, da immer noch keine Logik vorhanden ist. <pre>python -m pytest</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Implementieren Sie Primärada pter.	1. Erstellen Sie eine -Funktion für die API-Geschäftslogik und deklarieren Sie sie als API-Ressource.
	
	`@tracer.capture_me thod @app.post("/p roducts") @utils.parse_even t(model=api_model. CreateProductReque st, app_context=app) def create_product( request: api_model .CreateProductRequ est, ) -> api_model .CreateProductResp onse: """Creates a product.""" ...`
	
	Hinweis: Alle Decorator en, die Sie sehen, sind Features der AWS Lambda Powertools for Python-Bi bliothek. Weitere Informati onen finden Sie auf der AWS Lambda Powertools for Python-Website.
	2. Implementieren Sie die API-Logik.
	
	`id=create_product_ command_handler.ha`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>ndle_create_produc
	t_command(
	        command=c
	reate_product_comm
	and.CreateProductC
	ommand(
	            name=requ
	est.name,
	            descripti
	on=request.descrip
	tion,
	        ),
	        unit_of_w
	ork=unit_of_work,
	    )
	    response =
	 api_model.CreatePr
	oductResponse(id=i
	d)
	    return response.
	dict()</pre> 3. Führen Sie den Komponententest aus, um zu sehen, dass er erfolgreich war.
	<pre>python -m pytest</pre>	

Zugehörige Ressourcen

APG-Leitfaden

- Erstellen hexhexhexhexhexhexhexhexhex-Architekturen in AWS

AWS-Referenzen

- AWS Lambda-Dokumentation
- AWS-CDK-Dokumentation

  - Ihre erste AWS-CDK-App
- API Gateway-Dokumentation
  - Steuern des Zugriffs auf eine API mit IAM-Berechtigungen
  - Verwenden der API Gateway-Konsole zum Testen einer REST-API-Methode
- Amazon-DynamoDB-Dokumentation

Tools

- git-scm.com-Website
- Installieren von Git
- Erstellen eines neuen GitHub Repositorys
- Python-Website
- AWS Lambda Powertools für Python
- Postman-Website
- Python-Mock-Objektbibliothek
- Geoetry-Website

IDEs

- Visual-Studio-Code-Website
- AWS Cloud9-Dokumentation
- PyCharm Website

Mehr Muster

- Automatisieren der Stack-Set-Bereitstellung mithilfe von AWS CodePipeline und AWS CodeBuild
- Automatisches Anfügen einer von AWS verwalteten Richtlinie für Systems Manager an EC2-Instance-Profile mithilfe von Cloud Custodian und AWS CDK
- Erstellen einer Videoverarbeitungs-Pipeline mithilfe von Amazon Kinesis Video Streams und AWS Fargate
- Verketten von AWS-Services mithilfe eines Serverless-Ansatzes
- Konvertieren des Datentyps VARCHAR2(1) für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Bereitstellen einer geclusterten Anwendung in Amazon ECS mithilfe von AWS Copilot
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Bereitstellen von Lambda-Funktionen mit Container-Images
- Generieren Sie eine statische ausgehende IP-Adresse mithilfe einer Lambda-Funktion, Amazon VPC und einer serverlosen Architektur
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Implementieren einer Gitflow-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten
- Implementieren einer GitHub Flow-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten
- Implementierung einer Trunk-Verzweigungsstrategie für DevOps Umgebungen mit mehreren Konten
- Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS
- Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 EC2-Linux-Instance aus
- Führen Sie Komponententests für Python-ETL-Jobs in AWS Glue mithilfe des Pytest-Frameworks aus
- Übertragen Sie umfangreiche Db2-z/OS-Daten in CSV-Dateien an Amazon S3
- Lokales Validieren des Codes Account Factory für Terraform (AFT)

Speicher und Backup

Themen

EC2-Instances Schreibzugriff auf S3-Buckets in AMS-Konten gewähren

Erstellt von Mansi Suratwala (AWS)

Umgebung: Produktion	Technologien: Speicher und Backup; Datenbanken; Sicherheit, Identität, Compliance; Betrieb	Workload: Alle anderen Workloads
AWS-Services: Amazon S3; AWS Managed Services		

Übersicht

AWS Managed Services (AMS) hilft Ihnen, Ihre Amazon Web Services (AWS)-Infrastruktur effizienter und sicher zu betreiben. AMS-Konten verfügen über Sicherheitsvorkehrungen für die standardisierte Verwaltung Ihrer AWS-Ressourcen. Ein Integritätsschutz besteht darin, dass standardmäßige Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Profile keinen Schreibzugriff auf Amazon Simple Storage Service (Amazon S3)-Buckets zulassen. Ihre Organisation verfügt jedoch möglicherweise über mehrere S3-Buckets und benötigt mehr Kontrolle über den Zugriff durch EC2-Instances. Sie können beispielsweise Datenbank-Backups von EC2-Instances in einem S3-Bucket speichern.

Dieses Muster erklärt, wie Sie Requests for Change (RFCs) verwenden, um Ihren EC2-Instances Schreibzugriff auf S3-Buckets in Ihrem AMS-Konto zu ermöglichen. Ein RFC ist eine Anforderung, die von Ihnen oder AMS erstellt wurde, um eine Änderung in Ihrer verwalteten Umgebung vorzunehmen, und die eine Änderungstyp-ID (CT) für eine bestimmte Operation enthält.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AMS-Advanced-Konto. Weitere Informationen dazu finden Sie unter AMS-Betriebspläne in der AWS Managed Services-Dokumentation.

- Zugriff auf die customer-mc-user-role AWS Identity and Access Management (IAM)-Rolle zum Senden von RFCs.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert mit den EC2-Instances in Ihrem AMS-Konto.
- Ein Verständnis dafür, wie RFCs in AMS erstellt und übermittelt werden. Weitere Informationen dazu finden Sie unter Was sind AMS-Änderungstypen? in der AWS Managed Services-Dokumentation.
- Ein Verständnis der manuellen und automatisierten Änderungstypen (CTs). Weitere Informationen dazu finden Sie unter Automatisierte und manuelle CTs in der AWS Managed Services-Dokumentation.

Architektur

Technologie-Stack

- AMS
- AWS CLI
- Amazon EC2
- Amazon S3
- IAM

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer für ihre Nutzung authentifiziert und autorisiert ist.
- AWS Managed Services (AMS) hilft Ihnen, Ihre AWS-Infrastruktur effizienter und sicherer zu betreiben.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

Polen

Erstellen eines S3-Buckets mit einem RFC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket mit einem automatisierten RFC.	1. Melden Sie sich bei Ihrem AMS-Konto an, wählen Sie die Seite Änderungstyp auswählen, wählen Sie RFCs und dann RFC erstellen aus. 2. Senden Sie das automatisierte RFC zum Erstellen eines S3-Buckets. Hinweis: Stellen Sie sicher, dass Sie den Namen des S3-Buckets aufzeichnen.	AWS-Systemadministrator, AWS-Entwickler

Erstellen Sie ein IAM-Instance-Profil und verknüpfen Sie es mit den EC2-Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie ein manuelles RFC, um eine IAM-Rolle zu erstellen.	Wenn ein AMS-Konto eingegliedert wird, wird ein standardmäßiges customer-mc-ec2-Instance-Profil-IAM-Instance-Profil erstellt und jeder EC2-Instance in Ihrem AMS-Konto zugeordnet. Das Instance-Profil verfügt jedoch nicht über Schreibberechtigungen für Ihre S3-Buckets.	AWS-Systemadministrator, AWS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um die Schreibberechtigungen hinzuzufügen, senden Sie das Handbuch IAM-Resource erstellen RFC, um eine IAM-Rolle zu erstellen, die die folgenden drei Richtlinien hat: customer_ec2_instance_, customer_deny_policy und customer_ec2_s3_integration_policy. Wichtig: Die Richtlinien customer_ec2_instance_ und customer_deny_policy sind bereits in Ihrem AMS-Konto vorhanden. Sie müssen jedoch die Richtlinie customer_ec2_s3_integration_policy mithilfe der folgenden Beispielrichtlinie erstellen: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "", "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Role Permissions:
	{
	"Version":
	"2012-10-17",
	"Statement": [
	{
	"Action": [
	"s3:ListBucket",
	"s3:GetBucketLocation"
	],
	"Resource": "arn:aws:s3:::",
	"Effect":
	"Allow"
	},
	{
	"Action": [
	"s3:GetObject",
	"s3:PutObject",
	"s3:ListMultipartUploadParts",
	"s3:AbortMultipartUpload"
	],
	"Resource": "arn:aws:s3:::/*",
	"Effect":
	"Allow"
	}
	]
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie ein manuelles RFC, um das IAM-Instance-Profil zu ersetzen.	Senden Sie ein manuelles RFC, um die EC2-Ziel-Instances dem neuen IAM-Instance-Profil zuzuordnen.	AWS-Systemadministrator, AWS-Entwickler
Testen Sie einen Kopiervor gang in den S3-Bucket.	Testen Sie einen Kopiervor gang in den S3-Bucket, indem Sie den folgenden Befehl in der AWS CLI ausführen: `aws s3 cp test.txt s3://<S3 Bucket>/test2.txt`	AWS-Systemadministrator, AWS-Entwickler

Zugehörige Ressourcen

- Erstellen eines IAM-Instance-Profils für Ihre Amazon EC2-Instances
- Erstellen eines S3-Buckets (mit der Amazon S3-Konsole, AWS SDKs oder AWS CLI)

Automatisieren der Datenstromaufnahme in eine Snowflake-Datenbank mithilfe von Snowflake Snowpipe, Amazon S3, Amazon SNS und Amazon Data Firehose

Erstellt von Bikash Chandra Rout (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Speicher und Backup

Übersicht

Dieses Muster beschreibt, wie Sie Services in der Amazon Web Services (AWS) Cloud verwenden können, um einen kontinuierlichen Datenstrom zu verarbeiten und ihn in eine Snowflake-Datenbank zu laden. Das Muster verwendet Amazon Data Firehose, um die Daten an Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) zu senden, um Benachrichtigungen zu senden, wenn neue Daten empfangen werden, und Snowflake Snowpipe, um die Daten in eine Snowflake-Datenbank zu laden.

Wenn Sie diesem Muster folgen, können Sie kontinuierlich generierte Daten innerhalb von Sekunden zur Analyse zur Verfügung stellen, mehrere manuelle COPY-Befehle vermeiden und beim Laden volle Unterstützung für halbstrukturierte Daten bieten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Datenquelle, die kontinuierlich Daten an einen Firehose-Bereitstellungs-Stream sendet.
- Ein vorhandener S3-Bucket, der die Daten aus dem Firehose-Bereitstellungs-Stream empfängt.
- Ein aktives Snowflake-Konto.

Einschränkungen

- Snowflake Snowpipe stellt keine direkte Verbindung zu Firehose her.

Architektur

Technologie-Stack

- Amazon Data Firehose
- Amazon SNS
- Amazon S3
- Snowflake Snowpipe
- Snowflake-Datenbank

Tools

- Firehose – Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Echtzeit-Streaming-Daten an Ziele wie Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk und alle benutzerdefinierten HTTP-Endpunkte oder HTTP-Endpunkte, die unterstützten Drittanbietern gehören.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder das Senden von Nachrichten an abonnierende Endpunkte oder Clients.
- Snowflake – Snowflake ist ein analytisches Data Warehouse, das als Software-as-a-Service (SaaS) bereitgestellt wird.
- Snowflake Snowpipe – Snowpipe lädt Daten aus Dateien, sobald sie in einer Snowflake-Phase verfügbar sind.

Sekunden

Einrichten einer Snowflake Snowpipe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CSV-Datei in Snowflake.	Melden Sie sich bei Snowflake an und führen Sie den Befehl „CREATE FILE FORMAT“	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus, um eine CSV-Datei mit einem angegebenen Feldtrenn zeichen zu erstellen. Weitere Informationen zu diesem und anderen Snowflake-Befehlen finden Sie im Abschnitt „Zusätzliche Informationen“.	
Erstellen Sie eine externe Snowflake-Stufe.	Führen Sie den Befehl „CREATE STAGE“ aus, um eine externe Snowflake-Stufe zu erstellen, die auf die zuvor erstellte CSV-Datei verweist. Wichtig: Sie benötigen die URL für den S3-Bucket, Ihren AWS-Zugriffsschlüssel und Ihren geheimen AWS-Zugri ffsschlüssel. Führen Sie den Befehl „SHOW STAGES“ aus, um zu überprüfen, ob die Snowflake-Phase erstellt wurde.	Developer
Erstellen Sie die Snowflake-Zieltabelle.	Führen Sie den Befehl „CREATE TABLE“ aus, um die Snowflake-Tabelle zu erstellen .	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipe.	Führen Sie den Befehl „CREATE PIPE“ aus. Stellen Sie sicher, dass „auto_ing est=true“ im Befehl ist. Führen Sie den Befehl „SHOW PIPES“ aus, um zu überprüfe n, ob die Pipe erstellt wurde. Kopieren Sie den Spaltenwe rt „notification_channel“ und speichern Sie ihn. Dieser Wert wird verwendet, um Amazon S3-Ereignisbenachrichtigung en zu konfigurieren.	Developer

Konfigurieren des S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine 30-tägige Lebenszyklusrichtlinie für den S3-Bucket.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3-Konsole. Wählen Sie den S3-Bucket aus, der die Daten aus Firehose enthält. Wählen Sie dann im S3-Bucket die Registerkarte „Management“ und dann „Lebenszyklusregel hinzufügen“. Geben Sie im Dialogfeld „Lebenszyklusregel “ einen Namen für Ihre Regel ein und konfigurieren Sie eine 30-tägige Lebenszyklusregel für Ihren Bucket. Hilfe zu dieser und anderen Artikeln	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie im Abschnitt „Verwandte Ressourcen“.	
Erstellen Sie eine IAM-Richtlinie für den S3-Bucket.	Öffnen Sie die AWS Identity and Access Management (IAM)-Konsole und wählen Sie „Richtlinien“. Wählen Sie „Richtlinie erstellen“ und dann die Registerkarte „JSON“. Kopieren Sie die Richtlinie aus dem Abschnitt „Zusätzliche Informationen“ und fügen Sie sie in das JSON-Feld ein. Diese Richtlinie gewährt „PutObject“- und „DeleteObject“-Berechtigungen sowie „GetObject“- GetObject Versionund „ListBucket“-Berechtigungen. Wählen Sie „Richtlinie überprüfen“, geben Sie einen Richtliniennamen ein und wählen Sie dann „Richtlinie erstellen“.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie die Richtlinie einer IAM-Rolle zu.	Öffnen Sie die IAM-Konsole und wählen Sie dann „Rollen“ und dann „Rolle erstellen“ aus. Wählen Sie „Ein anderes AWS-Konto“ als vertrauen swürdige Entität aus. Geben Sie Ihre AWS-Konto-ID ein und wählen Sie „Externe ID erforderlich“. Geben Sie eine Platzhalter-ID ein, die Sie später ändern werden. Wählen Sie „Nächste“ und weisen Sie die zuvor erstellte IAM-Richt linie zu. Erstellen Sie dann die IAM-Rolle.	Systemadministrator, Entwickler
Kopieren Sie den Amazon-Re ssourcennamen (ARN) für die IAM-Rolle.	Öffnen Sie die IAM-Konso le und wählen Sie „Rollen“. Wählen Sie die IAM-Rolle aus, die Sie zuvor erstellt haben, und kopieren und speichern Sie dann den „Rollen-ARN“.	Systemadministrator, Entwickler

Einrichten einer Speicherintegration in Snowflake

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Speicheri ntegration in Snowflake.	Melden Sie sich bei Snowflake an und führen Sie den Befehl „CREATE STORAGE INTEGRATION“ aus. Dadurch wird die Vertrauen sstellung geändert, Zugriff auf Snowflake gewährt und die	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	externe ID für Ihre Snowflake-Stufe angegeben.	
Rufen Sie die IAM-Rolle für Ihr Snowflake-Konto ab.	Führen Sie den Befehl „DESC INTEGRATION“ aus, um den ARN für die IAM-Rolle abzurufen. Wichtig: <integration_name> ist der Name der Snowflake-Speicherintegration, die Sie zuvor erstellt haben.	Systemadministrator, Entwickler
Notieren Sie zwei Spaltenwerte.	Kopieren und speichern Sie die Werte für die Spalten „storage_aws_iam_user_arn“ und „storage_aws_external_id“.	Systemadministrator, Entwickler

Snowflake Snowpipe den Zugriff auf den S3-Bucket erlauben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die IAM-Rollenrichtlinie.	Öffnen Sie die IAM-Konsole und wählen Sie „Rollen“. Wählen Sie die IAM-Rolle aus, die Sie zuvor erstellt haben, und wählen Sie die Registerkarte „Vertrauensstellungen“. Wählen Sie „Vertrauensstellung bearbeiten“. Ersetzen Sie „snowflake_external_id“ durch den Wert „storage_aws_external_id“, den Sie zuvor kopiert haben. Ersetzen Sie „snowflake_user_arn“ durch den Wert	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	storage_aws_iam_user_arn, den Sie zuvor kopiert haben. Wählen Sie dann „Vertraue nsrichtlinie aktualisieren“.	

Aktivieren und Konfigurieren von SNS-Benachrichtigungen für den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Ereignisb enachrichtigungen für den S3-Bucket.	Öffnen Sie die Amazon S3-Konsole und wählen Sie Ihren Bucket aus. Wählen Sie „Eigenschaften“ und unter „Erweiterte Einstellu ngen“ „Ereignisse“ aus. Wählen Sie „Benachrichtigung hinzufügen“ und geben Sie einen Namen für dieses Ereignis ein. Wenn Sie keinen Namen eingeben, wird eine global eindeutige Kennung (GUID) verwendet.	Systemadministrator, Entwickler
Konfigurieren Sie Amazon SNS-Benachrichtigungen für den S3-Bucket.	Wählen Sie unter „Ereignis se“ die Option „ObjectCr eate (Alle)“ und dann in der Dropdownliste „SQS-Wart eschlange“ aus. Wählen Sie in der Liste „SNS“ die Option „SQS-Warteschlangen-ARN hinzufügen“ aus und fügen Sie den zuvor kopierten Wert „notification_channel“ ein. Wählen Sie dann „Speichern“.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie die Snowflake-SQS-Warteschlange für das SNS-Thema.	Abonnieren Sie die Snowflake-SQS-Warteschlange für das von Ihnen erstellte SNS-Thema. Hilfe zu diesem Schritt finden Sie im Abschnitt „Verwandte Ressourcen“.	Systemadministrator, Entwickler

Überprüfen der Snowflake-Stufenintegration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und testen Sie Snowpipe.	Melden Sie sich bei Snowflake an und öffnen Sie die Snowflake-Phase. Löschen Sie Dateien in Ihren S3-Bucket und überprüfen Sie, ob die Snowflake-Tabelle sie lädt. Amazon S3 sendet SNS-Benachrichtigungen an Snowpipe, wenn neue Objekte im S3-Bucket angezeigt werden.	Systemadministrator, Entwickler

Zugehörige Ressourcen

- Erstellen einer Lebenszyklusrichtlinie für einen S3-Bucket
- Abonnieren der Snowflake-SQS-Warteschlange für das Amazon SNS-Thema

Zusätzliche Informationen

Erstellen Sie ein Dateiformat:

```
CREATE FILE FORMAT <name>
```

```
TYPE = 'CSV'
FIELD_DELIMITER = '|'
SKIP_HEADER = 1;
```

Erstellen Sie eine externe Stufe:

```
externalStageParams (for Amazon S3) ::=
  URL = 's3://[//]'

  [ { STORAGE_INTEGRATION =  } | { CREDENTIALS = ( {  { AWS_KEY_ID = `` AWS_SECRET_KEY
 = `` [ AWS_TOKEN = `` ] } | AWS_ROLE = ``  } ) ) }` ]
  [ ENCRYPTION = ( [ TYPE = 'AWS_CSE' ] [ MASTER_KEY = '' ] |
                   [ TYPE = 'AWS_SSE_S3' ] |
                   [ TYPE = 'AWS_SSE_KMS' [ KMS_KEY_ID = '' ] |
                   [ TYPE = NONE ] )
```

Erstellen einer Tabelle:

```
CREATE [ OR REPLACE ] [ { [ LOCAL | GLOBAL ] TEMP[ORARY] | VOLATILE } | TRANSIENT ]
 TABLE [ IF NOT EXISTS ]
  <table_name>
    ( <col_name> <col_type> [ { DEFAULT <expr>
                              | { AUTOINCREMENT | IDENTITY } [ ( <start_num> ,
 <step_num> ) | START <num> INCREMENT <num> ] } ]
                               /* AUTOINCREMENT / IDENTITY supported only for numeric
 data types (NUMBER, INT, etc.) */
                            [ inlineConstraint ]
      [ , <col_name> <col_type> ... ]
      [ , outoflineConstraint ]
      [ , ... ] )
  [ CLUSTER BY ( <expr> [ , <expr> , ... ] ) ]
  [ STAGE_FILE_FORMAT = ( { FORMAT_NAME = '<file_format_name>'
                          | TYPE = { CSV | JSON | AVRO | ORC | PARQUET | XML }
 [ formatTypeOptions ] } ) ]
  [ STAGE_COPY_OPTIONS = ( copyOptions ) ]
  [ DATA_RETENTION_TIME_IN_DAYS = <num> ]
  [ COPY GRANTS ]
  [ COMMENT = '<string_literal>' ]
```

Phasen anzeigen:

```
SHOW STAGES;
```

Erstellen Sie eine Pipe:

```
CREATE [ OR REPLACE ] PIPE [ IF NOT EXISTS ]
  [ AUTO_INGEST = [ TRUE | FALSE ] ]
  [ AWS_SNS_TOPIC =  ]
  [ INTEGRATION = '' ]
  [ COMMENT = '' ]
  AS
```

Pipes anzeigen:

```
SHOW PIPES [ LIKE '<pattern>' ]
           [ IN { ACCOUNT | [ DATABASE ] <db_name> | [ SCHEMA ] <schema_name> } ]
```

Erstellen einer Speicherintegration:

```
CREATE STORAGE INTEGRATION <integration_name>
  TYPE = EXTERNAL_STAGE
  STORAGE_PROVIDER = S3
  ENABLED = TRUE
  STORAGE_AWS_ROLE_ARN = '<iam_role>'
  STORAGE_ALLOWED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/')
  [ STORAGE_BLOCKED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/') ]
```

Beispiel:

```
create storage integration s3_int
  type = external_stage
  storage_provider = s3
  enabled = true
  storage_aws_role_arn = 'arn:aws:iam::001234567890:role/myrole'
  storage_allowed_locations = ('s3://mybucket1/mypath1/', 's3://mybucket2/mypath2/')
  storage_blocked_locations = ('s3://mybucket1/mypath1/sensitivedata/', 's3://
mybucket2/mypath2/sensitivedata/');
```

Weitere Informationen zu diesem Schritt finden Sie unter Konfigurieren einer Snowflake-Speicherintegration für den Zugriff auf Amazon S3 in der Snowflake-Dokumentation.

Beschreiben einer Integration:

```
DESC INTEGRATION <integration_name>;
```

S3-Bucket-Richtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetObjectVersion",
              "s3:DeleteObject",
              "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "/*"
                    ]
                }
            }
        }
    ]
}
```

Automatisches Verschlüsseln vorhandener und neuer Amazon-EBS-Volumes

Erstellt von Tony DeMarco (AWS) und Josh Joy (AWS)

Code-Repository: https://github.com/aws-samples/aws-system-manager-automation-unencrypted-to-encrypted-resources/tree/main/ebs	Umgebung: Produktion	Technologien: Speicher und Backup; Sicherheit, Identität, Compliance; Management und Governance
AWS-Services: AWS Config; Amazon EBS; AWS KMS; AWS Organizations ;AWS Systems Manager		

Übersicht

Die Verschlüsselung von Amazon Elastic Block Store (Amazon EBS)-Volumes ist für die Datenschutzstrategie einer Organisation wichtig. Es ist ein wichtiger Schritt beim Aufbau einer gut strukturierten Umgebung. Obwohl es keine direkte Möglichkeit gibt, vorhandene unverschlüsselte EBS-Volumes oder Snapshots zu verschlüsseln, können Sie sie verschlüsseln, indem Sie ein neues Volume oder einen neuen Snapshot erstellen. Weitere Informationen finden Sie unter Verschlüsseln von EBS-Ressourcen in der Amazon EC2Dokumentation. Dieses Muster bietet präventive und detektivische Kontrollen für die Verschlüsselung Ihrer neuen und vorhandenen EBS-Volumes. In diesem Muster konfigurieren Sie Kontoeinstellungen, erstellen automatisierte Korrekturprozesse und implementieren Zugriffskontrollen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS)-Konto
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert unter macOS , Linux oder Windows
- jq , installiert und konfiguriert unter macOS , Linux oder Windows

- AWS Identity and Access Management (IAM)-Berechtigungen werden bereitgestellt, um Lese- und Schreibzugriff auf AWS CloudFormation, Amazon Elastic Compute Cloud (Amazon EC2), AWS Systems Manager , AWS Config und AWS Key Management Service (AWS KMS) zu haben.
- AWS Organizations ist mit allen aktivierten Funktionen konfiguriert, eine Anforderung für Service-Kontrollrichtlinien
- AWS Config ist in den Zielkonten aktiviert

Einschränkungen

- In Ihrem AWS-Zielkonto darf es keine AWS Config-Regeln mit dem Namen encrypted-volumes geben. Diese Lösung stellt eine Regel mit diesem Namen bereit. Vorhandene Regeln mit diesem Namen können dazu führen, dass die Bereitstellung fehlschlägt und zu unnötigen Gebühren im Zusammenhang mit der mehrmaligen Verarbeitung derselben Regel führt.
- Diese Lösung verschlüsselt alle EBS-Volumes mit demselben AWS KMS-Schlüssel.
- Wenn Sie die Verschlüsselung von EBS-Volumes für das Konto aktivieren, ist diese Einstellung regionsspezifisch. Wenn Sie es für eine AWS-Region aktivieren, können Sie es nicht für einzelne Volumes oder Snapshots in dieser Region deaktivieren. Weitere Informationen finden Sie unter Standardmäßige Verschlüsselung in der Amazon EC2Dokumentation.
- Wenn Sie vorhandene, unverschlüsselte EBS-Volumes korrigieren, stellen Sie sicher, dass die EC2-Instance nicht verwendet wird. Diese Automatisierung fährt die Instance herunter, um das unverschlüsselte Volume zu trennen und das verschlüsselte anzuhängen. Während der Behebung kommt es zu Ausfallzeiten. Wenn dies ein entscheidender Bestandteil der Infrastruktur für Ihre Organisation ist, stellen Sie sicher, dass manuelle oder automatische Hochverfügbarkeitskonfigurationen vorhanden sind, um die Verfügbarkeit von Anwendungen, die auf der Instance ausgeführt werden, nicht zu beeinträchtigen. Wir empfehlen, kritische Ressourcen nur während Standardwartungsfenstern zu korrigieren.

Architektur

Automation-Workflow

1. AWS Config erkennt ein unverschlüsseltes EBS-Volume.
2. Ein Administrator verwendet AWS Config, um einen Korrekturbefehl an Systems Manager zu senden.

3. Die Systems Manager-Automatisierung erstellt einen Snapshot des unverschlüsselten EBS-Volumes.
4. Die Systems Manager-Automatisierung verwendet AWS KMS, um eine verschlüsselte Kopie des Snapshots zu erstellen.
5. Die Systems Manager-Automatisierung führt Folgendes aus:
   a. Stoppt die betroffene EC2-Instance, wenn sie ausgeführt wird
   b. Fügt die neue, verschlüsselte Kopie des Volumes an die EC2-Instance an
   c. Setzt die EC2-Instance in den ursprünglichen Zustand zurück

Tools

AWS-Services

- AWS CLI – Die AWS Command Line Interface (AWS CLI) bietet direkten Zugriff auf die öffentlichen Anwendungsprogrammierschnittstellen (APIs) von AWS-Services. Sie können die Funktionen eines Services mit der AWS CLI erkunden und Shell-Skripts zur Verwaltung Ihrer Ressourcen entwickeln. Zusätzlich zu den Low-Level-API-Befehlen bieten mehrere AWS-Services Anpassungen für die AWS CLI. Anpassungen können Befehle auf einer höheren Ebene enthalten, die die Verwendung eines Services durch eine komplexe API vereinfachen.
- AWS CloudFormation – AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt. Sie erstellen eine Vorlage, die alle gewünschten AWS-Ressourcen beschreibt (z. B. Amazon EC2-Instances) und diese Ressourcen für Sie CloudFormation bereitstellt und konfiguriert.
- AWS Config – AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.
- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der anpassbare Rechenkapazität bereitstellt, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- AWS KMS – AWS Key Management Service (AWS KMS) ist ein Verschlüsselungs- und Schlüsselverwaltungsservice, der für die Cloud skaliert ist. AWS KMS-Schlüssel und -Funktionalität werden von anderen AWS-Services verwendet und Sie können sie zum Schutz von Daten in Ihrer AWS-Umgebung verwenden.
- AWS Organizations – AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

- AWS Systems Manager Automation – Systems Manager Automation vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben für Amazon EC2-Instances und andere AWS-Ressourcen.

Andere -Services

- jq – jq ist ein einfacher und flexibler Befehlszeilen-JSON-Prozessor. Sie verwenden dieses Tool, um Schlüsselinformationen aus der AWS CLI-Ausgabe zu extrahieren.

Code

- Der Code für dieses Muster ist im Repository GitHub Automatische Behebung unverschlüsselter EBS-Volumes mithilfe von Kunden-KMS-Schlüsseln verfügbar.

Polen

Automatisieren der Behebung unverschlüsselter Volumes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Skripts und CloudFormation Vorlagen herunter.	Laden Sie das Shell-Skript, die JSON-Datei und die CloudFormation Vorlagen aus dem Repository GitHub Automatische Korrektur unverschlüsselter EBS-Volumes mithilfe von Kunden-KMS-Schlüsseln herunter.	AWS-Administrator, Allgemeines AWS
Identifizieren Sie den Administrator für den AWS KMS-Schlüssel.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/. 2. Identifizieren Sie einen Benutzer oder eine Rolle, der/die der AWS KMS-	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schlüsseladministrator sein soll. Wenn zu diesem Zweck ein neuer Benutzer oder eine neue Rolle erstellt werden muss, erstellen Sie sie jetzt. Weitere Informationen finden Sie unter IAM-Identitäten in der IAM-Dokumentation. Diese Automatisierung erstellt einen neuen AWS KMS-Schlüssel. 3. Kopieren Sie nach der Identifizierung den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle. Weitere Informationen finden Sie unter IAM-ARNs in der IAM-Dokumentation. Sie verwenden diesen ARN im nächsten Schritt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Stack1 CloudFormation template bereit.	1. Öffnen Sie die AWS-CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Stellen Sie die `Stack1.yaml` Vorlage in CloudFormationbereit. Beachten Sie die folgenden Bereitstellungsdetails: • Geben Sie dem Stack einen eindeutigen und beschreibenden Namen. Notieren Sie sich den Stack-Namen, da Sie diesen Wert im nächsten Schritt benötigen. • Fügen Sie den ARN des Schlüsseladministrators in das einzige Parameterfeld in Stack1 ein. Dieser Benutzer oder diese Rolle wird der Administrator für den AWS KMS-Schlüssel, der vom Stack erstellt wurde. Weitere Informationen zum Bereitstellen einer CloudFormation Vorlage finden Sie unter Arbeiten mit AWS-CloudFormation Vorlagen	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der - CloudFormation Dokumentation.	
Stellen Sie die Stack2 CloudFormation -Vorlage bereit.	Stellen Sie die `Stack2.yaml` Vorlage in CloudFormationbereit. Beachten Sie die folgenden Bereitstellungsdetails: • Geben Sie dem Stack einen eindeutigen und beschreibenden Namen. • Geben Sie für den einzigen Parameter von Stack2 den Namen des Stacks ein, den Sie im vorherigen Schritt erstellt haben. Auf diese Weise kann Stack2 auf den neuen AWS KMS-Schlüssel und die Rolle verweisen, die im vorherigen Schritt vom Stack bereitgestellt wurden.	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein unverschlüsseltes Volume zum Testen.	Erstellen Sie eine EC2-Instance mit einem unverschlüsselten EBS-Volume. Anweisungen finden Sie unter Erstellen eines Amazon-EBS-Volumes in der Amazon EC2Dokumentation. Der Instance-Typ spielt keine Rolle und der Zugriff auf die Instance ist nicht erforderlich. Sie können eine t2.micro-Instance erstellen, um im kostenlosen Kontingent zu bleiben, und Sie müssen kein Schlüsselpaar erstellen.	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die AWS Config-Regel.	1. Öffnen Sie die AWS Config-Konsole unter https://console.aws.amazon.com/config/. Wählen Sie auf der Seite Regeln die Regel für verschlüsselte Volumes aus. 2. Vergewissern Sie sich, dass Ihre neue, unverschlüsselte Test-Instance in der Liste der nicht konformen Ressourcen angezeigt wird. Wenn das Volume nicht sofort angezeigt wird, warten Sie einige Minuten und aktualisieren Sie die Ergebnisse. Die AWS Config-Regel erkennt die Ressourcenänderungen kurz nach der Erstellung der Instance und des Volumes. 3. Wählen Sie die Ressource aus und klicken Sie dann auf Remediate. Sie können den Korrektur fortschritt und den Status in Systems Manager wie folgt anzeigen: 1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.a	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ws.amazon.com/systems-manager/. 2. Klicken Sie im Navigatio nsbereich auf Automation. 3. Wählen Sie den Link Ausführungs-ID, um die Schritte und den Status anzuzeigen.	
Konfigurieren Sie zusätzliche Konten oder AWS-Regionen.	Wiederholen Sie dieses Epic nach Bedarf für alle zusätzlic hen Konten oder AWS-Regio nen.	AWS-Administrator, Allgemein es AWS

Aktivieren der Verschlüsselung von EBS-Volumes auf Kontoebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Aktivieru ngsskript aus.	1. Verwenden Sie in einer Bash-Shell den `cd`Befehl , um in das geklonte Repository zu navigieren. 2. Geben Sie den folgenden Befehl ein, um das `enable-ebs-encrypt ion-for-account -` Skript auszuführen. `./Bash/enable-ebs-encryption-for-acc ount.sh`	AWS-Administrator, Allgemein es AWS, Bash

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie, dass die Einstellungen aktualisiert wurden.	1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. 2. Wählen Sie auf der rechten Seite des Bildschirms unter Einstellungen die Option Datenschutz und Sicherheit aus. 3. Vergewissern Sie sich im Abschnitt EBS-Verschlüsselung, dass Neue EBS-Volumes immer verschlüsseln aktiviert ist und dass der Standardverschlüsselungsschlüssel auf den zuvor angegebenen ARN festgelegt ist. Hinweis: Wenn die Einstellung Neue EBS-Volumes immer verschlüsseln deaktiviert ist oder der Schlüssel immer noch auf alias/aws/ebs gesetzt ist, vergewissern Sie sich, dass Sie bei demselben Konto und derselben AWS-Region angemeldet sind, in der Sie das Shell-Skript ausgeführt haben, und überprüfen Sie Ihre Shell auf Fehlermeldungen.	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie zusätzliche Konten oder AWS-Regionen.	Wiederholen Sie dieses Epic nach Bedarf für alle zusätzlichen Konten oder AWS-Regionen.	AWS-Administrator, Allgemeines AWS

Verhindern der Erstellung unverschlüsselter Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Service-Kontrollrichtlinie.	1. Öffnen Sie die AWS Organizations-Konsole unter https://console.aws.amazon.com/organizations/v2/. 2. Erstellen Sie eine neue Service-Kontrollrichtlinie. Weitere Informationen finden Sie unter Erstellen einer Service-Kontrollrichtlinie in der AWS Organizations-Dokumentation. 3. Fügen Sie der Richtlinie den Inhalt von `DenyUnencryptedEC2.json` hinzu und speichern Sie ihn. Sie haben diese JSON-Datei aus dem GitHub Repository im ersten Epos heruntergeladen. 4. Fügen Sie diese Richtlinie dem Organisationsstamm oder allen erforderlichen	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Organisationseinheiten (OUs) an. Weitere Informationen finden Sie unter Anfügen und Trennen von Service-Kontrollrichtlinien in der AWS Organizations-Dokumentation.	

Zugehörige Ressourcen

AWS-Servicedokumentation

- AWS-CLI
- AWS Config
- AWS CloudFormation
- Amazon EC2
- AWS KMS
- AWS Organizations
- AWS Systems Manager Automation

Sonstige Ressourcen

- jq manual (jq-Website)
- jq-Download (GitHub)

Sichern von SunSpeedRC-Servern im Stromasys Charon-SSP-Emulator in der AWS Cloud

Erstellt von Kevin Yung (AWS), Luis Ramos (asys) und Rohit Darji (AWS)

Umgebung: Produktion	Technologien: Speicher und Backup; Betriebssysteme; DevOps	Workload: Oracle
AWS-Services: Amazon EFS ; Amazon S3; AWS Storage Gateway ; AWS Systems Manager ; Amazon EC2		

Übersicht

Dieses Muster bietet vier Optionen zum Sichern Ihrer Sun MicrosystemsRC-Server nach einer Migration von einer On-Premises-Umgebung zur Amazon Web Services (AWS) Cloud. Diese Backup-Optionen helfen Ihnen bei der Implementierung eines Backup-Plans, der dem Recovery Point Objective (RPO) und dem Recovery Time Objective (RTO) Ihrer Organisation entspricht, automatisierte Ansätze verwendet und Ihre Gesamtbetriebskosten senkt. Das Muster bietet einen Überblick über die vier Backup-Optionen und Schritte, um sie zu implementieren.

Wenn Sie einen SonSpeedRC-Server verwenden, der als Gast auf einem Stromasys-Choron-SSP-Emulator gehostet wird, können Sie eine der folgenden drei Backup-Optionen verwenden:

- Backup-Option 1: Virtuelles Stromasys-Band – Verwenden Sie die Funktion Virtuelles Charon-SSP-Band, um eine Backup-Einrichtung auf dem SunSpeedRC-Server einzurichten und Ihre Backup-Dateien mithilfe von AWS Systems Manager Automation in Amazon Simple Storage Service (Amazon S3) und Amazon Simple Storage Service Glacier zu archivieren. AWS Systems Manager

- Backup-Option 2: Stromasys-Snapshot – Verwenden Sie die Charon-SSP-Snapshot-Funktion, um eine Backup-Einrichtung für die son KerRC-Gastserver in Charon-SSP einzurichten.

- Backup-Option 3: Volume-Snapshot von Amazon Elastic Block Store (Amazon EBS) – Wenn Sie den Charon-SSP-Emulator auf Amazon Elastic Compute Cloud (Amazon EC2) hosten, können Sie einen Amazon-EBS-Volume-Snapshot verwenden, um Backups für ein Son-RC-Dateisystem zu erstellen.

Wenn Sie einen als Gast auf Hardware und Charon-SSP auf Amazon EC2 gehosteten Son KerRC-Server verwenden, können Sie die folgende Sicherungsoption verwenden:

- Backup-Option 4: Virtuelle Bandbibliothek (VTL) von AWS Storage Gateway – Verwenden Sie eine Backup-Anwendung mit einem Storage Gateway VTL Tape Gateway, um die Son-TravelRC-Server zu sichern.

Wenn Sie einen SonSpeedRC-Server verwenden, der als Zeitzone auf einem SoRC-Server gehostet wird, können Sie die Backup-Optionen 1, 2 und 4 verwenden.

Stromasys bietet Software und Services zur Emulation älterer, kritischer Systeme von ORRC, Alpha, VAX und PA-C. Weitere Informationen zur Migration in die AWS Cloud mithilfe der Stromasys-Emulation finden Sie unter Hostwechsel von microSDRC-, Alpha- oder anderen Legacy-Systemen zu AWS mit Stromasys im AWS Blog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vorhandene SunSpeedRC-Server.
- Bestehende Lizenzen für Charon-SSP. Lizenzen für Charon-SSP sind über AWS Marketplace verfügbar und Lizenzen für Stromasys Virtual Environment (VE) sind über Stromasys verfügbar. Weitere Informationen erhalten Sie von Stromasys sales .
- Vertrautheit mit SunSpeedRC-Servern und Linux-Backups.
- Vertrautheit mit der Charon-SSP-Emulationstechnologie. Weitere Informationen dazu finden Sie unter Stromasys Legacy Server Emulation in der Stromasys-Dokumentation.
- Wenn Sie die virtuelle Bandeinrichtung oder Backup-Anwendungen für Ihre SunSpeedRC-Server-Dateisysteme verwenden möchten, müssen Sie die Backup-Einrichtungen für das SunSpeedRC-Server-Dateisystem erstellen und konfigurieren.

- Ein Verständnis von RPO und RTO. Weitere Informationen dazu finden Sie unter Ziele für die Notfallwiederherstellung aus dem Whitepaper Säule der Zuverlässigkeit in der AWS Well-Architected Framework-Dokumentation.
- Um Backup-Option 4 verwenden zu können, benötigen Sie Folgendes:
  - Eine softwarebasierte Sicherungsanwendung, die ein Storage Gateway VTL Tape Gateway unterstützt. Weitere Informationen dazu finden Sie unter Arbeiten mit VTL-Geräten in der AWS Storage Gateway-Dokumentation.
  - Bac Director oder eine ähnliche Backup-Anwendung, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Bac Director-Dokumentation.

Die folgende Tabelle enthält Informationen zu den vier Backup-Optionen in diesem Muster.

Backup-Optionen	Erzielt Absturzkonsistenz?	Erzielt Anwendungskonsistenz?	Lösung der virtuellen Backup-Appliance?	Typische Anwendungsfälle
Option 1 – Virtuelles Stromasys-Band	Ja Sie können Snapshots des SunSpeedRC-Dateisystems automatisieren, um Daten auf einem virtuellen Band zu sichern. Sie können beispielsweise UFS- oder ZFS-Snapshots verwenden.	Ja Diese Sicherungsoption erfordert ein automatisiertes Skript, um laufende Transaktionen zu leeren, während des Dateisystem-Snapshots einen schreibgeschützten oder temporären Offline-Modus zu konfigurieren oder einen Anwendungsdaten-Dump	Ja	Sicherung von Sun-TravelRC-Server-Dateisystemen mit .tar- oder .zip-Dateien Backup von Anwendungsdaten

zu erstellen. Möglicherweise benötigen Sie auch Anwendung sausfallzeit oder schreibge schützten Modus.

Option 2 – Stromasys-Snapshot	Ja Sie müssen Charon-SSP Manager konfigurieren oder ein Befehlszeilen-Startup-Argument verwenden, um diese Funktion zu aktivieren. Sie müssen auch einen Linux-Befehl ausführen, um den Charon-SSP-Emulator aufzufordern, den Status des SunSpeedRC-Gastservers in einer Snapshot-Datei zu speichern. Wichtig: Sie müssen den Gastserver von SunSpeedRC herunterfahren.	Ja Diese Sicherungsoption erstellt einen Snapshot des emulierten Gastservers, einschließlich seiner virtuellen Festplatten und Speicherabbild. Wichtig: Sie müssen den Gastserver von SunSpeedRC während des Snapshots herunterfahren.	Nein	Snapshot des SonSpeedRC-Servers Backup von Anwendungsdaten

Option 3 – Amazon-EBS-Volume-Snapshot	Ja Sie können AWS Backup verwenden, um den Amazon EBS-Snapshot zu automatisieren.	Ja Diese Sicherungsoption erfordert ein automatisiertes Skript, um laufende Transaktionen zu leeren und während des Amazon-EBS-Volume-Snapshots einen schreibgeschützten oder temporären Stopp der EC2-Instance zu konfigurieren. Wichtig: Diese Sicherungsoption erfordert möglicherweise Anwendungsausfallzeit oder schreibgeschützten Modus, um die Anwendungskonsistenz zu erreichen.	Nein	Snapshot des Sun-TravelRC-Serverdateisystems Backup von Anwendungsdaten

Option 4 – AWS Storage Gateway VTL	Ja Sie können mithilfe eines Backup-Agenten automatisch Sicherungsdaten des SunSpeedRC-Dateisystems in der VTL sichern.	Ja Diese Sicherungsoption erfordert ein automatisiertes Skript, um laufende Transaktionen zu leeren und während des Dateisystem-Snapshots oder des Anwendungsdaten-Dumps einen schreibgeschützten oder temporären Offline-Modus zu konfigurieren. Wichtig: Diese Backup-Option erfordert möglicherweise Anwendungsausfallzeit oder schreibgeschützten Modus.	Ja	Eine große Flotte von Backups für das SunSpeedRC-Serverdateisystem Backup von Anwendungsdaten

Einschränkungen

- Sie können die Ansätze dieses Musters verwenden, um einzelne SunSpeedRC-Server zu sichern, aber Sie können diese Backup-Optionen auch für gemeinsam genutzte Daten verwenden, wenn Sie Anwendungen haben, die in einem Cluster ausgeführt werden.

Tools

Backup-Option 1: Virtuelles Stromasys-Band

- Stromasys Charon-SSP-Emulator – Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen microSDRC-Hardware in einem mit x86 kompatiblen Standardcomputersystem mit 64 Bit. Es führt den ursprünglichen BolRC-Binärcode aus, einschließlich Betriebssystemen (OSs) wie SunOS oder Bolis, deren mehrschichtigen Produkte und Anwendungen.
- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der anpassbare Rechenkapazität bereitstellt, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- Amazon EFS – Amazon Elastic File System (Amazon EFS) bietet ein einfaches, Serverless- set-and-forget Elastic-Dateisystem für die Verwendung mit AWS Cloud-Services und On-Premises-Ressourcen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.
- Amazon S3 Glacier – Amazon Simple Storage Service Glacier ist eine sichere, dauerhafte und extrem kostengünstige Amazon S3-Speicherklasse für die Datenarchivierung und langfristige Sicherung.
- AWS Systems Manager Automation – Automation, eine Funktion von AWS Systems Manager, vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von EC2-Instances und anderen AWS-Ressourcen.

Backup-Option 2: Stromasys-Snapshot

- Stromasys Charon-SSP-Emulator – Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen microSDRC-Hardware in einem mit x86 kompatiblen Standardcomputersystem mit 64 Bit. Es führt den ursprünglichen microSDRC-Binärcode aus, einschließlich OSs wie SunOS oderis, deren mehrschichtige Produkte und Anwendungen.
- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der anpassbare Rechenkapazität bereitstellt, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- Amazon EFS – Amazon Elastic File System (Amazon EFS) bietet ein einfaches, Serverless- set-and-forget Elastic-Dateisystem für die Verwendung mit AWS Cloud-Services und On-Premises-Ressourcen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.

- Amazon S3 Glacier – Amazon Simple Storage Service Glacier ist eine sichere, dauerhafte und extrem kostengünstige Amazon S3-Speicherklasse für die Datenarchivierung und langfristige Sicherung.
- AWS Systems Manager Automation – Automation, eine Funktion von AWS Systems Manager, vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von EC2-Instances und anderen AWS-Ressourcen.

Backup-Option 3: Amazon-EBS-Volume-Snapshot

- Stromasys Charon-SSP-Emulator – Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen microSDRC-Hardware in einem mit x86 kompatiblen Standardcomputersystem mit 64 Bit. Es führt den ursprünglichen microSDRC-Binärcode aus, einschließlich OSs wie SunOS oderis, deren mehrschichtige Produkte und Anwendungen.
- AWS Backup – AWS Backup ist ein vollständig verwalteter Datenschutzservice, der die Zentralisierung und Automatisierung über AWS-Services, in der Cloud und On-Premises vereinfacht.
- Amazon EBS – Amazon Elastic Block Store (Amazon EBS) stellt Volumes für die Speicherung auf Blockebene für die Verwendung mit EC2-Instances bereit.
- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der anpassbare Rechenkapazität bereitstellt, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.

Backup-Option 4: AWS Storage Gateway VTL

- Stromasys Charon-SSP-Emulator – Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen microSDRC-Hardware in einem mit x86 kompatiblen Standardcomputersystem mit 64 Bit. Es führt den ursprünglichen microSDRC-Binärcode aus, einschließlich OSs wie SunOS oderis, deren mehrschichtige Produkte und Anwendungen.
- Bac – Bac ist ein Open-Source-System für Computer-Backups auf Unternehmensebene. Weitere Informationen darüber, ob Ihre vorhandene Sicherungsanwendung Tape Gateway unterstützt, finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway in der AWS Storage Gateway-Dokumentation.

- Amazon EC2 – Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der anpassbare Rechenkapazität bereitstellt, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- Amazon RDS for MySQL – Amazon Relational Database Service (Amazon RDS) unterstützt DB-Instances, die mehrere Versionen von MySQL ausführen.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.
- Amazon S3 Glacier – Amazon Simple Storage Service Glacier ist eine sichere, dauerhafte und extrem kostengünstige Amazon S3-Speicherklasse für die Datenarchivierung und langfristige Sicherung.
- AWS Storage Gateway – Storage Gateway verbindet eine On-Premises-Software-Appliance mit cloudbasiertem Speicher, um eine nahtlose Integration mit Datensicherheitsfunktionen zwischen Ihrer On-Premises-IT-Umgebung und der AWS-Speicherinfrastruktur zu ermöglichen.

Polen

Backup-Option 1 – Erstellen eines virtuellen Stromasys-Band-Backups

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein freigegebenes Amazon-EFS-Dateisystem für den virtuellen Banddateispeicher.	Melden Sie sich bei der AWS-Managementkonsole an oder verwenden Sie AWS CLI, um ein Amazon EFS-Dateisystem zu erstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Amazon-EFS-Dateisystems in der Amazon-EFS-Dokumentation.	Cloud-Architekt
Konfigurieren Sie den Linux-Host zum Mounten des freigegebenen Dateisystems.	Installieren Sie den Amazon-EFS-Treiber auf der Amazon EC2-Linux-Instance und konfigurieren Sie das Linux-Betriebssystem so, dass das freigegebene Amazon-EFS-	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dateisystem während des Startups gemountet wird. Weitere Informationen dazu finden Sie unter Mounting von Dateisystemen mit der EFS-Mountinghilfe in der Amazon-EFS-Dokumentation.	
Installieren Sie den Charon-SSP-Emulator.	Installieren Sie den Charon-SSP-Emulator auf der Amazon EC2 Linux-Instance. Weitere Informationen dazu finden Sie unter Einrichten einer AWS Cloud-Instance für Charon-SSP in der Stromasys -Dokumentation.	DevOps Techniker
Erstellen Sie einen virtuelle n Banddateicontainer im gemeinsam genutzten Dateisystem für jeden SunSpeedRC-Gastserver.	Führen Sie den `touch <vtape-container-name>` Befehl aus, um einen virtuellen Banddatei container im gemeinsam genutzten Dateisystem für jeden im Charon-SSP-Emulato r bereitgestellten SonSpeedR C-Gastserver zu erstellen.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Charon-SSP Manager, um virtuelle Bandgeräte für die sonnenbea ufsichtigten Gastserver zu erstellen.	Melden Sie sich bei Charon-SSP Manager an, erstellen Sie virtuelle Bandgeräte und konfigurieren Sie sie so, dass sie die virtuellen Bandcontainerdateien für jeden sonnenauftretenden Gastserver verwenden. Weitere Informationen dazu finden Sie im Benutzerh andbuch von Charon-SSP 5.2 für Linux in der Stromasys-Dokumentation.	DevOps Techniker
Stellen Sie sicher, dass das virtuelle Bandgerät auf den Gastservern von SunSpeedR C verfügbar ist.	Melden Sie sich bei jedem soN-TravelRC-Gastserver an und führen Sie den `mt -f /dev/rmt/1` Befehl aus, um zu überprüfen, ob das virtuelle Bandgerät im Betriebssystem konfiguriert ist.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie das Systems Manager Automation-Runbook und die Automatisierung.	Entwickeln Sie das Systems Manager Automation-Runbook und richten Sie Wartungsfenster und -zuordnungen in Systems Manager ein, um den Backup-Prozess zu planen. Weitere Informationen dazu finden Sie unter Automation-Walkthroughs und Einrichten von Wartungsfenstern in der AWS Systems Manager-Dokumentation.	Cloud-Architekt
Konfigurieren Sie Systems Manager Automation, um gedrehte virtuelle Bandcontainerdateien zu archivieren.	Verwenden Sie das Codebeispiel aus Back-Option 1 im Abschnitt Zusätzliche Informationen, um ein Systems Manager Automation-Runbook zu entwickeln, um rotierte virtuelle Bandcontainerdateien in Amazon S3 und Amazon S3 Glacier zu archivieren.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Systems Manager Automation-Runbook für die Archivierung und Terminplanung bereit.	Stellen Sie das Systems Manager Automation-Runbook bereit und planen Sie es so, dass es automatisch in Systems Manager ausgeführt wird. Weitere Informationen dazu finden Sie unter Automation Walkthroughs in der Systems Manager-Dokumentation.	Cloud-Architekt

Backup-Option 2 – Erstellen eines Stromasys-Snapshots

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein freigegeb enes Amazon-EFS-Dateisy stem für den virtuellen Banddateispeicher.	Melden Sie sich bei der AWS-Managementkonsole an oder verwenden Sie AWS CLI, um ein Amazon EFS-Dateisystem zu erstellen. Weitere Informationen dazu finden Sie unter Erstellen Ihres Amazon-EFS-Dateisystems in der Amazon-EFS-Dokumen tation.	Cloud-Architekt
Konfigurieren Sie den Linux-Host zum Mounten des freigegebenen Dateisystems.	Installieren Sie den Amazon-EFS-Treiber in der Amazon EC2-Linux-Instance und konfigurieren Sie das Linux-Betriebssystem so, dass das freigegebene Amazon-EF	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S-Dateisystem beim Start gemountet wird. Weitere Informationen dazu finden Sie unter Mounting von Dateisystemen mit der EFS-Mountinghilfe in der Amazon-EFS-Dokumentation.	
Installieren Sie den Charon-SSP-Emulator.	Installieren Sie den Charon-SSP-Emulator auf der Amazon EC2 Linux-Instance. Weitere Informationen dazu finden Sie unter Einrichten einer AWS Cloud-Instance für Charon-SSP in der Stromasys -Dokumentation.	DevOps Techniker
Konfigurieren Sie die so, dass sie mit der Snapshot-Option beginnen.	Verwenden Sie den Charon-SSP Manager, um die Snapshot-Option für jeden son-TravelRC-Gastserver einzurichten. Weitere Informationen dazu finden Sie im Benutzerhandbuch von Charon-SSP 5.2 für Linux in der Stromasys-Dokumentation.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie das Systems Manager Automation-Runbook .	Verwenden Sie das Codebeispiel aus Backup-Option 2 im Abschnitt Zusätzliche Informationen, um ein Systems Manager Automation-Runbook zu entwickeln, mit dem Sie den Snapshot-Befehl während eines Wartungsfensters remote auf einem sonnenaufgehenden Gastserver ausführen können.	Cloud-Architekt
Stellen Sie das Systems Manager Automation-Runbook bereit und richten Sie die Zuordnung zu den Amazon EC2 Linux-Hosts ein.	Stellen Sie das Systems Manager Automation-Runbook bereit und richten Sie Wartungsfenster und -zuordnungen in Systems Manager ein, um den Backup-Prozess zu planen. Weitere Informationen dazu finden Sie unter Automation-Walkthroughs und Einrichten von Wartungsfenstern in der AWS Systems Manager-Dokumentation.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Archivieren Sie Snapshots im Langzeitspeicher.	Verwenden Sie den Runbook-Beispielcode aus dem Abschnitt Zusätzliche Informationen, um ein Systems Manager Automation-Runbook zum Archivieren von Snapshot-Dateien in Amazon S3 und Amazon S3 Glacier zu entwickeln.	Cloud-Architekt

Backup-Option 3 – Erstellen eines Amazon-EBS-Volume-Snapshots

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Charon-SSP-Emulator.	Installieren Sie den Charon-SSP-Emulator auf der Amazon EC2 Linux-Instance. Weitere Informationen dazu finden Sie unter Einrichten einer AWS Cloud-Instance für Charon-SSP in der Stromasys -Dokumentation.	DevOps Techniker
Erstellen Sie EBS-Volumes für die So SPRAC-Gastserver.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon EBS-Konsole und erstellen Sie dann EBS-Volumes für die So SPRAC-Gastserver. Weitere Informationen dazu finden Sie unter Einrichten einer AWS Cloud-Instance für	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Charon-SSP in der Stromasys -Dokumentation.	
Fügen Sie die EBS-Volumes an die Amazon EC2 Linux-Instance an.	Fügen Sie in der Amazon EC2-Konsole die EBS-Volumes an die Amazon EC2 Linux-Instance an. Weitere Informationen dazu finden Sie unter Anfügen eines Amazon-EBS-Volumes an eine Instance in der Amazon EC2Dokumentation.	AWS DevOps
Ordnen Sie EBS-Volumes als SCSI-Laufwerke im Charon-SSP-Emulator zu.	Konfigurieren Sie den Charon-SSP Manager so, dass die EBS-Volumes als SCSI-Laufwerke auf den son-Trave IRC-Gastservern zugeordnet werden. Weitere Informationen dazu finden Sie im Abschnitt SCSI-Speicherkonfiguration im Handbuch Charon-SSP V5.2 für Linux in der Stromasys-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den AWS Backup-Zeitplan für die Snapshots der EBS-Volumes.	Richten Sie AWS Backup-Richtlinien und -Zeitpläne ein, um Snapshots der EBS-Volumes zu erstellen. Weitere Informationen dazu finden Sie im Tutorial Amazon EBS-Backup und -Wiederherstellung mit AWS Backup in der AWS Developer Center-Dokumentation.	AWS DevOps

Backup-Option 4 – Erstellen einer AWS Storage Gateway-VTL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Tape Gateway-Gerät.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS Storage Gateway-Konsole und erstellen Sie dann ein Tape Gateway-Gerät in einer VPC. Weitere Informationen dazu finden Sie unter Erstellen eines Gateways in der AWS Storage Gateway-Dokumentation.	Cloud-Architekt
Erstellen Sie eine Amazon RDS-DB-Instance für den Bac Catalog.	Öffnen Sie die Amazon-RDS-Konsole und erstellen Sie eine Amazon-RDS-für-MySQL-DB-Instance.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen dazu finden Sie unter Erstellen einer MySQL-DB-Instance und Herstellen einer Verbindung mit einer Datenbank auf einer MySQL-DB-Instance in der Amazon RDS-Dokumentation.	
Stellen Sie den Backup-Anwendungscontroller in der VPC bereit.	Installieren Sie Bac auf der EC2-Instance, stellen Sie den Backup-Anwendungscontroller bereit und konfigurieren Sie dann den Backup-Speicher für die Verbindung mit dem Tape Gateway-Gerät. Sie können die Bac Director-Speicher-Daemon-Beispielkonfiguration in der `Bacula-storage-daemon-config.txt` Datei (angefügt) verwenden. Weitere Informationen dazu finden Sie in der Bac-Dokumentation.	AWS DevOps
Richten Sie die Backup-Anwendung auf den Gastservern von SunSpeedRC ein.	Richten Sie einen zweiten Client ein, um die Backup-Anwendung auf den Gastservern von SunSpeedRC zu installieren und einzurichten, indem Sie die Bac-Beispielkonfiguration in der `-SUN-SPARC-Guest-Bacula-Config.txt` Datei (angefügt) verwenden.	DevOps Techniker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Backup-Konfiguration und den Zeitplan ein.	Richten Sie die Backup-Konfiguration und Zeitpläne im Backup-Anwendungscontroller ein, indem Sie die Bac Director-Beispielkonfiguration in der `-Bacula-Directory-Config.txt` Datei (angefügt) verwenden. Weitere Informationen dazu finden Sie in der Bac-Dokumentation.	DevOps Techniker
Überprüfen Sie, ob die Backup-Konfiguration und die Zeitpläne korrekt sind.	Folgen Sie den Anweisungen in der Bac-Dokumentation, um die Validierungs- und Backup-Tests für Ihr Setup auf den son-TravelRC-Gastservern durchzuführen. Sie können beispielsweise die folgenden Befehle verwenden, um die Konfigurationsdateien zu validieren: • `bacula-dir -t -c bacula-dir.conf` • `bacula-fd -t -c bacula-fd.conf` • `bacula-sd -t -c bacula-sd.conf`	DevOps Techniker

Zugehörige Ressourcen

- Virtuelles KerRC von Charon mit VE-Lizenzierung

- Virtuelles KerRC in Charon
- Verwenden von Cloud-Services und Objektspeicher mit Bac Enterprise Edition
- Notfallwiederherstellungs-Ziele (DR)
- Legacy-Systememulationslösungen von Charon

Zusätzliche Informationen

Backup-Option 1 – Erstellen eines virtuellen Stromasys-Bands

Sie können den folgenden Beispiel-Runbook-Code für Systems Manager Automation verwenden, um die Sicherung automatisch zu starten und dann die Bänder auszutauschen:

```
...
# example backup script saved in SUN SPARC Server
 #!/usr/bin/bash
 mt -f  rewind
 tar -cvf
 mt -f  offline
...
         mainSteps:
         - action: aws:runShellScript
           name:
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # Validate tape backup container file exists
               if [ ! -f {{TapeBackupContainerFile}} ]; then
                 logger -s -p local3.warning "Tape backup container file is not exists
 - {{TapeBackupContainerFile}}, create a new one"
                 touch {{TapeBackupContainerFile}}
               fi
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               user={{BACKUP_USER}}
```

```
              keypair={{KEYPAIR_PATH}}
              server={{SUN_SPARC_IP}}
              backup_script={{BACKUP_SCRIPT}}
              ssh -i $keypair $user@$server -c "/usr/bin/bash $backup_script"
        - action: aws:runShellScript
          name: swapVirtualDiskContainer
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              mv {{TapeBackupContainerFile}} {{TapeBackupContainerFile}}.$(date +%s)
              touch {{TapeBackupContainerFile}}
        - action: aws:runShellScript
          name: uploadBackupArchiveToS3
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              aws s3 cp {{TapeBackupContainerFile}} s3://{{BACKUP_BUCKET}}/
{{SUN_SPARC_IP}}/$(date '+%Y-%m-%d')/
 ...
```

Backup-Option 2 – Stromasys-Snapshot

Sie können den folgenden Beispiel-Runbook-Code für Systems Manager Automation verwenden, um den Backup-Prozess zu automatisieren:

```
      ...

         mainSteps:
         - action: aws:runShellScript
           name: startSnapshot
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # You may consider some graceful stop of the application before taking a
 snapshot
               # Query SSP PID by configuration file
```

```
              # Example: ps ax | grep ssp-4 | grep Solaris10.cfg | awk '{print $1"
 "$5}' | grep ssp4 | cut -f1 -d" "
              pid=`ps ax | grep ssp-4 | grep {{SSP_GUEST_CONFIG_FILE}} | awk '{print
 $1" "$5}' | grep ssp4 | cut -f1 -d" "`
              if [ -n "${pid}" ]; then
                kill -SIGTSTP ${pid}
              else
                echo "No PID found for SPARC guest with config
 {{SSP_GUEST_CONFIG_FILE}}"
                exit 1
              fi
        - action: aws:runShellScript
          name: startBackup
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              # upload snapshot and virtual disk files into S3
              aws s3 sync {{SNAPSHOT_FOLDER}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
              aws s3 cp {{VIRTUAL_DISK_FILE}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
        - action: aws:runShellScript
          name: restratSPARCGuest
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              /opt/charon-ssp/ssp-4u/ssp4u -f {{SSP_GUEST_CONFIG_FILE}} -d -a
 {{SPARC_GUEST_NAME}} --snapshot {{SNAPSHOT_FOLDER}}
 ...
```

Backup-Option 4 – AWS Storage Gateway VTL

Wenn Sie Bolis Nicht-Global Zones verwenden, um virtualisierte Legacy-SunRC-Server auszuführen, kann der Ansatz der Backup-Anwendung auf Nicht-Global Zones angewendet werden, die auf den SunSpeedRC-Servern ausgeführt werden (z. B. kann der Backup-Client innerhalb der Nicht-Global Zones ausgeführt werden). Der Backup-Client kann jedoch auch auf demis-Host ausgeführt werden und Snapshots der nicht globalen Zonen erstellen. Die Snapshots können dann auf einem Band gesichert werden.

Die folgende Beispielkonfiguration fügt das Dateisystem, das die nicht globalen Bolis-Zonen hostet, zur Backup-Konfiguration für denis-Host hinzu:

```
FileSet {
   Name = "Branded Zones"
   Include {
     Options {
       signature = MD5
     }
     File = /zones
   }
 }
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die diesem Dokument zugeordnet sind, entpacken Sie die folgende Datei: attachment.zip

Sichern und Archivieren von Daten in Amazon S3 mit Veeam Backup & Replication

Erstellt vonna, Anthony Fiore (AWS) (AWS) und Bol Quigley

Umgebung: Produktion	Technologien: Speicher und Backup	AWS-Services: Amazon EC2; Amazon S3; Amazon S3 Glacier

Übersicht

Dieses Muster beschreibt den Prozess zum Senden von Backups, die von Veeam Backup & Replication erstellt wurden, an unterstützte Amazon Simple Storage Service (Amazon S3)-Objektspeicherklassen mithilfe der Veeam-Scale-Out-Backup-Repository-Funktion.

Veeam unterstützt mehrere Amazon S3-Speicherklassen, um Ihren spezifischen Anforderungen am besten zu entsprechen. Sie können den Speichertyp basierend auf den Datenzugriffs-, Ausfallsicherheits- und Kostenanforderungen Ihrer Sicherungs- oder Archivdaten auswählen. Sie können beispielsweise Daten, die Sie 30 Tage oder länger nicht verwenden möchten, in Amazon S3 Infrequent Access (IA) speichern, um die Kosten zu senken. Wenn Sie Daten 90 Tage oder länger archivieren möchten, können Sie Amazon Simple Storage Service Glacier (Amazon S3 Glacier) Flexible Retrieval oder S3 Glacier Deep Archive mit der Archivstufe von Veeam verwenden. Sie können auch die S3-Objektsperre verwenden, um Backups in Amazon S3 unveränderlich zu machen.

Dieses Muster behandelt nicht, wie Veeam Backup & Replication mit einem Band-Gateway in AWS Storage Gateway eingerichtet wird. Informationen zu diesem Thema finden Sie unter Veeam Backup & Replication using AWS VTL Gateway – Bereitstellungshandbuch auf der Veeam-Website.

> Warnung: Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfrist igen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, dass Sie diesen Benutzern nur die Berechtigungen gewähren, die sie zur Ausführung der Aufgabe benötigen, und dass Sie diese Benutzer entfernen, wenn sie nicht mehr benötigt werden. Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informati onen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Veeam Backup & Replication, einschließlich Veeam Availability Suite oder Veeam Backup microSD, installiert (Sie können sich für eine kostenlose Testversion registrieren)
- Veeam Backup & Replication-Lizenz mit Enterprise- oder Enterprise Plus-Funktionalität, die Veeam Universal License (VUL) enthält
- Ein aktiver AWS Identity and Access Management (IAM)-Benutzer mit Zugriff auf einen Amazon S3-Bucket
- Ein aktiver IAM-Benutzer mit Zugriff auf Amazon Elastic Compute Cloud (Amazon EC2) und Amazon Virtual Private Cloud (Amazon VPC) (bei Verwendung der Archivstufe)
- Netzwerkkonnektivität von On-Premises zu AWS-Services mit verfügbarer Bandbreite für die Sicherung und Wiederherstellung des Datenverkehrs über eine öffentliche Internetverbindung oder eine öffentliche virtuelle Schnittstelle (VIF) von AWS Direct Connect
- Die folgenden Netzwerkports und Endpunkte werden geöffnet, um eine ordnungsgemäße Kommunikation mit Objektspeicher-Repositorys sicherzustellen:
  - Amazon S3-Speicher – TCP – Port 443: Wird für die Kommunikation mit Amazon S3-Speicher verwendet.
  - Amazon S3-Speicher – Cloud-Endpunkte – *.amazonaws.com für AWS-Regionen und AWS GovCloud (US)-Regionen oder *.amazonaws.com.cn für China-Regionen: Wird für die Kommunikation mit Amazon S3-Speicher verwendet. Eine vollständige Liste der Verbindungsendpunkte finden Sie unter Amazon S3-Endpunkte in der AWS-Dokumentation.
  - Amazon S3-Speicher – TCP HTTP – Port 80: Wird verwendet, um den Zertifikatstatus zu überprüfen. Beachten Sie, dass sich die Endpunkte der Zertifikatüberprüfung – CRL-URLs (Zertifikatsperrliste) und OCSP-Server (Online Certificate Status Protocol) – ändern können. Die tatsächliche Liste der Adressen finden Sie im Zertifikat selbst.
  - Amazon S3-Speicher – Endpunkte zur Zertifikatüberprüfung – *.amazontrust.com: Wird verwendet, um den Zertifikatstatus zu überprüfen. Beachten Sie, dass sich die Endpunkte zur Zertifikatüberprüfung (CRL-URLs und OCSP-Server) ändern können. Die tatsächliche Liste der Adressen finden Sie im Zertifikat selbst.

Einschränkungen

- Veeam unterstützt keine S3-Lebenszyklusrichtlinien für S3-Buckets, die als Veeam-Objektspeicher-Repositorys verwendet werden. Dazu gehören Richtlinien mit Amazon S3-Speicherklassenübergängen und Ablaufregeln für den S3-Lebenszyklus. Veeam muss die einzige Entität sein, die diese Objekte verwaltet. Die Aktivierung von S3-Lebenszyklusrichtlinien kann unerwartete Ergebnisse haben, einschließlich Datenverlust.

Produktversionen

- Veeam Backup & Replication v9.5 Update 4 oder höher (nur Backup oder Kapazitätsstufe)
- Veeam Backup & Replication v10 oder höher (Backup- oder Kapazitätsebene und S3-Objektsperre)
- Veeam Backup & Replication v11 oder höher (Backup- oder Kapazitätsebene, Archiv- oder Archivebene und S3-Objektsperre)
- Veeam Backup & Replication v12 oder höher (Leistungsstufe, Backup- oder Kapazitätsstufe, Archiv- oder Archivstufe und S3-Objektsperre)
- S3 Standard
- S3 Standard-IA
- S3 One Zone-IA
- S3 Glacier Flexible Retrieval (nur v11 und höher)
- S3 Glacier Deep Archive (nur v11 und höher)
- S3 Glacier Instant Retrieval (nur v12 und höher)

Architektur

Quelltechnologie-Stack

- On-Premises-Installation von Veeam Backup & Replication mit Konnektivität von einem Veeam-Backup-Server oder einem Veeam-Gateway-Server zu Amazon S3

Zieltechnologie-Stack

- Amazon S3
- Amazon VPC und Amazon EC2 (bei Verwendung der Archivstufe)

Zielarchitektur: SOBR

Das folgende Diagramm zeigt die Scale-Out Backup Repository (SOBR)-Architektur.

Die Software Veeam Backup and Replication schützt Daten vor logischen Fehlern wie Systemausfällen, Anwendungsfehlern oder versehentlichem Löschen. In diesem Diagramm werden Backups zuerst On-Premises ausgeführt und eine sekundäre Kopie wird direkt an Amazon S3 gesendet. Ein Backup stellt eine point-in-time Kopie der Daten dar.

Der Workflow besteht aus drei primären Komponenten, die für das Tiering oder Kopieren von Backups in Amazon S3 erforderlich sind, und einer optionalen Komponente:

- Veeam Backup & Replication (1) – Der Backup-Server, der für die Koordination, Steuerung und Verwaltung der Backup-Infrastruktur, Einstellungen, Aufträge, Wiederherstellungsaufgaben und anderer Prozesse verantwortlich ist.
- Veeam-Gateway-Server (im Diagramm nicht dargestellt) – Ein optionaler On-Premises-Gateway-Server, der erforderlich ist, wenn der Veeam-Backup-Server keine ausgehende Verbindung zu Amazon S3 hat.
- Scale-Out-Backup-Repository (2) – Repository-System mit horizontaler Skalierungsunterstützung für mehrstufige Speicherung von Daten. Das Scale-Out-Backup-Repository besteht aus einem oder mehreren Backup-Repositorys, die einen schnellen Zugriff auf Daten ermöglichen, und kann mit Amazon S3-Objektspeicher-Repositorys für die langfristige Speicherung (Kapazitätsstufe) und Archivierung (Archivierungsebene) erweitert werden. Veeam verwendet das Scale-Out-Backup-Repository, um Daten automatisch zwischen lokalem (Leistungsstufe) und Amazon S3-Objektspeicher (Kapazitäts- und Archivstufen) zu stufen.
- Amazon S3 (3) – AWS-Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

Zielarchitektur: DTO

Das folgende Diagramm zeigt die direct-to-object (DTO)-Architektur.

In diesem Diagramm werden Sicherungsdaten direkt an Amazon S3 weitergeleitet, ohne zuerst On-Premises gespeichert zu werden. Sekundäre Kopien können in S3 Glacier gespeichert werden.

Automatisierung und Skalierung

Sie können die Erstellung von IAM-Ressourcen und S3-Buckets mithilfe der im VeeamHub GitHub Repository bereitgestellten AWS- CloudFormation Vorlagen automatisieren. Die Vorlagen enthalten sowohl Standard- als auch unveränderliche Optionen.

Tools

Tools und AWS-Services

- Veeam Backup & Replication ist eine Lösung von Veeam zum Schutz, Sichern, Replizieren und Wiederherstellen Ihrer virtuellen und physischen Workloads.
- AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, deren Bereitstellung schnell und konsistent und deren Verwaltung während ihres gesamten Lebenszyklus. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere AWS-Konten und AWS-Regionen hinweg verwalten und bereitstellen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können Amazon EC2 verwenden, um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können auf- oder abskalieren.
- AWS Identity and Access Management (IAM) ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services. Mit IAM können Sie Benutzer, Sicherheitsanmeldeinformationen wie Zugriffsschlüssel und Berechtigungen, die steuern, auf welche AWS-Ressourcen Benutzer und Anwendungen zugreifen können, zentral verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon S3 Glacier (S3 Glacier) ist ein sicherer und dauerhafter Service für die kostengünstige Archivierung und langfristige Sicherung von Daten.
- Amazon Virtual Private Cloud (Amazon VPC) stellt einen logisch isolierten Abschnitt der AWS Cloud bereit, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Code

Verwenden Sie die im VeeamHub GitHub Repository bereitgestellten CloudFormation Vorlagen, um die IAM-Ressourcen und S3-Buckets für dieses Muster automatisch zu erstellen. Wenn Sie diese Ressourcen lieber manuell erstellen möchten, führen Sie die Schritte im Abschnitt „Pics“ aus.

Bewährte Methoden

- Gemäß den bewährten Methoden von IAM empfehlen wir dringend, die langfristigen IAM-Benutzeranmeldeinformationen regelmäßig zu rotieren, z. B. den IAM-Benutzer, den Sie zum Schreiben von Veeam-Backup- und Replikations-Backups in Amazon S3 verwenden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in der IAM-Dokumentation.

Polen

Konfigurieren des Amazon S3-Speichers in Ihrem Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen IAM-Benutzer.	Folgen Sie den Anweisungen in der IAM-Dokumentation, um einen IAM-Benutzer zu erstellen. Dieser Benutzer sollte keinen AWS-Konsolenzugriff haben, und Sie müssen einen Zugriffsschlüssel für diesen Benutzer erstellen. Veeam verwendet diese Entität, um sich bei AWS zu authentifizieren, um Ihre S3-Buckets zu lesen und in sie zu schreiben. Sie müssen die geringsten Berechtigungen erteilen (d. h. nur die Berechtigungen erteilen, die zum Ausführen einer Aufgabe erforderlich sind), damit der Benutzer nicht mehr Autorität hat, als	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	er benötigt. Beispiele für IAM-Richtlinien, die Ihrem Veeam-IAM-Benutzer angefügt werden können, finden Sie im Abschnitt Zusätzliche Informationen. Hinweis Alternativ können Sie die im VeeamHub GitHub Repository bereitgestellten CloudFormation Vorlagen verwenden, um einen IAM-Benutzer und einen S3-Bucket für dieses Muster zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3. 2. Wenn Sie noch keinen vorhandenen S3-Bucket als Zielspeicher haben, wählen Sie Bucket erstellen und geben Sie einen Bucket-Namen, eine AWS-Region und Bucket-Einstellungen an. • Wir empfehlen Ihnen, die Option Block Public Access für den S3-Bucket zu aktivieren und die Zugriffs- und Benutzerberechtigungsrichtlinien einzurichten, um die Anforderungen Ihrer Organisation zu erfüllen. Ein Beispiel finden Sie in der Amazon S3-Dokumentation. • Wir empfehlen Ihnen, die S3-Objektsperre zu aktivieren, auch wenn Sie sie nicht sofort verwenden möchten. Diese Einstellung kann nur zum Zeitpunkt der Erstellung des S3-Buckets aktiviert werden.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Erstellen eines Buckets in der Amazon S3-Dokumentation.	

Hinzufügen von Amazon S3 und S3 Glacier Flexible Retrieval (oder S3 Glacier Deep Archive) zu Veeam Backup & Replication

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Assistenten für das neue Objekt-Repository.	Bevor Sie die Objektspeicher- und Aufskalierungs-Backup-Repositorys in Veeam einrichten, müssen Sie die Amazon S3- und Amazon S3-Glacier-Speicher-Repositorys hinzufügen, die Sie für die Kapazitäts- und Archivstufen verwenden möchten. Im nächsten Epic verbinden Sie diese Speicher-Repositorys mit Ihrem Scale-Out-Backup-Repository. 1. Öffnen Sie in der Veeam-Konsole die Ansicht Backup-Infrastruktur. 2. Wählen Sie im Bestandsbereich den Knoten Backup-Repositorys und dann Repository hinzufügen aus. 3. Wählen Sie im Dialogfeld Backup-Repository hinzufügen die Option	AWS-Administrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Objektspeicher , Amazon S3 aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Amazon S3-Speicher für die Kapazitätsebene hinzu.	1. Wählen Sie im Dialogfeld Amazon Cloud Storage Services Amazon S3 aus. 2. Geben Sie im Schritt Name des Assistenten den Objektspeichernamen und eine kurze Beschreibung an, z. B. das Ersteller- und Erstellungsdatum. 3. Geben Sie im Schritt Konto des Assistenten das Objektspeicherkonto an. • Wählen Sie für Anmeldeinformationen den IAM-Benutzer aus, den Sie im ersten Epic erstellt haben, um auf Ihren Amazon S3-Objektspeicher zuzugreifen. • Wählen Sie für AWS-Region die AWS-Region aus, in der sich der Amazon S3-Bucket befindet. 4. Geben Sie im Schritt Bucket des Assistenten Einstellungen für den Objektspeicher an. • Wählen Sie für Rechenzentrumsregion die AWS-Region aus, in der sich der Amazon S3-Bucket befindet.	AWS-Administrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie für Bucket den S3-Bucket aus, den Sie im ersten Epic erstellt haben. • Erstellen Sie für Ordner einen Cloud-Ordner, dem Sie Ihr Objektspeicher-Repository zuordnen möchten, oder wählen Sie ihn aus. • Wenn Sie Unverände rlichkeit aktivieren möchten, wählen Sie Letzte Backups für X Tage unveränderlich machen und legen Sie den Zeitraum fest, in dem Ihre Backups gesperrt werden sollen. Beachten Sie, dass die Aktivierung von Unveränderlichkeit aufgrund der erhöhten Anzahl von API-Aufrufen von Veeam an Amazon S3 zu höheren Kosten führt. 5. Überprüfen Sie im Schritt Zusammenfassung des Assistenten die Konfigura tionsinformationen und wählen Sie dann Fertig stellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie S3-Glacier-Speicher für die Archivstufe hinzu.	Wenn Sie eine Archivstufe erstellen möchten, verwenden Sie die im Abschnitt Zusätzliche Informationen beschriebenen IAM-Berechtigungen. 1. Starten Sie den Assistenten für das neue Objekt-Repository wie zuvor beschrieben. 2. Wählen Sie im Dialogfeld Amazon Cloud Storage Services Amazon S3 Glacier aus. 3. Geben Sie im Schritt Name des Assistenten den Objektspeichernamen und eine kurze Beschreibung an, z. B. das Ersteller- und Erstellungsdatum. 4. Geben Sie im Schritt Konto des Assistenten das Objektspeicherkonto an. • Wählen Sie für Anmeldeinformationen den IAM-Benutzer aus, den Sie im ersten Epic erstellt haben, um auf Ihren Amazon S3-Glacier-Objektspeicher zuzugreifen. • Wählen Sie für AWS-Region die AWS-Region aus, in der sich der	AWS-Administrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon S3-Bucket befindet. 5. Geben Sie im Schritt Bucket des Assistenten Einstellungen für den Objektspeicher an. • Wählen Sie für Rechenzentrumsregion die AWS-Region aus. • Wählen Sie für Bucket einen S3-Bucket aus, in dem Ihre Sicherungsdaten gespeichert werden sollen. Dies kann derselbe Bucket sein, den Sie für die Kapazitätsstufe verwendet haben. • Erstellen oder wählen Sie für Ordner einen Cloud-Ordner aus, dem Sie Ihr Objektspeicher-Repository zuordnen möchten. • Wenn Sie Unveränderlichkeit aktivieren möchten, wählen Sie Letzte Backups für die gesamte Dauer ihrer Aufbewahrungsrichtlinie unveränderlich machen aus. Beachten Sie, dass die Aktivierung von Unveränderlichkeit aufgrund der erhöhten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anzahl von API-Aufrufen von Veeam an Amazon S3 zu höheren Kosten führt. • Wenn Sie S3 Glacier Deep Archive als Archivspeicherklasse verwenden möchten, wählen Sie Deep Archive Storage Class verwenden aus. 6. Konfigurieren Sie im Schritt Proxy Appliance des Assistenten die zusätzlic he Instance, die zum Übertragen der Daten von Amazon S3 zu Amazon S3 Glacier verwendet wird. Sie können die Standarde instellungen verwenden oder jede Einstellung manuell konfigurieren. So konfigurieren Sie die Einstellungen manuell: • Wählen Sie Anpassen aus. • Wählen Sie für den EC2-Instance-Typ den Instance-Typ für die Proxy-Appliance aus, basierend auf Ihren Geschwindigkeits- und Kostenanforderungen für die Übertragung der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sicherungsdateien auf die Archivebene Ihres Scale-Out-Backup-Repositorys. • Wählen Sie für Amazon VPC die VPC für die Ziel-Instance aus. • Wählen Sie für Subnetz das Subnetz für die Proxy-Appliance aus. • Wählen Sie für Sicherheitsgruppe die Sicherheitsgruppe aus, die der Proxy-Appliance zugeordnet werden soll. • Geben Sie für Umleitungsport den TCP-Port für Weiterleitungsanforderungen zwischen der Proxy-Appliance und den Komponenten der Backup-Infrastruktur an. • Wählen Sie OK, um Ihre Einstellungen zu bestätigen. 7. Überprüfen Sie im Schritt Zusammenfassung des Assistenten die Konfigurationsinformationen und wählen Sie dann Fertig stellen aus.	

Hinzufügen von Scale-Out-Backup-Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Assistenten für das neue Scale-Out-Backup-Repository.	1. Öffnen Sie in der Veeam-Konsole die Ansicht Backup-Infrastruktur. 2. Wählen Sie im Bestandsbereich Aufskalierungs-Repositorys und dann Aufskalierungs-Repository hinzufügen aus.	App-Eigentümer, AWS-Systemadministrator
Fügen Sie ein Scale-Out-Backup-Repository hinzu und konfigurieren Sie Kapazitäts- und Archivstufen.	1. Geben Sie im Schritt Name des Assistenten den Namen und eine kurze Beschreibung des Scale-Out-Backup-Repositorys an. 2. Fügen Sie bei Bedarf Leistungserweiterungen hinzu. Sie können auch Ihr vorhandenes lokales Veeam-Backup-Repository als Ihre Leistungsstufe verwenden. Ab Veeam Version 12 können Sie einen S3-Bucket als Leistungserweiterung für direct-to-object (DTO)-Backups hinzufügen, wodurch eine lokale Leistungsstufe umgangen wird. 3. Wählen Sie Erweitert und geben Sie zusätzliche Optionen für das Aufskalie	App-Eigentümer, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rungs-Backup-Repository an. • Wählen Sie Sicherungsdateien pro Computer verwenden, um für jeden Computer eine separate Sicherungsdatei zu erstellen und diese Dateien gleichzeitig in das Sicherungs-Repository in mehreren Streams zu schreiben. Diese Option wird für eine bessere Speicher- und Rechenressourcennutzung empfohlen. • Wählen Sie Vollständige Sicherung durchführen, wenn der erforderliche Umfang offline ist, um eine vollständige Sicherungsdatei zu erstellen, falls ein Umfang, der Wiederherstellungspunkte für eine inkrementelle Sicherung enthält, offline geht. Diese Option benötigt freien Speicherplatz im Scale-Out-Backup-Repository, um eine vollständige Sicherungsdatei zu hosten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Geben Sie im Schritt Richtlinie des Assistent en die Backup-Platzierung srichtlinie für das Repositor y an. • Wählen Sie Datenlokalität aus, um vollständige und inkrementelle Sicherung sdateien zu speichern, die zu derselben Kette gehören, und zwar in gleichem Umfang. Sie können Dateien, die zu einer neuen Sicherungskette gehören, in derselben oder in einer anderen Leistungs stufe speichern (es sei denn, Sie verwenden eine deduplizierende Speicher-Appliance als Leistungserweiterung). • Wählen Sie Leistung, um vollständige und inkrementelle Sicherung sdateien in unterschi edlichen Leistungs bereichen zu speichern . Diese Option erfordert eine schnelle und zuverlässige Netzwerkv erbindung. Wenn Sie Leistung wählen, können Sie die Arten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von Sicherungsdateien einschränken, die bei jeder Leistungserweiterung gespeichert werden sollen. Sie können beispielsweise vollständige Sicherungsdateien in einem Umfang und in anderen Umfang inkrementelle Sicherungsdateien speichern. So wählen Sie Dateitypen aus: • Wählen Sie Anpassen aus. • Wählen Sie im Dialogfeld Einstellungen für die Backup-Platzierung eine Leistungserweiterung und dann Bearbeiten aus. • Wählen Sie den Typ der Sicherungsdateien aus, die Sie in dem Umfang speichern möchten. 5. Konfigurieren Sie im Schritt Kapazitätsebene des Assistenten die langfristige Speicherebene, die Sie an das Scale-Out-Backup-Repository anfügen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie Scale-Out -Backup-Repository-Kapazität mit Objektspeicher erweitern aus. Wählen Sie für das Objektspeicher-Repository den Amazon S3-Speicher für die Kapazitätsstufe aus, die Sie im vorherigen Epi hinzugefügt haben. • Wählen Sie Fenster, um ein Zeitfenster für das Verschieben oder Kopieren von Daten auszuwählen. • Wählen Sie Backups in den Objektspeicher kopieren aus, sobald sie erstellt wurden, um alle oder nur kürzlich erstellten Backup-Dateien bis zum Kapazitätsumfang zu kopieren. • Wählen Sie Sicherungen in den Objektspeicher verschieben, wenn sie aus dem Fenster für betriebliche Wiederherstellungen auslaufen, um inaktive Sicherungsketten in den Kapazitätsbereich zu übertragen. Geben Sie im Feld Sicherung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sdateien älter als X Tage verschieben eine Dauer an, nach der Sicherung sdateien ausgelage rt werden sollen. (Um inaktive Sicherungsketten an dem Tag auszulage rn, an dem sie erstellt wurden, geben Sie 0 Tage an.) Sie können auch Überschreiben wählen, um Sicherung sdateien früher zu verschieben, wenn das Scale-Out-Sicherungs-Repository einen von Ihnen angegebenen Schwellenwert erreicht hat. • Wählen Sie In Objektspe icher hochgeladene Daten verschlüsseln und geben Sie ein Passwort an, um alle Daten und ihre Metadaten zum Auslagern zu verschlüs seln. Wählen Sie Passwörter hinzufüge n oder verwalten, um ein neues Passwort anzugeben. 6. Konfigurieren Sie im Schritt Archivstufe des Assistent en die Archivspeicherstuf	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e, die Sie an das Scale-Out-Backup-Repository anfügen möchten. (Dieser Schritt wird nicht angezeigt, wenn Sie das Hinzufügen von Amazon S3-Glacier-Speicher übersprungen haben.) • Wählen Sie Vollständige GFS-Backups im Objektspeicher archivieren aus. Wählen Sie für das Objektspeicher-Repository den Amazon S3-Glacier-Speicher aus, den Sie im vorherigen Epos hinzugefügt haben. • Wählen Sie für GFS-Backups archivieren, die älter als N Tage sind, ein Zeitfenster für das Verschieben von Dateien in den Archivumfang aus. (Um inaktive Sicherungsketten an dem Tag zu archivieren, an dem sie erstellt wurden, geben Sie 0 Tage an.) 7. Überprüfen Sie im Schritt Zusammenfassung des Assistenten die Konfiguration des Scale-Out-Backup-Repositorys und wählen Sie dann Fertig stellen aus.	

Zugehörige Ressourcen

- Erstellen eines IAM-Benutzers in Ihrem AWS-Konto (IAM-Dokumentation)
- Erstellen eines Buckets (Amazon S3-Dokumentation)
- Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher (Amazon S3-Dokumentation)
- Verwenden der S3-Objektsperre (Amazon S3-Dokumentation)
- Technische Dokumentation von Veeam
- So erstellen Sie eine sichere IAM-Richtlinie für die Verbindung mit S3 Object Storage (Veeam-Dokumentation)

Zusätzliche Informationen

In den folgenden Abschnitten finden Sie Beispiele für IAM-Richtlinien, die Sie verwenden können, wenn Sie einen IAM-Benutzer im Abschnitt „Epics“ dieses Musters erstellen.

IAM-Richtlinie für Kapazitätsebene

Hinweis Ändern Sie den Namen der S3-Buckets in der Beispielrichtlinie von `<yourbucketname>` in den Namen des S3-Buckets, den Sie für Veeam-Kapazitätsstufen-Backups verwenden möchten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutObjectLegalHold",
                "s3:GetBucketVersioning",
                "s3:GetObjectLegalHold",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObject*",
                "s3:GetObject*",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObject*",
```

```
                "s3:DeleteObjectVersion",
                "s3:GetBucketLocation"

            ],
            "Resource": [
                "arn:aws:s3:::/*",
                "arn:aws:s3:::"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM-Richtlinie für Archivstufe

Beachten Sie, dass Sie den Namen der S3-Buckets in der Beispielrichtlinie von `<yourbucketname>` in den Namen des S3-Buckets ändern, den Sie für Backups auf Veeam-Archivebene verwenden möchten.

So verwenden Sie Ihre vorhandene VPC, Ihr Subnetz und Ihre Sicherheitsgruppen:

```
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
          "s3:DeleteObject",
          "s3:PutObject",
          "s3:GetObject",
          "s3:RestoreObject",
          "s3:ListBucket",
          "s3:AbortMultipartUpload",
          "s3:GetBucketVersioning",
```

```
          "s3:ListAllMyBuckets",
          "s3:GetBucketLocation",
          "s3:GetBucketObjectLockConfiguration",
          "s3:PutObjectRetention",
          "s3:GetObjectVersion",
          "s3:PutObjectLegalHold",
          "s3:GetObjectRetention",
          "s3:DeleteObjectVersion",
          "s3:ListBucketVersions",
          "ec2:DescribeInstances",
          "ec2:CreateKeyPair",
          "ec2:DescribeKeyPairs",
          "ec2:RunInstances",
          "ec2:DeleteKeyPair",
          "ec2:DescribeVpcAttribute",
          "ec2:CreateTags",
          "ec2:DescribeSubnets",
          "ec2:TerminateInstances",
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeImages",
          "ec2:DescribeVpcs"
        ],
        "Resource": "*"
      }
    ]
}
```

So erstellen Sie neue VPC-, Subnetz- und Sicherheitsgruppen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:GetObject",
        "s3:RestoreObject",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:GetBucketVersioning",
```

```
          "s3:ListAllMyBuckets",
          "s3:GetBucketLocation",
          "s3:GetBucketObjectLockConfiguration",
          "s3:PutObjectRetention",
          "s3:GetObjectVersion",
          "s3:PutObjectLegalHold",
          "s3:GetObjectRetention",
          "s3:DeleteObjectVersion",
          "s3:ListBucketVersions",
          "ec2:DescribeInstances",
          "ec2:CreateKeyPair",
          "ec2:DescribeKeyPairs",
          "ec2:RunInstances",
          "ec2:DeleteKeyPair",
          "ec2:DescribeVpcAttribute",
          "ec2:CreateTags",
          "ec2:DescribeSubnets",
          "ec2:TerminateInstances",
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeImages",
          "ec2:DescribeVpcs",
          "ec2:CreateVpc",
          "ec2:CreateSubnet",
          "ec2:DescribeAvailabilityZones",
          "ec2:CreateRoute",
          "ec2:CreateInternetGateway",
          "ec2:AttachInternetGateway",
          "ec2:ModifyVpcAttribute",
          "ec2:CreateSecurityGroup",
          "ec2:DeleteSecurityGroup",
          "ec2:AuthorizeSecurityGroupIngress",
          "ec2:AuthorizeSecurityGroupEgress",
          "ec2:DescribeRouteTables",
          "ec2:DescribeInstanceTypes"
        ],
        "Resource": "*"
      }
    ]
}
```

Konfiguration von Veritas NetBackup für VMware Cloud on AWS

Erstellt von Shubham Salani (AWS)

Umgebung: Produktion	Technologien: Speicher und Backup; Cloud-nativ	Arbeitslast: Alle anderen Workloads
AWS-Dienste: Amazon S3; AWS Transit Gateway; Amazon VPC; Amazon EBS		

Übersicht

> Hinweis: Seit dem 30. April 2024 wird VMware Cloud on AWS nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS-Vertreter zu wenden.

Viele Unternehmen verwenden Veritas NetBackup als Backup- und Wiederherstellungslösung für ihre lokalen VMware vSphere-basierten Workloads. Sobald Unternehmen ihre Workloads auf softwaredefinierte Rechenzentren (SDDCs) in der Infrastruktur von VMware Cloud on Amazon Web Services (AWS) migriert haben, gibt es kein klares lift-and-shift Verfahren für die Integration. NetBackup Dieses Muster beschreibt, wie Sie Veritas NetBackup in Ihrem AWS-Konto einrichten und es so konfigurieren können, dass die Workloads in Ihren VMware-SDDCs gesichert werden.

Dieses Muster enthält keine Anweisungen für die Migration Ihrer Workloads. Weitere Informationen finden Sie unter Migrieren von VMware SDDC zu VMware Cloud on AWS mithilfe von VMware HCX. Verwenden Sie beim Einrichten Ihrer Workloads für VMware Cloud on AWS einen ausgeweiteten Cluster (VMware-Dokumentation). In dieser Konfiguration erstreckt sich Ihr Cluster über zwei AWS Availability Zones innerhalb einer einzigen Region. Dies bietet hohe Verfügbarkeit und Resilienz für den Fall, dass eine der Availability Zones nicht verfügbar ist. Elastic DRS und ein vSAN-Witness-Host (VMware-Dokumentation) kopieren die Daten nahtlos in eine dritte Availability Zone, die als Fault Domain bezeichnet wird. Diese Paritätslösung kann Ihnen helfen, die Daten im Falle eines Fehlers wiederherzustellen. Da für diesen Ansatz drei Availability Zones erforderlich sind, sollten Sie bei der Auswahl einer AWS-Region für Ihre VMware Cloud-Umgebung sicherstellen, dass diese

über drei oder mehr Availability Zones verfügt. Weitere Informationen finden Sie unter Regionen und Availability Zones.

In diesem Muster hat jedes SDDC einen Backup-Host, bei dem es sich um einen Proxyserver handelt. Mithilfe von Amazon Elastic Compute Cloud (Amazon EC2) -Instances richten Sie den NetBackup Master- und Medienserver in einer separaten Virtual Private Cloud (VPC) ein, einen für jedes SDDC. Da elastische Netzwerkschnittstellen eine hohe Bandbreite und eine geringe Latenz bieten, verwenden Sie sie, um die Konnektivität zwischen den Backup-Hosts und ihren entsprechenden NetBackup Master- und Medienservern zu konfigurieren. Die EC2-Instances leiten die Backups an Amazon Elastic Block Store (Amazon EBS) -Volumes weiter, was der erste Backup-Punkt ist. Sie können AWS verwenden DataSync , um Ihre EBS-Volumes für die SDDCs zu synchronisieren.

Sie können auch AWS Transit Gateway und einen VPC-Schnittstellen-Endpunkt verwenden, um die EBS-Volumes mit einem anderen Speicherservice wie Amazon Simple Storage Service (Amazon S3) zu verbinden. Gemäß Ihrer Aufbewahrungsrichtlinie können Sie S3 Intelligent-Tiering S3 Glaciering-Speicherklassen verwenden, um Ihre Speicherkosten zu optimieren. Weitere Informationen finden Sie unter Verwenden von Amazon S3 S3-Speicherklassen (Amazon S3 S3-Dokumentation).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ihre VMware Cloud on AWS AWS-Umgebung verwendet einen ausgedehnten Cluster, der sich über zwei Availability Zones erstreckt.
- Der Backup-Host muss sich auf dem VMware Cloud on AWS AWS-SDDC befinden, das Zugriff auf den Datenspeicher hat, in dem die VMware Virtual Machine Disk File (VMDK) -Dateien bereitgestellt werden.
- HotAdd Der Transportmodus muss auf dem NetBackup Client aktiviert sein, um virtuelle Maschinen (VMs) zu sichern und wiederherzustellen, und er muss Wiederherstellungen von benutzergesteuerten Dateien und Ordnern ermöglichen.

Einschränkungen

- Der NetBackup Masterserver muss die DNS-Auflösung für eine private IP-Adresse für den vCenter-Backup-Host im SDDC verwenden.
- Die Hosts-Dateien auf dem NetBackup Masterserver und dem Backup-Host sollten Folgendes enthalten:

  - Die private IP-Adresse und der private DNS-Name des Masterservers
  - Die private IP-Adresse und der private DNS-Name des Backup-Hosts
- Wenn Sie VPC-Schnittstellen-Endpunkte für einen S3-Bucket konfigurieren, muss die SDDC Compute Gateway-Firewall so konfiguriert sein, dass HTTPS von einer Classless Inter-Domain Routing (CIDR) -Blockquelle zugelassen wird. Weitere Informationen finden Sie unter Zugreifen auf einen S3-Bucket mithilfe eines S3-Endpunkts (VMware-Dokumentation).
- VMware Cloud on AWS unterstützt die folgenden Funktionen von nicht NetBackup:
  - VM-Vorlagen sichern oder wiederherstellen
  - Verwenden des NetBackup vSphere Client (HTML5-Plug-In)
  - Sperren und Entsperren von VMs für Backups oder Wiederherstellungen
  - Backups können nicht in einem vSAN-Datenspeicher gespeichert werden
  - Netzwerkblockgerät (NBD), NBDSSL und SAN-Transportmodi

Produktversionen

- VMware Cloud on AWS SDDC Version 1.0 oder höher
- Veritas NetBackup Version 8.1.2 oder höher
- Linux-Version 6.8 oder höher
- VMware vSphere Version 6.0 oder höher

Architektur

Das folgende Diagramm zeigt die Konfiguration von NetBackup für VMware Cloud on AWS. Die NetBackup Master- und Medienserver werden in einer separaten VPC bereitgestellt und sind über elastische Netzwerkschnittstellen mit den Backup-Hosts in den SDDCs verbunden. Die NetBackup Master- und Medienserver speichern die Backups auf Amazon EBS-Volumes. Sie können optional zusätzlichen Speicher in Amazon S3 S3-Buckets konfigurieren, indem Sie AWS Transit Gateway und einen VPC-Endpunkt mit PrivateLink AWS-Schnittstelle verwenden.

Tools

AWS-Services und -Tools

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- AWS PrivateLink hilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren Virtual Private Clouds (VPCs) zu Services außerhalb der VPC herzustellen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Andere Dienste

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von Amazon Web Services (AWS) und VMware entwickelt wurde.
- NetBackup for VMware sichert und stellt die virtuellen VMware-Maschinen wieder her, die auf VMware ESXi-Hosts ausgeführt werden.

Epen

Konfigurieren Sie die Server NetBackup

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Firewall-Regeln.	Aktualisieren Sie die Firewallr egeln, um die Konnektivität zwischen dem VMware Cloud on AWS AWS-SDDC und den NetBackup Master- und Medienservern herzustellen. Gehen Sie wie folgt vor: 1. Melden Sie sich unter https://vmc.vmware.com/ bei VMware Cloud on AWS an	Netzwerkadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit die Option Gateway Firewall aus. 3. Wählen Sie auf der Seite Gateway Firewall die Option Compute Gateway aus. 4. Wählen Sie Regel HINZUFÜGEN und erstellen Sie dann eine neue Regel mit den erforderlichen Firewall-Port-Einstellungen. Weitere Informationen finden Sie unter Anforderungen an NetBackup Firewall-Ports (Veritas-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den NetBackup Master- und Medienserver.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon EC2 EC2-Konsole unter https://console.aws.amazon.com/ec2/ 2. Starten Sie eine EC2-Instance (Amazon EC2 EC2-Dokumentation) und verwenden Sie die folgenden Konfigurationsdetails: a. Wählen Sie für den NetBackup Master- und Medienserver das `NBU-Linux-GA-8-1-2-Setup-f032d23e-881b-4dee-ba70-b9ca3e915910-ami-072509a7ffc156938.4` Amazon Machine Image (AMI) aus. Dieses vorkonfigurierte AMI ist über den AWS Marketplace erhältlich. b. Wählen Sie einen Instanztyp aus. NetBackup empfiehlt `m5.2xlarge` für den Master- und Medienserver.	Cloud-Administrator, Backup-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Backup-Host für NetBackup.	1. Melden Sie sich unter https://vmc.vmware.com/ bei VMware Cloud on AWS an 2. Wählen Sie das SDDC aus. 3. Wählen Sie die Registerkarte „VCENTER öffnen“. Dadurch wird das SDDC vCenter geöffnet. 4. Notieren Sie sich den vollqualifizierten Domänennamen (FQDN) des Backup-Hosts. 5. Melden Sie sich bei der NetBackup Verwaltungskonsole an. Weitere Informationen finden Sie unter Bei der NetBackup Verwaltungskonsole anmelden (Veritas-Dokumentation). 6. Wählen Sie den Master- und den Medienserver und dann VMware Access Hosts aus. 7. Fügen Sie den FQDN des Backup-Hosts hinzu. 8. Wählen Sie Übernehmen und anschließend OK aus.	Cloud-Administrator, Backup-Administrator

(Optional) Amazon S3 S3-Speicher einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Speicher in Amazon S3.	1. Lesen Sie die Amazon S3 S3-Cloud-Speicheroptionen (Veritas-Dokumentation) und wählen Sie die passende Speicherklasse für Ihre Anforderungen aus. 2. Konfigurieren NetBackup Sie die Verwendung von Amazon S3 als Cloud-Speicher gemäß den Anweisungen unter Cloud-Speicher konfigurieren in NetBackup (Veritas-Dokumentation).	Cloud-Administrator, Allgemeine AWS

Zugehörige Ressourcen

AWS-Dokumentation

- Erstellen Sie einen VPC-Schnittstellen-Endpunkt (PrivateLink AWS-Dokumentation)

Veritas-Dokumentation

- NetBackup Anforderungen an den Firewall-Port

VMware-Dokumentation

- Stellen Sie eine VM anhand einer OVF-Vorlage in einer Inhaltsbibliothek bereit
- Datenübertragungsgebühren für VMware Cloud on AWS: Wie funktioniert das? (VMware-Blogbeitrag)
- VMware Cloud on AWS: Erweiterte Cluster

Kopieren Sie Daten mithilfe der AWS-CLI aus einem S3-Bucket in ein anderes Konto und eine andere Region

Erstellt von Appasaheb Bagali (AWS) und Purushotham G K (AWS)

Umgebung: Produktion	Technologien: Speicher und Backup; Cloud-nativ	AWS-Services: AWS CLI; AWS Identity and Access Management; Amazon S3

Übersicht

Dieses Muster beschreibt, wie Daten von einem Amazon Simple Storage Service (Amazon S3) - Bucket in einem AWS-Quellkonto zu einem Ziel-S3-Bucket in einem anderen AWS-Konto migriert werden, entweder in derselben AWS-Region oder in einer anderen Region.

Der Quell-S3-Bucket ermöglicht den Zugriff auf AWS Identity and Access Management (IAM) mithilfe einer angehängten Ressourcenrichtlinie. Ein Benutzer im Zielkonto muss eine Rolle übernehmen, die über `GetObject` Berechtigungen für den `PutObject` Quell-Bucket verfügt. Schließlich führen `copy` Sie `sync` Befehle aus, um Daten vom S3-Quell-Bucket in den S3-Ziel-Bucket zu übertragen.

Konten sind Eigentümer der Objekte, die sie in S3-Buckets hochladen. Wenn Sie Objekte zwischen Konten und Regionen kopieren, gewähren Sie dem Zielkonto das Eigentum an den kopierten Objekten. Sie können die Eigentümerschaft eines Objekts ändern, indem Sie dessen Zugriffskontrollliste (ACL) auf ändern`bucket-owner-full-control`. Es wird jedoch empfohlen, dem Zielkonto programmgesteuerte kontoübergreifende Berechtigungen zu gewähren, da es schwierig sein kann, ACLs für mehrere Objekte zu verwalten.

> Warnung: Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfrist igen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Die Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informati onen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Dieses Muster deckt eine einmalige Migration ab. Für Szenarien, die eine kontinuierliche und automatische Migration neuer Objekte von einem Quell-Bucket zu einem Ziel-Bucket erfordern, können Sie stattdessen die S3-Batch-Replikation verwenden, wie im Muster Kopieren von Daten aus einem S3-Bucket in ein anderes Konto und eine andere Region mithilfe von S3 Batch Replication beschrieben.

Voraussetzungen und Einschränkungen

- Zwei aktive AWS-Konten in derselben oder unterschiedlichen AWS-Regionen.
- Ein vorhandener S3-Bucket im Quellkonto.
- Wenn in Ihrem Amazon S3 S3-Quell- oder Ziel-Bucket die Standardverschlüsselung aktiviert ist, müssen Sie die Schlüsselberechtigungen für den AWS Key Management Service (AWS KMS) ändern. Weitere Informationen finden Sie im AWS-re:Post-Artikel zu diesem Thema.
- Vertrautheit mit kontoübergreifenden Berechtigungen

Architektur

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Bewährte Methoden

- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)
- Anwenden von Berechtigungen mit den geringsten Rechten (IAM-Dokumentation)

Epen

Erstellen Sie einen IAM-Benutzer und eine IAM-Rolle im AWS-Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen IAM-Benutzer und rufen Sie den Zugriffsschlüssel ab.	1. Melden Sie sich bei der AWS-Managementkonsole an und erstellen Sie einen IAM-Benutzer mit programmatischem Zugriff. Ausführliche Schritte finden Sie in der IAM-Dokumentation unter IAM-Benutzer erstellen. Es ist nicht erforderlich, Richtlinien für diesen Benutzer anzuhängen. 2. Generieren Sie einen Zugriffsschlüssel und einen geheimen Schlüssel für diesen Benutzer. Anweisungen finden Sie in der AWS-Dokumentation unter AWS-Konto und Zugriffsschlüssel.	AWS DevOps
Erstellen Sie eine identitätsbasierte IAM-Richtlinie.	Erstellen Sie eine identitätsbasierte IAM-Richtlinie, die mit den folgenden Berechtigungen benannt `S3MigrationPolicy` ist. Ausführliche Schritte finden Sie in der IAM-Dokumentation unter Erstellen von IAM-Richtlinien. `{`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "s3:ListBucket",
	  "s3:GetObject",
	  "s3:GetObjectTagging",
	  "s3:GetObjectVersion",
	  "s3:GetObjectVersionTagging"
	  ],
	  "Resource": [
	  "arn:aws:s3:::awsexamplesourcebucket",
	  "arn:aws:s3:::awsexamplesourcebucket/*"
	  ]
	  },
	  {
	  "Effect": "Allow",
	  "Action": [
	  "s3:ListBucket",
	  "s3:PutObject",
	  "s3:PutObjectAcl",</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"s3:PutObjectTaggi
	ng",
	
	"s3:GetObjectTaggi
	ng",
	
	"s3:GetObjectVersi
	on",
	
	"s3:GetObjectVersi
	onTagging"
	],
	"Resource":
	[
	
	"arn:aws:s3:::awse
	xampledestinationb
	ucket",
	
	"arn:aws:s3:::awse
	xampledestinationb
	ucket/*"
	]
	}
	]
	}</pre>
	Hinweis: Ändern Sie die Quell- und Ziel-Bucket-Namen entsprechend Ihrem Anwendungsfall.
	
	Diese identitätsbasierte Richtlinie ermöglicht es dem Benutzer, der diese Rolle übernimmt, auf den Quell-Bucket und den Ziel-Bucket zuzugreifen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Erstellen Sie eine IAM-Rolle , die `S3MigrationRole` nach der folgenden Vertrauen srichtlinie benannt ist, und hängen Sie dann die zuvor erstellte `S3Migrati onPolicy` an. Ausführliche Schritte finden Sie in der IAM-Dokumentation unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principa l": { "AWS": "arn:aws:iam::<des tination_account>: user/<user_name>" }, "Action": "sts:AssumeRole", "Conditio n": {} } ] }` Hinweis: Ändern Sie den Amazon-Ressourcennamen (ARN) der Ziel-IAM-Rolle oder	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Benutzernamen in der Vertrauensrichtlinie entsprechend Ihrem Anwendungsfall. Diese Vertrauensrichtlinie ermöglicht es dem neu erstellten IAM-Benutzer, zu übernehmen. `S3MigrationRole`	

Erstellen Sie die S3-Bucket-Richtlinie und fügen Sie sie dem Quellkonto hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine S3-Bucket-Richtlinie und fügen Sie sie an.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Quellkonto an und öffnen Sie die Amazon S3 S3-Konsole. Wählen Sie Ihren S3-Quell-Bucket und dann Permissions aus. Wählen Sie unter Bucket-Richtlinie die Option Bearbeiten aus und fügen Sie dann die folgende Bucket-Richtlinie ein. Wählen Sie Speichern. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "DelegateS3Access", "Effect": "Allow",`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Principa l": {"AWS": "arn:aws: iam::<destination_ account>:role/<Rol eName>"}, "Action": ["s3:ListBucket", "s3:GetObject", "s3:GetObjectTaggi ng", "s3:GetObjectVersi on", "s3:GetObjectVersi onTagging"], "Resource": ["arn:aws:s3:::awse xamplesourcebucket/ *", "arn:aws:s3:::awse xamplesourcebucket"] }] } Hinweis: Stellen Sie sicher, dass Sie die AWS-Konto-ID für das Zielkonto angeben und konfigurieren Sie die Bucket-Richtlinienvorlage gemäß Ihren Anforderungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Diese ressourcenbasierte Richtlinie ermöglicht der Zielrolle den `S3MigrationRole` Zugriff auf S3-Objekte im Quellkonto.	

Konfigurieren Sie den Ziel-S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Ziel-Bucket.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Zielkonto an, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann Create Bucket aus. Erstellen Sie einen S3-Bucket gemäß Ihren Anforderungen. Weitere Informationen finden Sie in der Amazon S3 S3-Dokumentation unter Bucket erstellen.	Cloud-Administrator

Kopieren Sie Daten in den Ziel-S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS CLI mit den neu erstellten Benutzeranmeldedaten.	1. Installieren Sie die neueste Version der AWS-CLI. Anweisungen finden Sie unter Installation oder Aktualisierung der neuesten Version der AWS-CLI in der AWS-CLI-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Führen Sie `$ aws configure` die CLI mit dem AWS-Zugriffsschlüssel des von Ihnen erstellten Benutzers aus und aktualisieren Sie sie. Weitere Informationen finden Sie unter Konfiguration und Einstellungen für Anmeldeinformationsdateien in der AWS-CLI-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie die S3-Migrationsrolle an.	1. Verwenden Sie die AWS-CLI, um Folgendes anzunehmen`S3MigrationRole` : `aws sts assume-role \ --role-arn "arn:aws:iam::<destination_account>:role/S3MigrationRole" \ --role-session-name AWSCLI-Session` Dieser Befehl gibt mehrere Informationen aus. Innerhalb des Anmeldeinformationsblocks benötigen Sie das `AccessKeyId SecretAccessKey` , und`SessionToken` . In diesem Beispiel werden die Umgebungsvariablen `RoleAccessKeyID RoleSecretKey` , und verwendet `RoleSessionToken` . Beachten Sie, dass der Zeitstempel des Ablaufdes in der UTC-Zeitzone liegt. Der Zeitstempel gibt an, wann die temporären Anmeldeinformationen der IAM-Rolle ablaufen. Wenn die temporären	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Anmeldeinformationen ablaufen, müssen Sie die `sts:AssumeRole` API erneut aufrufen.
	2. Erstellen Sie drei Umgebungsvariablen , um die IAM-Rolle zu übernehmen. Diese Umgebungsvariablen werden mit der folgenden Ausgabe gefüllt:
	`# Linux`
	`export AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`export AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`export AWS_SESSI ON_TOKEN=RoleSessi onToken`
	`# Windows`
	`set AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`set AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`set AWS_SESSI ON_TOKEN=RoleSessi onToken`
	3. Stellen Sie sicher, dass Sie die IAM-Rolle übernomme n haben, indem Sie den folgenden Befehl ausführen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws sts get-caller-identity` Weitere Informationen finden Sie im AWS Knowledge Center.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Kopieren und synchronisieren Sie Daten aus dem S3-Quell-Bucket in den S3-Ziel-Bucket.	Wenn Sie die Rolle übernommen haben, können `S3MigrationRole` Sie die Daten mit dem Befehl copy (cp) oder synchronize (sync) kopieren.
	
	Kopieren (Einzelheiten finden Sie in der AWS CLI Command Reference):
	
	`aws s3 cp s3:// DOC-EXAMPLE-BUCKET-SOURCE / \`
	`  s3:// DOC-EXAMPLE-BUCKET-TARGET / \`
	`  --recursive --source-region SOURCE-REGION-NAME --region  DESTINATION-REGION-NAME`
	
	Synchronisieren (Einzelheiten finden Sie in der AWS CLI Command Reference):
	
	`aws s3 sync s3://  DOC-EXAMPLE-BUCKET-SOURCE / \`
	`  s3:// DOC-EXAMPLE-BUCKET-TARGET / \`
	`  --source-region  SOURCE-REGION-NAME  --region DESTINATION-REGION-NAME`
		Cloud-Administrator

Fehlerbehebung

Problem	Lösung
Beim Aufrufen des `ListObjects` Vorgangs ist ein Fehler aufgetreten (`AccessDenied`): Zugriff verweigert	• Vergewissern Sie sich, dass Sie die Rolle übernommen haben`S3MigrationRole` . • Führen Sie `aws sts get-caller-identity` den Befehl aus, um die verwendete Rolle zu überprüfen. Wenn in der Ausgabe der ARN für nicht angezeigt wird`S3MigrationRole` , nehmen Sie die Rolle erneut an und versuchen Sie es erneut.

Zugehörige Ressourcen

- Einen S3-Bucket erstellen (Amazon S3 S3-Dokumentation)
- Amazon S3 S3-Bucket-Richtlinien und Benutzerrichtlinien (Amazon S3 S3-Dokumentation)
- IAM-Identitäten (Benutzer, Gruppen und Rollen) (IAM-Dokumentation)
- Befehl cp (AWS-CLI-Dokumentation)
- Sync-Befehl (AWS-CLI-Dokumentation)

Kopieren Sie Daten mithilfe von S3 Batch Replication von einem S3-Bucket in ein anderes Konto und eine andere Region

Erstellt von Appasaheb Bagali (AWS), Lakshmikanth B D (AWS), Purushotham G K (AWS), Shubham Harsora (AWS) und Suman Rajotia (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Speicher und Backup; Cloud-nativ	AWS-Services: Amazon S3; AWS Identity and Access Management

Übersicht

Dieses Muster erklärt, wie Sie Amazon Simple Storage Service (Amazon S3) Batch Replication verwenden können, um den Inhalt eines S3-Buckets automatisch und ohne manuelles Eingreifen in einen anderen S3-Bucket zu kopieren, nachdem Sie die Buckets eingerichtet haben. Die Quell- und Ziel-Buckets können sich im selben oder in unterschiedlichen Regionen befinden AWS-Konten .

Die S3-Stapelreplikation bietet Ihnen die Möglichkeit, Amazon S3 S3-Objekte zu replizieren, die vor der Einrichtung einer Replikationskonfiguration existierten, Objekte, die zuvor repliziert wurden, und Objekte, bei denen die Replikation fehlgeschlagen ist. Diese Methode verwendet einen S3 Batch Operations Job. Wenn der Job abgeschlossen ist, erhalten Sie einen Abschlussbericht.

Sie können S3 Batch Replication in Szenarien verwenden, die eine kontinuierliche und automatische Migration neuer Objekte von einem Quell-Bucket zu einem Ziel-Bucket erfordern. Für eine einmalige Migration können Sie stattdessen AWS Command Line Interface (AWS CLI) verwenden, wie im Muster Kopieren von Daten aus einem S3-Bucket in ein anderes Konto und eine andere Region beschrieben, indem Sie den verwenden AWS CLI.

Voraussetzungen und Einschränkungen

- Eine Quelle AWS-Konto.
- Ein Ziel AWS-Konto.
- Ein S3-Bucket im Quellkonto mit einigen Objekten (Dateien oder Ordner).
- Ein oder mehrere S3-Buckets im Zielkonto.
- Die S3-Versionierung ist für die Quell- und Ziel-Buckets aktiviert.

- AWS Identity and Access Management (IAM) -Berechtigungen zum Erstellen einer IAM-Richtlinie, einer IAM-Rolle und einer S3-Bucket-Richtlinie für die Quell- und Zielkonten.
- Die Amazon S3 S3-Lebenszyklusregeln sind deaktiviert, solange der S3-Batch-Replikationsauftrag aktiv ist. Dadurch wird die Parität zwischen den Quell- und Ziel-Buckets gewährleistet. Andernfalls ist der Ziel-Bucket möglicherweise kein exaktes Replikat des Quell-Buckets.

Architektur

Tools

AWS Dienstleistungen

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

Im folgenden Video von AWS re:Invent 2022 werden bewährte Methoden für die Verwendung der Amazon S3 S3-Replikation zur Einhaltung gesetzlicher Vorschriften, zum Datenschutz und zur Steigerung der Anwendungsleistung beschrieben.

Epen

Erstellen Sie eine IAM-Richtlinie und eine Rolle für die kontenübergreifende Replikation im Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie für die kontenübergreifende Replikation.	Im AWS Quellkonto: 1. Öffnen Sie die IAM-Konsole.	Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erstellen Sie eine neue IAM-Richtlinie. 3. Wählen Sie im Bereich Policy-Editor die Option JSON aus und fügen Sie den folgenden Code ein. `{ "Version": "2012-10-17", "Statement": [{ "Sid": "GetSourceBucketConfiguration", "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetBucketLocation", "s3:GetBucketAcl", "s3:GetReplicationConfiguration", "s3:GetObjectVersionForReplication", "s3:GetObjectVersionAcl", "s3:GetObjectVersionTagging"],`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Resource": ["arn:aws:s3:::source-bucket-name", "arn:aws:s3:::source-bucket-name/*"] }, { "Sid": "ReplicateToDestinationBuckets", "Effect": "Allow", "Action": ["s3:List*", "s3:*Object", "s3:ReplicateObject", "s3:ReplicateDelete", "s3:ReplicateTags"], "Resource": ["arn:aws:s3:::destination-bucket-name/*", "arn:aws:s3:::destination-bucket-name/*"]	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> },
	        {
	            "Sid":
	"PermissionToOverr
	ideBucketOwner",
	            "Effect":
	"Allow",
	            "Action":
	[
	
	"s3:ObjectOwnerOve
	rrideToBucketOwner"
	            ],
	            "Resource
	": [
	
	"arn:aws:s3:::dest
	ination-bucket-nam
	e/*",
	
	"arn:aws:s3:::dest
	ination-bucket-nam
	e/*"
	            ]
	        }
	    ]
	}</pre>
	Diese Richtlinie umfasst drei Aussagen:
	• `GetSourceBucketConfiguration` bietet Zugriff auf die Replikationskonfiguration und die Objektversion für die Replikation im Quell-Bucket.
	• `ReplicateToDestina`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`tionBuckets` bietet Zugriff auf die Replikation in den Ziel-Bucket. Sie können mehrere Ziel-Buckets im Array angeben. • `PermissionToOverrideBucketOwner` bietet Zugriff auf, `ObjectOwnerOverrideToBucketOwner` sodass der Ziel-Bucket Eigentümer der Objekte im Zielkonto ist, die aus dem Quellkonto repliziert wurden. 4. Wählen Sie Weiter, geben Sie einen Richtliniennamen wie ein`cross-account-bucket-replication-policy`, und wählen Sie dann Richtlinie erstellen aus. Weitere Informationen finden Sie in der IAM-Dokumentation unter IAM-Richtlinien erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für die kontenübergreifende Replikation.	Im AWS Quellkonto: 1. Erstellen Sie auf der IAM-Konsole eine IAM-Rolle mit den folgenden Informationen: a. Wählen Sie für Vertrauenswürdigen Entitätstyp die Option AWS-Service aus. b. Wählen Sie als Service S3 aus. c. Wählen Sie für den Anwendungsfall S3 Batch Operations. d. Wählen Sie die Richtlinie aus, die Sie im vorherigen Schritt erstellt haben. 2. Geben Sie einen Rollennamen wie cross-account-bucket-replication -role ein und wählen Sie dann Create role aus. Weitere Informationen finden Sie in der IAM-Dokumentation unter IAM-Rollen erstellen.	Cloud-Administrator, AWS-Administrator

Erstellen Sie eine Replikationsregel im Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsregel für den Quell-Bucket im Quellkonto.	Im AWS Quellkonto: 1. Öffnen Sie die Amazon S3-Konsole. 2. Navigieren Sie zum Quell-Bucket und wählen Sie den Tab Management aus. 3. Erstellen Sie eine Replikationsregel mit der folgenden Konfiguration: a. Geben Sie einen Regelnamen an, `s3-replication-rule` z. B. b. Wählen Sie für Status die Option Enabled. c. Wählen Sie unter Regelbereich die Option Gilt für alle Objekte im Bucket aus. d. Wählen Sie für Ziel die Option Spezifizieren Sie einen Bucket in einem anderen Konto aus und geben Sie dann die AWS-Konto Zielnummer und den Bucket-Namen ein. e. Wählen Sie die Option, um den Eigentümer des Objekts auf den Besitzer	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Ziel-Buckets zu ändern. f. Wählen Sie für die IAM-Rolle die Rolle aus, die Sie zuvor im Quellkonto erstellt haben. g. Wählen Sie für Zusätzliche Replikationsoptionen alle verfügbaren Optionen aus. Diese bieten die Möglichkeit, Inhalte schnell zu replizieren, den Fortschritt der Replikation anhand von CloudWatch Amazon-Metriken zu überwachen, Löschmarkierungen zu replizieren und Metadatenänderungen zu replizieren. h. Wählen Sie Speichern. 4. Wenn Sie mehrere Ziel-Buckets haben, erstellen Sie zusätzliche Replikationsregeln. Weitere Informationen finden Sie in der Amazon S3 S3-Dokumentation unter Konfiguration der Replikation, wenn Quell- und Ziel-Buck	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ets unterschiedlichen Konten gehören.	

Wenden Sie eine Bucket-Richtlinie auf den Ziel-Bucket an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie eine Bucket-Richtlinie auf den Ziel-Bucket an.	Dieser Schritt muss für jeden Ziel-Bucket einzeln in den AWS Zielkonten ausgeführt werden. Im AWS Zielkonto: 1. Öffnen Sie die IAM-Konsole, navigieren Sie zum Ziel-Bucket und wählen Sie den Tab Permissions aus. 2. Bearbeiten Sie die Bucket-Richtlinie, indem Sie den folgenden JSON-Code angeben, und speichern Sie die Richtlinie: `{ "Version": "2012-10-17", "Id": "PolicyForDestinationBucket", "Statement": [ { "Sid": "Permissions on objects and buckets", "Effect": "Allow",`	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"Principa
	l": {
	"AWS":
	"arn:aws:iam::Sour
	ceAWSAccountNumber
	:role/IAM-Role-cre
	ated-in-step1-in-s
	ource-account"
	},
	"Action": [
	"s3:List*",
	"s3:GetBucketVersi
	oning",
	"s3:PutBucketVersi
	oning",
	"s3:ReplicateDelete",
	"s3:ReplicateObject"
	],
	"Resource":
	[
	"arn:aws:s3:::dest
	ination-bucket",
	"arn:aws:s3:::dest
	ination-bucket/*"
	]
	},
	{
	"Sid":
	"Permission to
	override bucket owner",
	"Effect":
	"Allow",
	"Principa
	l": {	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"AWS":
	"arn:aws:iam::SourceAWSAccountNumber:role/IAM-Role-created-in-step1-in-source-account"
	},
	"Action":
	"s3:ObjectOwnerOverrideToBucketOwner",
	"Resource": "arn:aws:s3:::destination-bucket/*"
	}
	]
	}</pre> Diese Richtlinie umfasst zwei Aussagen:
	• `Permissions on objects and bucketsgibt` an, dass der Ziel-Bucket Inhalte basierend auf der im Quellkonto definierten Rolle replizieren kann. Die Rolle stellt Berechtigungen für den Quell-Bucket bereit.
	• `Permission to override bucket ownergibt` an, dass der Ziel-Bucket berechtigt ist, die Inhaberschaft des Quellkontos außer Kraft zu setzen.	

Testen Sie die kontoübergreifende Amazon S3 S3-Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Replikation ordnungsgemäß funktioniert.	1. Fügen Sie dem Quell-Bucket ein Objekt hinzu. 2. Stellen Sie sicher, dass das neue Objekt in den S3-Buckets der Zielkonten erscheint. 3. CloudWatch Metriken anzeigen: a. Wählen Sie im Quell-Bucket die Registerkarte Metriken aus. b. Wählen Sie im Abschnitt Replikationsmetriken eine Replikationsregel aus. c. Wählen Sie Display charts (Diagramme anzeigen). Die Diagramme geben den Status der Replikation wieder, indem sie die Vorgänge, deren Replikation noch aussteht, die Replikationslatenz und die zur Replikation anstehenden Byte anzeigen. Weitere Informationen finden Sie unter Überwachen von Metriken mit Amazon	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudWatch in der Amazon S3 S3-Dokumentation.	

Zugehörige Ressourcen

- Wann verwende ich IAM? (IAM-Dokumentation)
- So funktioniert IAM (IAM-Dokumentation)
- IAM-Rollen erstellen (IAM-Dokumentation)
- IAM-Richtlinien erstellen (IAM-Dokumentation)
- Überblick über die Zugriffsverwaltung: Berechtigungen und Richtlinien (IAM-Dokumentation)
- Amazon S3 S3-Buckets erstellen, konfigurieren und damit arbeiten (Amazon S3 S3-Dokumentation)
- Objekte in Amazon S3 hochladen, herunterladen und mit ihnen arbeiten (Amazon S3 S3-Dokumentation)
- Objekte replizieren (Amazon S3 S3-Dokumentation)

Migrieren von Daten aus einer lokalen Hadoop-Umgebung zu Amazon S3 mithilfe von DistCp mit AWS PrivateLink für Amazon S3

Erstellt von Jason Owens (AWS), Andres Cantor (AWS), Klostein (AWS), Bruno RochaSpeed und Sam Schmidt (AWS)

Umgebung: Produktion	Quelle: Hadoop	Ziel: Beliebiges
R-Typ: Plattformwechsel	Workload: Open-Source	Technologien: Speicher und Backup; Analytik
AWS-Services: Amazon S3; Amazon EMR		

Übersicht

Dieses Muster zeigt, wie nahezu jede Datenmenge von einer On-Premises-Apache-Hadoop-Umgebung in die Amazon Web Services (AWS) Cloud migriert wird, indem das Apache-Open-Source-Tool DistCp mit AWS PrivateLink für Amazon Simple Storage Service (Amazon S3) verwendet wird. Anstatt das öffentliche Internet oder eine Proxy-Lösung zum Migrieren von Daten zu verwenden, können Sie AWS PrivateLink für Amazon S3 verwenden, um Daten über eine private Netzwerkverbindung zwischen Ihrem On-Premises-Rechenzentrum und einer Amazon Virtual Private Cloud (Amazon VPC) zu Amazon S3 zu migrieren. Wenn Sie DNS-Einträge in Amazon Route 53 verwenden oder Einträge in der Datei /etc/hosts in allen Knoten Ihres lokalen Hadoop-Clusters hinzufügen, werden Sie automatisch zum richtigen Schnittstellenendpunkt weitergeleitet.

Dieses Handbuch enthält Anweisungen zur Verwendung von DistCp für die Migration von Daten in die AWS Cloud. DistCp ist das am häufigsten verwendete Tool, aber andere Migrationstools sind verfügbar. Sie können beispielsweise Offline-AWS-Tools wie AWS Snowball oder AWS Snowmobile oder Online-AWS-Tools wie AWS Storage Gateway oder AWS DataSync verwenden. Darüber hinaus können Sie andere Open-Source-Tools wie Apache NiFi verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einer privaten Netzwerkverbindung zwischen Ihrem On-Premises-Rechenzentrum und der AWS Cloud
- Hadoop , On-Premises mit installiert DistCp
- Ein Hadoop-Benutzer mit Zugriff auf die Migrationsdaten im Hadoop Distributed File System (HDFS)
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Berechtigungen zum Ablegen von Objekten in einen S3-Bucket

Einschränkungen

Virtual Private Cloud (VPC)-Einschränkungen gelten für AWS PrivateLink für Amazon S3. Weitere Informationen finden Sie unter Eigenschaften und Einschränkungen von Schnittstellenendpunkten und AWS- PrivateLink Kontingente (AWS- PrivateLink Dokumentation).

AWS PrivateLink für Amazon S3 unterstützt Folgendes nicht:

- Endpunkte für den Federal Information Processing Standard (FIPS).
- Website-Endpunkte
- Globale Legacy-Endpunkte

Architektur

Quelltechnologie-Stack

- Hadoop-Cluster mit DistCp installiertem

Zieltechnologie-Stack

- Amazon S3
- Amazon VPC

Zielarchitektur

Das Diagramm zeigt, wie der Hadoop-Administrator verwendet, DistCp um Daten über eine private Netzwerkverbindung, z. B. AWS Direct Connect, über einen Amazon S3-Schnittstellenendpunkt aus einer On-Premises-Umgebung nach Amazon S3 zu kopieren.

Tools

AWS-Services

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie steuern, wer authentifiziert und zur Nutzung autorisiert ist.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, bietet jedoch die Vorteile der skalierbaren Infrastruktur von AWS.

Andere Tools

- Apache Hadoop DistCp (verteilte Kopie) ist ein Tool, das zum Kopieren großer Cluster und Intra-Cluster verwendet wird. DistCp verwendet Apache MapReduce für Verteilung, Fehlerbehandlung und Wiederherstellung sowie Berichterstattung.

Polen

Migrieren von Daten in die AWS Cloud

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Endpunkt für AWS PrivateLink für Amazon S3.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole . 2. Wählen Sie im Navigationsbereich Endpunkte und dann Endpunkt erstellen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie für Service category die Option AWS services. 4. Geben Sie im Suchfeld s3 ein und drücken Sie dann die Eingabetaste. 5. Wählen Sie in den Suchergebnissen den Servicenamen com.amazonaws.<your-aws-region>.s3 aus, wobei der Wert in der Spalte Typ Interface lautet. 6. Wählen Sie unter VPC Ihre VPC aus. Wählen Sie für Subnetze Ihre Subnetze aus. 7. Wählen oder erstellen Sie für Sicherheitsgruppe eine Sicherheitsgruppe, die TCP 443 zulässt. 8. Fügen Sie Tags basierend auf Ihren Anforderungen hinzu und wählen Sie dann Endpunkt erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Endpunkte und suchen Sie die DNS-Einträge.	1. Öffnen Sie die Amazon-VPC-Konsole, wählen Sie Endpunkte und dann den Endpunkt aus, den Sie zuvor erstellt haben. 2. Suchen Sie auf der Registerkarte Details den ersten DNS-Eintrag für DNS-Namen . Dies ist der regionale DNS-Eintrag. Wenn Sie diesen DNS-Namen verwenden, wechseln Anforderungen zwischen DNS-Einträgen, die für Availability Zones spezifisch sind. 3. Wählen Sie die Registerkarte Subnetze aus. Sie finden die Adresse der Elastic Network-Schnittstelle des Endpunkts in jeder Availability Zone.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Firewall-Regeln und Routing-K onfigurationen.	Um zu bestätigen, dass Ihre Firewall-Regeln geöffnet sind und dass Ihre Netzwerkk onfiguration korrekt eingerich tet ist, verwenden Sie Telnet, um den Endpunkt auf Port 443 zu testen. Beispielsweise:
	
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	
	`Trying 10.104.88.6...`
	
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	
	`...`
	
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	
	`Trying 10.104.71.141...`
	
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	
	Hinweis: Wenn Sie den regionalen Eintrag verwenden , zeigt ein erfolgreicher Test, dass das DNS zwischen den
		Netzwerkadministrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	beiden IP-Adressen wechselt, die Sie auf der Registerkarte Subnetze für den von Ihnen ausgewählten Endpunkt in der Amazon-VPC-Konsole sehen können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Namensauflösung.	Sie müssen die Namensauflösung so konfigurieren, dass Hadoop auf den Amazon S3-Schnittstellenendpunkt zugreifen kann. Sie können den Endpunktnamen selbst nicht verwenden. Stattdessen müssen Sie `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` oder auflösen `*.s3.<your-aws-region>.amazonaws.com` . Weitere Informationen zu dieser Benennungsbeschränkung finden Sie unter Einführung des Hadoop-S3A-Clients (Hadoop-Website). Wählen Sie eine der folgenden Konfigurationsoptionen aus: • Verwenden Sie On-Premises-DNS, um die private IP-Adresse des Endpunkts aufzulösen. Sie können das Verhalten für alle Buckets oder ausgewählten Buckets überschreiben. Weitere Informationen finden Sie unter „Option 2: Zugriff auf Amazon S3 mit Domain Name System Response Policy Zones (DNS RPZ)“	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in Sicherer Hybridzugriff auf Amazon S3 mit AWS PrivateLink (AWS-Blog beitrag). • Konfigurieren Sie On-Premises-DNS, um Datenverkehr bedingt an die eingehenden Resolver-Endpunkte in der VPC weiterzuleiten. Der Datenverkehr wird an Route 53 weitergeleitet. Weitere Informationen finden Sie unter „Option 3: Weiterleiten von DNS-Anfor derungen von On-Premis es mit Amazon Route 53 Resolver Inbound Endpoints “ in Sicherer Hybridzugriff auf Amazon S3 mit AWS PrivateLink (AWS-Blog beitrag). • Bearbeiten Sie die Datei / etc/hosts auf allen Knoten in Ihrem Hadoop-Cluster. Dies ist eine temporäre Testlösung und wird nicht für die Produktion empfohlen. Um die Datei /etc/hosts zu bearbeiten, fügen Sie einen Eintrag für `<your-bucket-name> .s3.<your-aws-regi on>.amazonaws.com`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder hinzus3.<your-aws-region>.amazonaws.com . Die Datei /etc/hosts kann nicht mehrere IP-Adressen für einen Eintrag haben. Sie müssen eine einzelne IP-Adresse aus einer der Availability Zones auswählen, die dann zu einem einzigen Fehlerpunkt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Authentifizierung für Amazon S3.	Um sich über Hadoop bei Amazon S3 zu authentifizieren, empfehlen wir Ihnen, temporäre Rollenanmeldeinformationen in die Hadoop-Umgebung zu exportieren. Weitere Informationen finden Sie unter Authentifizierung mit S3 (Hadoop-Website). Bei Aufträgen mit langer Laufzeit können Sie einen Benutzer erstellen und eine Richtlinie zuweisen, die über die Berechtigung verfügt, Daten nur in einen S3-Bucket zu übertragen. Der Zugriffsschlüssel und der geheime Schlüssel können auf Hadoop gespeichert werden, auf den nur der DistCp Auftrag selbst und der Hadoop-Administrator zugreifen können. Weitere Informationen zum Speichern von Secrets finden Sie unter Speichern von Secrets mit Hadoop-Anmeldeinformationsanbietern (Hadoop-Website). Weitere Informationen zu anderen Authentifizierungsmethoden finden Sie unter So rufen Sie Anmeldeinformationen einer IAM-Rolle für die Verwendung mit CLI-Zugriff auf ein AWS-Konto ab	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	in der Dokumentation für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On).
	
	Um temporäre Anmeldeinformationen zu verwenden, fügen Sie die temporären Anmeldeinformationen zu Ihrer -Anmeldeinformationsdatei hinzu oder führen Sie die folgenden Befehle aus, um die Anmeldeinformationen in Ihre Umgebung zu exportieren:
	
	`export AWS_SESSION_TOKEN=SECRET-SESSION-TOKEN`
	`export AWS_ACCESS_KEY_ID=SESSION-ACCESS-KEY`
	`export AWS_SECRET_ACCESS_KEY=SESSION-SECRET-KEY`
	
	Wenn Sie eine herkömmliche Kombination aus Zugriffsschlüssel und geheimem Schlüssel haben, führen Sie die folgenden Befehle aus:
	
	`export AWS_ACCESS_KEY_ID=my.aws.key`
	`export AWS_SECRET_ACCESS_KEY=my.secret.key`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Wenn Sie eine Kombination aus Zugriffss chlüssel und geheimem Schlüssel verwenden, ändern Sie den Anbieter der Anmeldeinformationen in den DistCp Befehlen von `"org.apache.hadoop .fs.s3a.TemporaryA WSCredentialsProvi der"` in `"org.apac he.hadoop.fs.s3a.S impleAWSCredential sProvider"` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie Daten mithilfe von DistCp.	Um zum Übertragen von Daten DistCp zu verwenden , führen Sie die folgenden Befehle aus: `hadoop distcp -Dfs.s3a.aws.credentials.provider=\"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" \ -Dfs.s3a.access.key="${AWS_ACCESS_KEY_ID}" \ -Dfs.s3a.secret.key="${AWS_SECRET_ACCESS_KEY}" \ -Dfs.s3a.session.token="${AWS_SESSION_TOKEN}" \ -Dfs.s3a.path.style.access=true \ -Dfs.s3a.connection.ssl.enabled=true \ -Dfs.s3a.endpoint=s3.<your-aws-region>.amazonaws.com \ hdfs:///user/root/ s3a://<your-bucket-name>` Hinweis: Die AWS-Region des Endpunkts wird nicht automatisch erkannt, wenn Sie den DistCp Befehl mit AWS PrivateLink für Amazon S3 verwenden. Hadoop 3.3.2 und	Migrationsingenieur, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	höhere Versionen beheben dieses Problem, indem sie die Option aktivieren, die AWS-Region des S3-Bucket s explizit festzulegen. Weitere Informationen finden Sie unter S3A zum Hinzufügen der Option fs.s3a.endpoint.re gion zum Festlegen der AWS-Region (Hadoop-Website). Weitere Informationen zu zusätzlichen S3A-Anbietern finden Sie unter Allgemein e S3A-Client-Konfiguration (Hadoop-Website). Wenn Sie beispielsweise die Verschlüs selung verwenden, können Sie je nach Art der Verschlüs selung der obigen Befehlsre ihe die folgende Option hinzufügen: `-Dfs.s3a.server-si de-encryption-algo rithm=AES-256 [or SSE-C or SSE-KMS]` Hinweis: Um den Schnittst ellenendpunkt mit S3A zu verwenden, müssen Sie einen DNS-Aliaseintrag für den regionalen S3-Namen (z. B. `s3.<your-aws-regio n>.amazonaws.com`) für den Schnittstellenendp	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unkt erstellen. Anweisung en finden Sie im Abschnitt Konfigurieren der Authentif izierung für Amazon S3. Diese Problemumgehung ist für Hadoop 3.3.2 und frühere Versionen erforderlich. Für zukünftige Versionen von S3A ist diese Problemumgehung nicht erforderlich. Wenn Sie Signaturprobleme mit Amazon S3 haben, fügen Sie eine Option zur Verwendung der Signatur Version 4 (SigV4) hinzu: `-Dmapreduce.map.java.opts="-Dcom.amazonaws.services.s3.enableV4=true"`	

Verwenden von CloudEndure für die Notfallwiederherstellung einer On-Premises-Datenbank

Erstellt von Nishant Jain (AWS) und Anuraag Deekonda (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Speicher und Backup; Modernisierung; Datenbanken

Übersicht

> Warnung: IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherhei tsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, dass Sie diesen Benutzern nur die Berechtigungen gewähren, die sie zur Ausführung der Aufgabe benötigen, und dass Sie diese Benutzer entfernen, wenn sie nicht mehr benötigt werden.

Dieses Muster verwendet CloudEndure Notfallwiederherstellung und den CloudEndure Failback-Client für die Notfallwiederherstellung (DR). Es richtet DR für einen On-Premises-Rechenzentrum-Host mithilfe einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance ein.

Sie müssen den CloudEndure Failback-Client für die Replikation von einer Nicht-Cloud- oder einer anderen Cloud-Infrastruktur in die Amazon Web Services (AWS) Cloud verwenden. Nachdem Ihr Notfallereignis vorbei ist, möchten Sie Ihre Maschinen ausfallen. CloudEndure bereitet Sie auf ein Failback vor, indem es die Richtung der Datenreplikation vom Zielcomputer zurück zum Quellcomputer umkehrt. Die - CloudEndure Benutzerkonsole behandelt die aktuell gestarteten Zielmaschinen als Quellmaschinen. Die Replikation wird von den von Ihnen ausgewählten Zielcomputern zurück in Ihre ursprüngliche Quellinfrastruktur umgekehrt.

> Wichtig: Im November 2021 hat AWS AWS Elastic Disaster Recovery eingeführt, das jetzt der empfohlene Service für die Notfallwiederherstellung in AWS ist.
>
> Nach dem erfolgreichen Start von Elastic Disaster Recovery beginnt AWS mit der Einschränkung der Verfügbarkeit von CloudEndure Disaster Recovery in allen AWS-Regionen, einschließlich

AWS GovCloud (US)-Regionen (AWS China-Regionen werden weiterhin unterstützt). Dies erfolgt nach dem folgenden Zeitplan:

1. 1. September 2023 – Kunden können sich nicht mehr für neue CloudEndure DR-Konten in einer AWS-Region registrieren (außer AWS-Regionen in China).
2. 1. Dezember 2023 – Neue CloudEndure DR-Agent-Installationen werden in keiner AWS-Regio n mehr unterstützt (mit Ausnahme von AWS-Regionen in China). Beachten Sie, dass Upgrades vorhandener Kundendienstmitarbeiter unterstützt werden.
3. 31. März 2024 – CloudEndure DR wird in allen AWS-Regionen eingestellt (außer AWS-Regio nen in China).
4. Alle aktualisierten Zeitpläne für CloudEndure Disaster Recovery EOL finden Sie in der CloudEndure Dokumentation .

Diese Veröffentlichung wird am 31. März 2024 entfernt. Wenn Sie es für ein laufendes Migration sprojekt benötigen, laden Sie die PDF-Datei herunter und speichern Sie sie mithilfe des PDF-Links , der sich unter dem Titel auf dieser Seite befindet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine On-Premises-Datenbank

Architektur

Quelltechnologie-Stack

- Eine Datenbank in einem On-Premises-Rechenzentrum

Zieltechnologie-Stack

- Eine Datenbank auf einer EC2-Instance (eine vollständige Liste der unterstützten Betriebssystemversionen finden Sie unter Häufig FAQs zu Amazon EC2)

Quell- und Zielnetzwerkarchitektur

Tools

- CloudEndure Notfallwiederherstellung – CloudEndure Notfallwiederherstellung reduziert Ausfallzeiten und Datenverlust, indem sie eine schnelle, zuverlässige Wiederherstellung physischer, virtueller und cloudbasierter Server in AWS ermöglicht. CloudEndure Notfallwiederherstellung repliziert Ihre Maschinen (einschließlich Betriebssystem, Systemstatuskonfiguration, Datenbanken, Anwendungen und Dateien) kontinuierlich in einen kostengünstigen Stagingbereich in Ihrem AWS-Zielkonto und Ihrer bevorzugten Region. Im Katastrophenfall können Sie CloudEndure Disaster Recovery anweisen, innerhalb weniger Minuten automatisch Tausende von Maschinen in ihrem vollständig bereitgestellten Zustand zu starten.

Polen

Abonnieren von CloudEndure Notfallwiederherstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie CloudEndure Disaster Recovery.	CloudEndure Notfallwiederherstellung ist im AWS Marketplace verfügbar.	Allgemeines AWS
Erstellen Sie ein - CloudEndure Konto.	Registrieren Sie sich für CloudEndure und erstellen Sie ein -Konto. Bestätigen Sie dann per E-Mail das Abonnement.	Allgemeines AWS
Legen Sie das Kontopasswort fest und akzeptieren Sie die Allgemeinen Geschäftsbedingungen.	Passwörter müssen mindestens acht Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.	Allgemeines AWS

Erstellen eines CloudEndure Projekts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der -CloudEndure Benutzerkonsole an.	Melden Sie sich in der CloudEndure -Benutzer konsole mit den Anmeldein formationen an, die Sie im vorherigen Schritt erstellt haben.	CloudEndure Administrator
Erstellt ein neues Projekt.	Wählen Sie in der oberen linken Ecke der Konsole die Schaltfläche Plus (+), um ein Projekt zu erstellen. Wählen Sie Notfallwiederherst ellung als Projekttyp aus. Sie können eine Lizenz über AWS Marketplace erwerben.	CloudEndure Administrator

Erstellen und Verwenden von AWS-Anmeldeinformationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richt linie für die CloudEndure Lösung.	Die AWS Identity and Access Management (IAM)-Richtlinie, die Sie für die Ausführung der CloudEndure Lösung erstellen müssen, basiert auf einer vordefinierten CloudEndure Richtlinie . Diese CloudEndure Richtlinie enthält die erforderl ichen Berechtigungen für die Verwendung von AWS als Zielinfrastruktur.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen neuen IAM-Benutzer und generieren Sie AWS-Anmeldeinformationen.	Um die erforderlichen AWS-Anmeldeinformationen für die CloudEndure Benutzerkonsole zu generieren, erstellen Sie mindestens einen IAM-Benutzer und weisen Sie diesem Benutzer die CloudEndure Berechtigungsrichtlinie zu. Die Konsole benötigt eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel . Um bewährte Methoden für die Verwaltung von AWS-Zugriffsschlüsseln zu befolgen, sollten Sie IAM-Schlüssel regelmäßig rotieren. Das Ändern von IAM-Schlüsseln führt dazu, dass Replikationsserver neu gestartet werden, was zu einer vorübergehenden Verzögerung führt.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Anmeldein formationen für das Konto des Staging-Bereichs ein.	Melden Sie sich bei der CloudEndure -Benutzer konsole an und wählen Sie Ihr Migrationsprojekt aus. Navigieren Sie auf der Registerkarte Setup und Info zu den AWS-Anmeldeinforma tionen und geben Sie Ihre AWS-Zugriffsschlüssel-ID und die ID des geheimen Zugriffss chlüssels an.	AWS-Systemadministrator

Konfigurieren von Replikationseinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Replikati onsserver.	Weitere Informationen finden Sie in der CloudEndure - Dokumentation.	CloudEndure Administrator

Installieren von CloudEndure Agents auf Ihrem Quellcomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie Ihr Agent-Ins tallationstoken.	Navigieren Sie in der - CloudEndure Benutzerk onsole zu Machines , Machine Actions undAdd Machines . Wenn Sie die Installationsdatei auf einem Quellcomputer ausführen, werden Sie zunächst aufgefordert, Ihr	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Installationstoken einzugeben. Das Token ist eine eindeutige Zeichenfolge, die automatisch für Sie generiert wird, wenn Ihr CloudEndure Konto aktiviert wird. Sie können ein Installat ionstoken verwenden, um den Agent auf so vielen Quellcomp utern zu installieren, wie Ihr Projekt zulässt.	
Führen Sie auf Linux-Mas chinen das Installationsprogr amm aus.	Kopieren Sie für Linux-Mas chinen den Installationsbefeh l, melden Sie sich bei Ihren Quellmaschinen an und führen Sie das Installationsprogramm aus. Detaillierte Anweisungen finden Sie in der CloudEndure Dokumentation zu .	CloudEndure Administrator
Führen Sie auf Windows-Computern das Installat ionsprogramm aus.	Laden Sie für Windows-C omputer die Installationsdatei auf jeden Computer herunter und führen Sie dann den Installationsbefehl aus. Detaillierte Anweisungen finden Sie in der CloudEndure Dokumentation zu .	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Replizieren Sie die Daten.	Nachdem der Agent installiert wurde, CloudEndure startet , um den Quellcomputer zu replizieren, den Staging-Bereich. Wenn die erste Synchronisierung abgeschlossen ist, wird der Computer auf der Registerkarte Computer in der - CloudEndure Benutzerkonsole angezeigt.	CloudEndure Administrator

Konfigurieren des Blueprints des Zielcomputers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Quellcomputer für den Blueprint aus.	Wählen Sie in der - CloudEndure Benutzerkonsole auf der Registerkarte Maschinen den Quellcomputer aus, um auf den Bereich Maschinendetails zuzugreifen.	CloudEndure Administrator
Konfigurieren Sie den Blueprint für den Zielcomputer.	Konfigurieren Sie auf der Registerkarte Blueprint die Einstellungen für Ihren Zielcomputer entsprechend Ihren Anforderungen. Detaillierte Anweisungen finden Sie in der CloudEndure Dokumentation zu .	CloudEndure Administrator

Testen Ihrer DR-Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie den Testmodus, um die Lösung zu testen.	Detaillierte Anweisungen zum Testmodus und zur Überprüfung des Test-Cutover finden Sie in der CloudEndure Dokumentation .	CloudEndure Administrator
Testen Sie Ihre Ziel-Instance, die auf dem Amazon EC2-Server gestartet wurde.	Um jeden Ihrer Zielcompu ter zu testen, wählen Sie den Namen des Computers aus. Öffnen Sie dann die Registerk arte Ziel, kopieren Sie die neue IP-Adresse und melden Sie sich bei dem neu gestartet en Server auf der Amazon EC2-Instance an.	CloudEndure Administrator

Durchführen eines Failovers mit CloudEndure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status des Quellcomputers.	Überprüfen Sie auf der Seite CloudEndure -Benutzerk onsolen-Computer, ob der Quellcomputer, für den Sie ein Failover ausführen möchten, die folgenden Statusanzeigen aufweist: • Fortschritt der Datenrepl ikation – Kontinuierlicher Datenschutz • Status – Rocket-Symbol, das angibt, dass der	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zielcomputer gestartet werden kann • Notfallwiederherstellungs-Lebenszyklus – kürzlich getestet	
Starten Sie den Cutover.	1. Wählen Sie auf der Seite Maschinen Ihren Quellcomputer aus. 2. Wählen Sie auf der Registerkarte Zielmaschinen starten die Option Wiederherstellungsmodus aus. 3. Wählen Sie den Wiederherstellungspunkt für den Zielcomputer aus. Das System verwendet den Wiederherstellungspunkt, wenn die neuen Zielmaschinen für das Failover gestartet werden. Sie können den neuesten Wiederherstellungspunkt verwenden oder einen vorherigen Wiederherstellungspunkt aus der Liste auswählen. 4. Wählen Sie Mit Start fortfahren aus.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Auftragsfortschritt und den Abschlussstatus.	Im Fenster Auftragsfortschritt werden Details zum Startvorgang des Zielcomputers angezeigt. Nachdem das Failover abgeschlossen ist, ändert sich der Status des Notfallwiederherstellungs-Lebenszyklus in der - CloudEndure Benutzerkonsole in Fehlgeschlagen, um den erfolgreichen Abschluss anzuzeigen.	CloudEndure Administrator

Durchführen eines Failbacks mit dem CloudEndure Failback-Client

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CloudEndure Failback-Client-Anforderungen.	Verwenden Sie den CloudEndure Failback-Client für die Replikation von einer On-Premises- oder einer anderen Cloud-Infrastruktur zu AWS. Der CloudEndure Failback-Client hat die folgenden Anforderungen: • Maschinen müssen so konfiguriert sein, dass sie im BIOS-Modus starten und den MBR-Start unterstützen. Maschinen, die für den Start im UEFI-Modus konfiguriert sind und nur den GPT-Start	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unterstützen, werden nicht unterstützt. • Der CloudEndure Failback-Client benötigt mindestens 4 GB dedizierten RAM.	
Bereiten Sie sich auf ein Failback vor.	Bevor Sie die Aktion Vorbereiten auf Failback einleiten können, müssen alle Quellcomputer Zielcomputer entweder im Testmodus oder im Wiederherstellungsmodus gestartet haben. Wählen Sie im Menü Projektaktionen die Option Auf Failback vorbereiten und dann Weiter aus. Wenn CloudEndure Kundendienstmitarbeiter mit dem Failback-Client koppeln angezeigt wird, sind die Maschinen für ein Failback bereit.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den CloudEndure Failback-Client in Ihre On-Premises-Umgebung herunter.	Gehen Sie wie folgt vor, um den CloudEndure Failback-Client in Ihre Quellumgebung herunterzuladen: 1. Wählen Sie in Ihrem DR-Projekt Setup und Info aus. 2. Wählen Sie auf der Seite Replikationseinstellungen den Link Informationen zum Zurückschlagen auf „Andere Infrastruktur“ aus. 3. Wählen Sie im Dialogfeld Failing Back to an Unidentified Cloud/Other Infrastructure die Option Download von hier aus. Die Datei wird automatisch heruntergeladen.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie die Replikation des On-Premises-Computers.	Um die Replikation des Quellcomputers zu initiiere n, muss der Zielcomputer im CloudEndure Failback-Client-Image (`failback_client.iso`) gestartet werden. Wenn der Client die Netzwerkeinstellungen nicht mit dem Dynamic Host Configuration Protocol (DHCP) abrufen kann, geben Sie die Einstellungen manuell ein. Der CloudEndure Failback-Client stellt über TCP-Port 443 eine Verbindung zu console.clouendure.com her und authentifiziert sich mit den CloudEndure Anmeldein formationen, zu deren Eingabe Sie aufgefordert werden.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie den Anweisungen, um die erforderlichen Details bereitzustellen.	Geben Sie die folgenden Details an: • Installationstoken • Maschinen-ID des Quellcomputers • Festplattenzuordnung zwischen Quelle und Ziel Stellen Sie sicher, dass der CloudEndure Failback-Client über öffentliche oder private IP-Adressen eine Verbindung zur - CloudEndure Benutzerk onsole und zum Zielcomputer hat.	CloudEndure Administrator
Suchen Sie die ID des Quellcomputers.	Um die ID des Quellcomputers zu finden, wählen Sie den Namen des Computers auf der Registerkarte Maschinen aus und kopieren Sie die ID aus der Registerkarte Quelle.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbinden Sie den Quellcomp uter mit dem Zielcomputer.	Geben Sie die Quellcomp uter-ID (der Server auf AWS ist jetzt die Quelle für das Failback) auf dem On-Premis es-Server (Zielcomputer) an. Die AWS-Maschine (Quelle) stellt eine Verbindung zum On-Premises-Server (Ziel) auf TCP-Port 1500 her, um die Replikation zu starten. Nachdem die erste Replikation abgeschlossen ist, zeigt die - CloudEndure Benutzerkonsole an, dass sich die Replikation im kontinuierlichen Datenschu tzmodus befindet.	CloudEndure Administrator
Bearbeiten Sie die Failback-Einstellungen, falls erforderl ich.	Um die Failback-Einstellungen zu bearbeiten, wählen Sie den Computernamen und dann die Registerkarte Failback-Einstellungen aus.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Zielcomputer.	Gehen Sie wie folgt vor, um den Zielcomputer zu starten: Aktivieren Sie das Kontrollk ästchen links neben jedem Computernamen, wählen Sie Starten x Zielcomputer und dann Wiederherstellungs modus aus. Wählen Sie im Dialogfeld Weiter aus. Wählen Sie den letzten Wiederherstellungspunkt und dann Mit Start fortfahren aus. Nachdem der Startvorgang abgeschlossen ist, zeigt die CloudEndure -Benutzer konsole den Status Den CloudEndure Agenten mit dem Replikationsserver koppeln unter Datenreplikationsf ortschritt an.	CloudEndure Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Setzen Sie die Maschinen in den normalen Betrieb zurück.	Ändern Sie nun die Richtung der Datenreplikation so, dass der On-Premises-Comput er die Quelle und der AWS-Computer das Ziel ist. Wählen Sie Projektaktionen und dann Zurück zum Normal und Weiter aus. Die Richtung der Datenrepl ikation wird umgekehrt , und die Maschinen durchlaufen den ersten Synchronisierungsprozess. Der Failback-Prozess ist abgeschlossen, wenn die Spalte Fortschritt der Datenreplikation den Status Kontinuierlicher Datenschutz für alle Maschinen anzeigt.	CloudEndure Administrator

Zugehörige Ressourcen

AWS Marketplace

- CloudEndure Notfallwiederherstellung

CloudEndure -Dokumentation

- Anmelden bei der Konsole
- Erstellen eines Projekts
- Generieren und Verwenden von Anmeldeinformationen
- Konfigurieren von Replikationseinstellungen
- Installieren von CloudEndure Agents

- Durchführen eines Failovers für die Notfallwiederherstellung

Tutorials und Videos

- CloudEndure Fehlerbehebung beim Playbook
- CloudEndure Videos
- Demo zur Notfallwiederherstellung in AWS

Mehr Muster

- Automatisieren von ereignisgesteuerten Backups von CodeCommit zu Amazon S3 mithilfe von CodeBuild und - CloudWatch Ereignissen
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatisches Sichern von SAP HANA-Datenbanken mit Systems Manager und EventBridge
- Sichern und Archivieren von Mainframe-Daten in Amazon S3 mithilfe von AMI-Cloud-Daten
- Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertieren des Datentyps VARCHAR2(1) für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2-Instances
- ???
- Schätzen der Speicherkosten für eine Amazon-DynamoDB-Tabelle
- Identifizieren öffentlicher S3-Buckets in AWS Organizations mithilfe von Security Hub
- Migrieren von DB-Instances von Amazon RDS für Oracle zu anderen Konten, die AMS verwenden
- Migrieren Sie mithilfe von AWS Transfer for SFTP einen lokalen SFTP-Server zu AWS
- Migrieren einer partitionierten Oracle-Tabelle zu PostgreSQL mithilfe von AWS DMS
- Migrieren von Daten von Microsoft Azure Blob zu Amazon S3 mithilfe von Rclone
- Migrieren von Oracle CLOB-Werten zu einzelnen Zeilen in PostgreSQL in AWS
- Migrieren gemeinsam genutzter Dateisysteme in einer großen AWS-Migration
- Migrieren Sie kleine Datensätze mithilfe von AWS SFTP von der lokalen Infrastruktur zu Amazon S3
- Überwachen von Amazon Aurora auf Instances ohne Verschlüsselung
- ???
- Führen Sie zustandsbehaftete Workloads mit persistenter Datenspeicherung aus, indem Sie Amazon EFS auf Amazon EKS mit AWS Fargate verwenden
- Erfolgreiches Importieren eines S3-Buckets als AWS- CloudFormation Stack
- Synchronisieren Sie Daten zwischen Amazon EFS-Dateisystemen in verschiedenen AWS-Regionen mithilfe von AWS DataSync

- EBS-Snapshot-Details für Ihr AWS-Konto oder Ihre Organisation anzeigen

Web- und mobile Apps

Themen

- Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit
- Erstellen Sie eine React-App mithilfe von AWS Amplify und fügen Sie die Authentifizierung mit Amazon Cognito hinzu
- Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein
- Mehr Muster

Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit

Erstellt von Deekshitulu Pentakota (AWS) und Sai Katakam (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Web- und mobile Apps DevOps; Modernisierung	AWS-Dienste: AWS Amplify; AWS CodeCommit

Übersicht

Moderne Webanwendungen sind als Single-Page-Anwendungen (SPAs) aufgebaut, die alle Anwendungskomponenten in statische Dateien packen. Mithilfe von AWS Amplify Hosting können Sie eine CI/CD-Pipeline (Continuous Integration and Continuous Deployment) aufbauen, die eine moderne Webanwendung erstellt, bereitstellt und hostet, die in einem Git-basierten Repository verwaltet wird. Wenn Sie Amplify Hosting mit dem Code-Repository verbinden, initiiert jeder Commit einen einzigen Workflow zur Bereitstellung des Frontends und Backends der Anwendung. Der Vorteil dieses Ansatzes besteht darin, dass die Webanwendung erst aktualisiert wird, nachdem die Bereitstellung erfolgreich abgeschlossen wurde, wodurch Inkonsistenzen zwischen Frontend und Backend vermieden werden.

In diesem Muster verwenden Sie ein CodeCommit AWS-Repository, um Ihre moderne Webanwendung zu verwalten. Die Beispiel-Webanwendung in dieser Anleitung verwendet das React SPA-Framework. Amplify Hosting unterstützt jedoch viele andere SPA-Frameworks wie Angular, Vue, Next.js und unterstützt auch Single-Site-Generatoren wie Gatsby, Hugo und Jekyll.

Dieses Muster richtet sich an AWS-Entwickler, die Erfahrung mit den folgenden Services und Konzepten haben:

- AWS CodeCommit
- AWS Amplify Hosting
- React
- JavaScript
- Node.js
- npm

- Git

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Erstellen von Ressourcen in Amplify und CodeCommit. Weitere Informationen finden Sie unter Identity and Access Management für Amplify und Identity and Access Management für AWS CodeCommit.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert.
- Ein Texteditor oder Code-Editor.
- CodeCommit, eingerichtet für HTTPS-Benutzer mit Git-Anmeldeinformationen.
- Eine IAM-Servicerolle für Amplify.
- npm und Node.js, installiert (npm-Dokumentation).

Einschränkungen

- Dieses Muster behandelt nicht die Entwicklung und Integration eines Backends für die Amplify-Anwendung, wie z. B. eine API, Authentifizierung oder Datenbank. Weitere Informationen zu Backends finden Sie unter Erstellen eines Backends in der Amplify-Dokumentation.

Produktversionen

- AWS-CLI Version 2.0
- Node.js Version 16.x oder höher

Architektur

Zieltechnologie-Stack

- CodeCommitAWS-Repository mit einem React-SPA
- AWS Amplify Hosting-Arbeitsablauf

Zielarchitektur

Tools

AWS-Services

- AWS Amplify Hosting bietet einen Git-basierten Workflow für das Hosten serverloser Full-Stack-Webanwendungen mit kontinuierlicher Bereitstellung.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Andere Tools

- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.

Epen

Erstellen Sie ein Repository CodeCommit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein -Repository.	Anweisungen finden Sie in der CodeCommit Dokumentation unter Erstellen eines CodeCommit AWS-Repositorys.	AWS DevOps
Klonen Sie das Repository	Anweisungen finden Sie in der CodeCommit Dokumentation unter Connect zum	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommit Repository durch Klonen des Repositorys. Wenn Sie dazu aufgefordert werden, geben Sie die Git-Anmeldeinformationen ein.	

Erstellen Sie eine React-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine neue React-Anwendung.	1. Geben Sie den folgenden Befehl ein, um zum geklonten Repo zu navigieren. Ersetzen Sie es `<repo name>` durch den Namen Ihres CodeCommit Repos.
	`$ cd <repo name>`
	2. Geben Sie den folgenden Befehl ein, um eine neue React-Anwendung im geklonten Repository zu erstellen.
	`$ npx create-react-app .`
	3. Codieren Sie die Anwendung und geben Sie dann den folgenden Befehl ein, um sie zu starten.
	`$ npm start`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Erstellen einer benutzerd efinierten React-Anwendung finden Sie in der Anleitung Create React App in der Dokumentation Create React App. Sie können auch eine React-Beispielanwendung für Ihr Amplify-Konto bereitste llen, indem Sie den Anweisung en unter Bereitstellen eines Frontends in der Amplify-D okumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Branch und übertragen Sie den Code.	1. Geben Sie den folgenden Befehl ein, um lokal einen neuen Zweig zu erstellen. Dabei <branch> handelt es sich um den Namen, den Sie dem neuen Zweig zuweisen möchten.
	`$ git checkout -b <branch>`
	2. Geben Sie den folgenden Befehl ein, um den Branch in das CodeCommit Repository zu übertragen. Dort <branch> befindet sich der Name, den Sie im vorherigen Schritt zugewiesen haben. Weitere Informationen finden Sie unter Mit Commits arbeiten.
	`$ git push --set-upstream origin <branch>`
		App-Developer

Stellen Sie die Anwendung in AWS Amplify Hosting bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect Amplify mit dem Repository.	Anweisungen finden Sie unter Ein Repository Connect in der Amplify Hosting-Dokumentation. Wählen Sie AWS CodeCommit und das	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repository und den Branch aus, die Sie zuvor erstellt haben.	

Definieren Sie die Frontend-Build-Einstellungen.	Anweisungen finden Sie unter Bestätigen der Build-Einstellungen für das Frontend in der Amplify Hosting-Dokumentation. Akzeptieren Sie die Standardeinstellungen oder geben Sie Folgendes ein.
	`Build settings:`
	`version: 0.1`
	`frontend:`
	`  phases:`
	`  preBuild:`
	`  commands:`
	`  - npm ci`
	`  build:`
	`  commands:`
	`  - npm run build`
	`  artifacts:`
	`  baseDirectory:`
	`build`
	`  files:`
	`  - '**/*'`
	`  cache:`
	`  paths:`
	`  - node_modules/`
	`**/*`
		App-Developer

Überprüfen und bereitstellen.	Anweisungen finden Sie unter Speichern und Bereitstellen in der Amplify Hosting-Dokumentation. Warten Sie, bis der Bereitstellungsvorgang abgeschlossen ist.	App-Developer

Bestätigen Sie die kontinuierliche Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die erste Bereitstellung.	Wenn der Bereitstellungsvorgang abgeschlossen ist, wählen Sie unter Domain den Link aus. Stellen Sie sicher, dass die Anwendung wie erwartet funktioniert.	App-Developer
Senden Sie eine Änderung in das Code-Repository.	Bearbeiten Sie den Code auf Ihrer lokalen Workstation und übertragen Sie die Änderungen in das CodeCommit Repository. Amplify Hosting erkennt die Änderung im Repository und startet automatisch den Build- und Bereitstellungsprozess. Vergewissern Sie sich, dass die Anwendungsupdates auf der Domain sichtbar sind.	App-Developer

Zugehörige Ressourcen

CodeCommit AWS-Dokumentation

- Einrichtung für AWS CodeCommit
  - Einrichtung für HTTPS-Benutzer mit Git-Anmeldeinformationen
  - Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Linux, macOS oder Unix mit dem AWS CLI Credential Helper
- Erste Schritte mit AWS CodeCommit

Dokumentation zum AWS Amplify Hosting

- Erste Schritte mit vorhandenem Code
- Benutzerdefinierte Domains einrichten

React-Ressourcen

- Erstellen Sie eine React App-Website
- Erstellen Sie die React-App-Dokumentation
- Erstellen Sie ein React-App-Repository (GitHub)

Erstellen Sie eine React-App mithilfe von AWS Amplify und fügen Sie die Authentifizierung mit Amazon Cognito hinzu

Erstellt von Rishi Singla (AWS)

Umgebung: PoC oder Pilotprojekt	Technologien: Web- und mobile Apps; Sicherheit, Identität, Compliance	Arbeitslast: Alle anderen Workloads
AWS-Dienste: AWS Amplify; Amazon Cognito		

Übersicht

Dieses Muster zeigt, wie Sie mit AWS Amplify eine React-basierte App erstellen und wie Sie mithilfe von Amazon Cognito Authentifizierung zum Frontend hinzufügen. AWS Amplify besteht aus einer Reihe von Tools (Open-Source-Framework, visuelle Entwicklungsumgebung, Konsole) und Services (Web-App und statisches Website-Hosting), um die Entwicklung von Mobil- und Web-Apps auf AWS zu beschleunigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Node.js und npm sind auf Ihrem Computer installiert

Produktversionen

- Node.js Version 10.x oder höher (um Ihre Version zu überprüfen, führen Sie es `node -v` in einem Terminalfenster aus)
- npm Version 6.x oder höher (um Ihre Version zu überprüfen, führen Sie es `npm -v` in einem Terminalfenster aus)

Architektur

Zieltechnologie-Stack

- AWS Amplify
- Amazon Cognito

Tools

- Befehlszeilenschnittstelle (CLI) Amplify
- Amplify Libraries (Open-Source-Clientbibliotheken)
- Amplify Studio (visuelle Oberfläche)

Epen

Installieren Sie AWS Amplify CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Amplify CLI.	Die Amplify CLI ist eine einheitliche Toolchain zur Erstellung von AWS-Cloud-Services für Ihre React-App. Führen Sie Folgendes aus, um die Amplify-CLI zu installieren: `npm install -g @aws-amplify/cli` npm benachrichtigt Sie, wenn eine neue Hauptversion verfügbar ist. Wenn ja, verwenden Sie den folgenden Befehl, um Ihre Version von npm zu aktualisieren:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`npm install -g npm@9.8.0` wobei sich 9.8.0 auf die Version bezieht, die Sie installieren möchten.	

Erstelle eine React-App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine React-App.	Verwenden Sie den folgenden Befehl, um eine neue React-App zu erstellen:
	
	`npx create-react-app amplify-react-application`
	
	wo `ampify-react-application` ist der Name der App.
	
	Wenn die App erfolgreich erstellt wurde, wird die Meldung angezeigt:
	
	`Success! Created amplify-react-application`
	
	Für die React-App wird ein Verzeichnis mit verschiedenen Unterordnern erstellt.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die App auf Ihrem lokalen Computer.	Gehen Sie zu dem Verzeichnis `amplify-react-application`, das im vorherigen Schritt erstellt wurde, und führen Sie den folgenden Befehl aus: `amplify-react-application% npm start` Dadurch wird die React-App auf Ihrem lokalen Computer gestartet.	App-Developer

Konfigurieren Sie die Amplify CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Amplify für die Verbindung mit Ihrem AWS-Konto.	Konfigurieren Sie Amplify, indem Sie den folgenden Befehl ausführen: `amplify-react-application % amplify configure` Die Amplify CLI fordert Sie auf, die folgenden Schritte auszuführen, um den Zugriff auf Ihr AWS-Konto einzurichten: 1. Melden Sie sich mit Ihrem AWS-Administratorkonto an.	Allgemein AWS, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie die AWS-Region an, die Sie verwenden möchten. 3. Erstellen Sie einen AWS Identity and Access Management (IAM) - Benutzer mit programmatischem Zugriff und hängen Sie die `AdministratorAccess-Amplify` Berechtigungsrichtlinie an den Benutzer an. 4. Erstellen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel und kopieren Sie sie anschließend. 5. Geben Sie diese Daten in das Terminal ein. 6. Erstellen Sie einen Profilnamen oder verwenden Sie das Standardprofil. Warnung: Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Die Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.
	
	Diese Schritte werden im Terminal wie folgt angezeigt.
	
	`Follow these steps to set up access to your AWS account:`
	`Sign in to your AWS administrator account: https://console.aws.amazon.com/`
	`Press Enter to continue`
	`Specify the AWS Region`
	`? region: us-east-1`
	`Follow the instructions at https://docs.amplify.aws/cli/start/install/#configure-the-amplify-cli`
	`to complete the user creation in the AWS console`
	`https://console.aws.amazon.com/iamv2/home#/users/create`
	`Press Enter to continue`
	`Enter the access key of the newly created user:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ? accessKeyId: ******************** ? secretAccessKey: ****************** ****************** **** This would update/cr eate the AWS Profile in your local machine ? Profile Name: new Successfully set up the new user. ``` Weitere Informationen zu diesen Schritten finden Sie in der Dokumentation im Amplify Dev Center.	

Amplify initialisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Amplify.	1. Um Amplify im neuen Verzeichnis zu initialisieren, führen Sie Folgendes aus: ``` amplify init ``` Amplify fordert Sie zur Eingabe des Projektnamens und der Konfigurationspara meter auf 2. Geben Sie alle Parameter an und drücken Sie dann Y, um das Projekt mit der	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	angegebenen Konfiguration zu initialisieren.
	
	`Project information`
	`| Name: amplifyre`
	`actproject`
	
	`| Environment: dev`
	
	`| Default editor:`
	` Visual Studio Code`
	
	`| App type: javascrip`
	`t`
	
	`| Javascript`
	` framework: react`
	
	`| Source Directory`
	` Path: src`
	
	`| Distribution`
	` Directory Path: build`
	
	`| Build Command: npm`
	` run-script build`
	
	`| Start Command: npm`
	` run-script start`
	
	3. Wählen Sie das Profil aus, das Sie im vorherigen Schritt erstellt haben. Die Ressourcen werden in der `dev` Umgebung des von Ihnen erstellten Amplify-P rojekts bereitgestellt.
	4. Um zu bestätigen, dass die Ressourcen erstellt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	wurden, können Sie die AWS Amplify Amplify-Konsole öffnen und die CloudFormation AWS-Vorlage, die zur Erstellung der Ressourcen verwendet wurde, sowie die Details anzeigen.
	
	`Deploying root stack amplifyreactproject [ ========== ---------- ---- ] 2/4 amplify-amplifyreactproject-d… AWS::CloudFormation::Stack CREATE_IN_PROGRESS`
	
	`UnauthRole AWS::IAM::Role CREATE_COMPLETE`
	
	`DeploymentBucket AWS::S3::Bucket CREATE_IN_PROGRESS`
	
	`AuthRole AWS::IAM::Role CREATE_COMPLETE`	

Fügen Sie dem Frontend eine Authentifizierung hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizierung hinzufügen.	Sie können den `amplify add <category>` Befehl verwenden, um Funktionen wie eine Benutzeranmeldung oder eine Backend-API hinzuzufügen. In diesem Schritt verwenden Sie den Befehl, um die Authentif izierung hinzuzufügen. Amplify bietet einen Backend-Authentifizierungsservice mit Amazon Cognito, Frontend-Bibliotheken und einer Drop-In-Authenticator-UI-Ko mponente. Zu den Funktionen gehören Benutzeranmeldung, Benutzeranmeldung, Multi-Faktor-Authentifizierung, Benutzerabmeldung und passwortlose Anmeldung. Sie können Benutzer auch authentifizieren, indem Sie föderierte Identitätsanbieter wie Amazon, Google und Facebook integrieren. Die Amplify-Authentifizierungsk ategorie lässt sich nahtlos in andere Amplify-Kategorien wie API, Analytik und Speicher integrieren, sodass Sie Autorisierungsregeln für authentifizierte und nicht	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	authentifizierte Benutzer definieren können.
	
	1. Führen Sie den folgenden Befehl aus, um die Authentifizierung für Ihre React-App zu konfigurieren:
	
	`amplify-react-application1 % amplify add auth`
	
	Dadurch werden die folgenden Informationen und Eingabeaufforderungen angezeigt. Sie können je nach Ihren Geschäfts- und Sicherheitsanforderungen die passende Konfiguration auswählen.
	
	`Using service: Cognito, provided by: awscloudformation The current configured provider is Amazon Cognito. Do you want to use the default authentication and security configuration? (Use arrow keys)`
	
	`# Default configuration`
	
	`Default configuration with Social`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Provider (Federation) Manual configuration I want to learn more.	
	2. Wählen Sie für ein einfaches Beispiel die Standardkonfiguration und dann den Anmeldemechanismus für Benutzer (in diesem Fall E-Mail): How do you want users to be able to sign in? Username # Email Phone Number Email or Phone Number I want to learn more.	
	3. Umgehen Sie die erweiterten Einstellungen, um das Hinzufügen von Authentifizierungsressourcen abzuschließen: Do you want to configure advanced	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>settings? (Use arrow keys)
	# No, I am done.
	
	 Yes, I want to make some additional changes.</pre>
	4. Erstellen Sie Ihre lokalen Backend-Ressourcen und stellen Sie sie in der Cloud bereit:
	<pre>amplify-react-application1 % amplify push</pre>
	Mit diesem Befehl werden die entsprechenden Änderungen an den Congito-Benutzerpools in Ihrem Konto vorgenommen.
	5. Drücken Sie Y, um die `auth` Ressource mithilfe von zu konfigurieren. CloudFormation
	
	Dadurch werden die folgenden Ressourcen konfiguriert:
	<pre>UserPool
	AWS::Cognito::UserPool
	CREATE_COMPLETE
	UserPoolClientWeb
	AWS::Cognito::UserPoolClient</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>CREATE_COMPLETE
	
	UserPoolClientWeb
	AWS::Cogn
	ito::UserPoolClient
	CREATE_COMPLETE
	
	UserPoolClientRole
	AWS::IAM:
	:Role
	CREATE_COMPLETE
	
	UserPoolClientLambda
	AWS::Lamb
	da::Function
	CREATE_COMPLETE
	UserPoolClientLam
	bdaPolicy
	AWS::IAM::Policy
	CREATE_CO
	MPLETE
	
	UserPoolClientLog
	Policy
	AWS::IAM::Policy
	CREATE_IN
	_PROGRESS</pre>
	Sie können diese Ressourcen auch mit der AWS Cognito-Konsole anzeigen (suchen Sie nach Cognito-Benutzerpools und Identitätspools).
	
	In diesem Schritt wird die `aws-exports.js` Datei im `src` Ordner für Ihre React-App mit den Cognito-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Benutzerpool- und Identität spool-Konfigurationen aktualisiert.	

Ändern Sie die Datei App.js

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Datei App.js.	Öffnen und überarbeiten Sie die `App.js` Datei in dem `src` Ordner. Die geänderte Datei sollte wie folgt aussehen: `{ App.Js File after modifications: import React from 'react'; import logo from './logo.svg'; import './App.css'; import { Amplify } from 'aws-amplify'; import { withAuthenticator, Button, Heading } from '@aws-amplify/ui-react'; import awsconfig from './aws-exports'; Amplify.configure(awsconfig); function App({ signOut }) { return (<div> <h1>Thankyou for doing verification</h1> <h2>My Content</h2>`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<button onClick={ signOut}>Sign out</ button>); } export default withAuthenticator(App);	
Importiere React-Pakete.	Die `App.js` Datei importiert zwei React-Pakete. Installie ren Sie diese Pakete mit dem folgenden Befehl: `amplify-react-appl ication1 % npm install --save aws-amplify @aws-amplify/ui-react`	App-Developer

Starten Sie die React-App und überprüfen Sie die Authentifizierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starte die App.	Starten Sie die React-App auf Ihrem lokalen Computer: `amplify-react-appl ication1 % npm start`	App-Entwickler, General AWS
Überprüfen Sie die Authentif izierung.	Prüfen Sie, ob die App zur Eingabe von Authentif izierungsparametern aufforder t. (In unserem Beispiel haben wir E-Mail als Anmeldeme thode konfiguriert.)	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Frontend-Benutzero berfläche sollte Sie zur Eingabe der Anmeldein formationen auffordern und eine Option zum Erstellen eines Kontos bieten. Sie können den Amplify-B uild-Prozess auch so konfiguri eren, dass das Backend als Teil eines kontinuierlichen Bereitstellungsworkflows hinzugefügt wird. Dieses Muster deckt diese Option jedoch nicht ab.	

Zugehörige Ressourcen

- Erste Schritte (npm-Dokumentation)
- Ein eigenständiges AWS-Konto erstellen (Dokumentation zur AWS-Kontoverwaltung)
- Dokumentation zu AWS Amplify
- Amazon Cognito Cognito-Dokumentation

Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront

Erstellt von Jean-Baptiste Guillois (AWS)

Code-Repository: React-basierte einseitige CORS-Anwendung	Umgebung: Produktion	Technologien: Web- und mobile Apps; Cloud-nativ; Serverlos
Arbeitslast: Alle anderen Workloads	AWS-Dienste: Amazon CloudFront; Amazon S3; Amazon API Gateway	

Übersicht

Eine einseitige Anwendung (SPA) ist eine Website oder Webanwendung, die den Inhalt einer angezeigten Webseite mithilfe von JavaScript APIs dynamisch aktualisiert. Dieser Ansatz verbessert die Benutzererfahrung und Leistung einer Website, da nur neue Daten aktualisiert werden, anstatt die gesamte Webseite vom Server neu zu laden.

Dieses Muster bietet einen step-by-step Ansatz zum Codieren und Hosten eines SPA, das in React auf Amazon Simple Storage Service (Amazon S3) und Amazon geschrieben ist CloudFront. Das SPA in diesem Muster verwendet eine REST-API, die von Amazon API Gateway verfügbar gemacht wird, und demonstriert auch bewährte Methoden für Cross-Origin Resource Sharing (CORS).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine integrierte Entwicklungsumgebung (IDE) wie AWS Cloud9.
- Node.js und`npm`, installiert und konfiguriert. Weitere Informationen finden Sie im Abschnitt Downloads der Dokumentation zu Node.js.
- Yarn, installiert und konfiguriert. Weitere Informationen finden Sie in der Yarn-Dokumentation.
- Git, installiert und konfiguriert. Weitere Informationen finden Sie in der Git-Dokumentation.

Architektur

Diese Architektur wird automatisch mithilfe von AWS CloudFormation (Infrastructure as Code) bereitgestellt. Es verwendet regionale Dienste wie Amazon S3 zum Speichern der statischen Ressourcen und Amazon API Gateway, um regionale API-Endpunkte (REST) verfügbar zu machen. Die Anwendungsprotokolle werden mithilfe von Amazon gesammelt CloudWatch. Alle AWS-API-Aufrufe werden in AWS CloudTrail geprüft. Die gesamte Sicherheitskonfiguration (z. B. Identitäten und Berechtigungen) wird in Amazon Identity and Access Management (IAM) verwaltet. Statische Inhalte werden über das Amazon CloudFront Content Delivery Network (CDN) bereitgestellt, und DNS-Abfragen werden von Amazon Route 53 bearbeitet.

Technologie-Stack

- Amazon API Gateway
- Amazon CloudFront
- Amazon Route 53
- Amazon S3
- IAM
- Amazon CloudWatch
- AWS CloudTrail
- AWS CloudFormation

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS Cloud9 ist eine IDE, die Sie beim Codieren, Erstellen, Ausführen, Testen und Debuggen von Software unterstützt. Es hilft Ihnen auch dabei, Software in der AWS-Cloud zu veröffentlichen.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.

- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und des Betriebsrisikos Ihres AWS-Kontos.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Beispielanwendungscode dieses Musters ist im GitHub React-basierten einseitigen CORS-Anwendungs-Repository verfügbar.

Epen

Erstellen und implementieren Sie Ihre Anwendung lokal

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Wir empfehlen die Verwendung von AWS Cloud9 als IDE für dieses Muster, aber Sie können auch eine andere IDE verwenden (z. B. Visual Studio Code oder IntelliJ IDEA). Führen Sie den folgenden Befehl aus, um das Repository der Beispielanwendung in Ihre IDE zu klonen: `git clone https://github.com/aws-samp`	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/react-cors-spa react-cors-spa && cd react-cors-spa`	
Stellen Sie die Anwendung lokal bereit.	1. Führen Sie im Projektverzeichnis den `npm install` Befehl aus, um die Anwendungsabhängigkeiten zu initiieren. 2. Führen Sie den `yarn start` Befehl aus, um die Anwendung lokal zu starten.	App-Entwickler, AWS DevOps
Lokaler Zugriff auf die Anwendung.	Öffnen Sie ein Browserfenster und geben Sie die `http://localhost:3000` URL für den Zugriff auf die Anwendung ein.	App-Entwickler, AWS DevOps

Bereitstellen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation AWS-Konsole. 2. Wählen Sie Create Stack und dann With new resources (Standard) aus.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Upload a template file (Vorlagendatei hochladen). 4. Wählen Sie „Datei auswählen“, wählen Sie die `react-cors-spa-stack.yaml` Datei aus dem geklonten Repository aus und klicken Sie dann auf „Weiter“. 5. Geben Sie einen Namen für Ihren Stack ein und wählen Sie dann Weiter. 6. Behalten Sie alle Standardoptionen bei und wählen Sie dann Weiter. 7. Überprüfen Sie die endgültigen Einstellungen für Ihren Stapel und wählen Sie dann Stapel erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie Ihre Anwendung squelldateien an.	1. Öffnen Sie nach der Bereitstellung Ihres Stacks die Registerkarte Ausgabe und identifiz ieren Sie die `APIEndpoi nt` URL, den `Bucket` Namen und`CFDistrib utionURL` . 2. Kopieren Sie die URL des API-Endpunkts. 3. Navigieren Sie zu `<project_root>/ src/App.js` und fügen Sie die URL dann in den `APIEndPoint` Variablen wert in Zeile 26 der `App.js` Datei ein.	App-Developer
Erstellen Sie das Anwendung spaket.	Führen Sie in Ihrem Projektverzeichnis den `yarn build` Befehl aus, um das Anwendungspaket zu erstellen .	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Anwendung spaket bereit.	1. Öffnen Sie die Amazon S3-Konsole. 2. Identifizieren Sie den S3-Bucket, den Sie zuvor erstellt haben, und wählen Sie ihn aus. 3. Wählen Sie Hochladen und dann Dateien hinzufügen. 4. Wählen Sie den Inhalt Ihres Build-Ordners aus. 5. Wählen Sie Ordner hinzufügen und wählen Sie dann das statische Verzeichnis aus. Wichtig: Wählen Sie nicht den Inhalt, sondern das Verzeichnis. 6. Wählen Sie Hochladen, um die Dateien und das Verzeichnis in Ihren S3-Bucket hochzuladen.	App-Entwickler, AWS DevOps

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Anwendung zu und testen Sie sie.	Öffnen Sie ein Browserfenster und fügen Sie dann die URL (die `CFDistributionURL` Ausgabe aus dem CloudFormation Stack, den Sie zuvor bereitgestellt haben) ein, um auf die Anwendung zuzugreifen.	App-Entwickler, AWS DevOps

Säubere die Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Inhalt des S3-Buckets.	1. Öffnen Sie die Amazon S3 S3-Konsole und wählen Sie den Bucket aus, der zuvor vom Stack erstellt wurde (der erste Bucket, dessen Name mit beginnt`react-cors-spa-`). 2. Wählen Sie Leer, um den Inhalt des Buckets zu löschen. 3. Wählen Sie den zweiten Bucket aus, der zuvor vom Stack erstellt wurde (den zweiten Bucket, dessen Name mit beginnt `react-cors-spa-` und endet mit`-logs`). 4. Wählen Sie Leer, um den Inhalt des Buckets zu löschen.	AWS DevOps, App-Entwickler
Löschen Sie den CloudFormation AWS-Stack.	1. Öffnen Sie die CloudFormation AWS-Konsole und wählen Sie den Stack aus, den Sie zuvor erstellt haben. 2. Wählen Sie Löschen, um den Stack und alle zugehörigen Ressourcen zu löschen.	AWS DevOps, App-Entwickler

Zusätzliche Informationen

Um Ihre Webanwendung bereitzustellen und zu hosten, können Sie auch AWS Amplify Hosting verwenden, das einen Git-basierten Workflow für das Hosten serverloser Full-Stack-Web-Apps mit kontinuierlicher Bereitstellung bietet. Amplify Hosting ist Teil von AWS Amplify, das eine Reihe von speziell entwickelten Tools und Funktionen bietet, mit denen Frontend-Web- und Mobilentwickler schnell und einfach Full-Stack-Anwendungen auf AWS erstellen können.

Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit

Erstellt von Saurabh Kothari (AWS)

Umwelt: Produktion	Technologien: Web- und mobile Apps; Netzwerke; Serverlos; Infrastruktur	AWS-Services: Amazon API Gateway; Amazon Route 53; AWS Certificate Manager (ACM)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Amazon API Gateway Gateway-API auf einer internen Website bereitstellen, auf die von einem lokalen Netzwerk aus zugegriffen werden kann. Sie lernen, einen benutzerdefinierten Domainnamen für eine private API zu erstellen, indem Sie eine Architektur verwenden, die mit privaten Endpunkten, einem Application Load Balancer PrivateLink, AWS und Amazon Route 53 konzipiert ist. Diese Architektur verhindert die unbeabsichtigten Folgen der Verwendung eines benutzerdefinierten Domainnamens und eines Proxyservers zur Unterstützung des domänenbasierten Routing auf einer API. Wenn Sie beispielsweise einen VPC-Endpunkt (Virtual Private Cloud) in einem nicht routbaren Subnetz bereitstellen, kann Ihr Netzwerk das API Gateway nicht erreichen. Eine gängige Lösung besteht darin, einen benutzerdefinierten Domainnamen zu verwenden und dann die API in einem routingfähigen Subnetz bereitzustellen. Dies kann jedoch andere interne Websites beschädigen, wenn die Proxykonfiguration Traffic (`execute-api.{region}.vpce.amazonaws.com`) an AWS Direct Connect weiterleitet. Schließlich kann Ihnen dieses Muster dabei helfen, die organisatorischen Anforderungen für die Verwendung einer privaten API, die vom Internet aus nicht erreichbar ist, und eines benutzerdefinierten Domainnamens zu erfüllen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Server Name Indication (SNI) -Zertifikat für Ihre Website und API

- Eine Verbindung von einer lokalen Umgebung zu einem AWS-Konto, das mithilfe von AWS Direct Connect oder AWS Site-to-Site VPN eingerichtet wurde
- Eine private gehostete Zone mit einer entsprechenden Domain (z. B. domain.com), die von einem lokalen Netzwerk aus aufgelöst wird und DNS-Abfragen an Route 53 weiterleitet
- Ein routbares privates Subnetz, das von einem lokalen Netzwerk aus erreichbar ist

Einschränkungen

Weitere Informationen zu Kontingenten (früher als Limits bezeichnet) für Load Balancer, Regeln und andere Ressourcen finden Sie unter Kontingente für Ihre Application Load Balancers in der Elastic Load Balancing Balancing-Dokumentation.

Architektur

Technologie-Stack

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS Certificate Manager
- AWS PrivateLink

Zielarchitektur

Das folgende Diagramm zeigt, wie ein Application Load Balancer in einer VPC bereitgestellt wird, der Web-Traffic auf der Grundlage von Application Load Balancer Balancer-Listener-Regeln an eine Website-Zielgruppe oder API-Gateway-Zielgruppe weiterleitet. Die API Gateway-Zielgruppe ist eine Liste von IP-Adressen für den VPC-Endpunkt in API Gateway. API Gateway ist so konfiguriert, dass die API mit ihrer Ressourcenrichtlinie privat ist. Die Richtlinie lehnt alle Anrufe ab, die nicht von einem bestimmten VPC-Endpunkt stammen. Benutzerdefinierte Domainnamen im API-Gateway werden aktualisiert und verwenden nun api.domain.com für die API und ihre Phase. Application Load Balancer Balancer-Regeln werden hinzugefügt, um den Datenverkehr auf der Grundlage des Hostnamens weiterzuleiten.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer aus einem lokalen Netzwerk versucht, auf eine interne Website zuzugreifen. Die Anfrage wird an ui.domain.com und api.domain.com gesendet. Anschließend wird die Anfrage an den internen Application Load Balancer des routbaren privaten Subnetzes weitergeleitet. Das SSL wird am Application Load Balancer für ui.domain.com und api.domain.com beendet.
2. Listener-Regeln, die auf dem Application Load Balancer konfiguriert sind, suchen nach dem Host-Header.

   a. Wenn der Host-Header api.domain.com lautet, wird die Anfrage an die API Gateway Gateway-Zielgruppe weitergeleitet. Der Application Load Balancer initiiert eine neue Verbindung zum API Gateway über Port 443.

   b. Wenn der Host-Header ui.domain.com lautet, wird die Anfrage an die Zielgruppe der Website weitergeleitet.
3. Wenn die Anfrage API Gateway erreicht, bestimmt die in API Gateway konfigurierte benutzerdefinierte Domänenzuordnung den Hostnamen und die auszuführende API.

Automatisierung und Skalierung

Die Schritte in diesem Muster können mithilfe von AWS CloudFormation oder dem AWS Cloud Development Kit (AWS CDK) automatisiert werden. Um die Zielgruppe der API-Gateway-Aufrufe zu konfigurieren, müssen Sie eine benutzerdefinierte Ressource verwenden, um die IP-Adresse des VPC-Endpunkts abzurufen. API-Aufrufe an describe-vpc-endpointsund describe-network-interfacesRückgabe der IP-Adressen und der Sicherheitsgruppe, die zur Erstellung der API-Zielgruppe von IP-Adressen verwendet werden können.

Tools

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS PrivateLink hilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren VPCs zu Services außerhalb der VPC herzustellen.

Epen

Erstellen Sie ein SNI-Zertifikat

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNI-Zertifikat und importieren Sie das Zertifikat in ACM.	1. Erstellen Sie ein SNI-Zertifikat für ui.domain.com und api.domain.com. Weitere Informationen finden Sie in der CloudFront Amazon-Dokumentation unter Auswählen, wie CloudFront HTTPS-Anfragen bearbeitet werden. 2. Importieren Sie die SNI-Zertifikate in AWS Certificate Manager (ACM). Weitere Informationen finden Sie in der ACM-Dokumentation unter Zertifikate in AWS Certificate Manager importieren.	Netzwerkadministrator

Stellen Sie einen VPC-Endpunkt in einem privaten Subnetz bereit, das nicht routbar ist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Schnittstellen-Endpunkt in API Gateway.	Um einen VPC-Schnittstellen-Endpunkt zu erstellen, folgen Sie den Anweisungen unter Zugreifen auf einen AWS-Service mithilfe eines Schnittstellen-VPC-Endpunkts in der Dokumentation zu Amazon	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Virtual Private Cloud (Amazon VPC).	

Den Application Load Balancer konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe für Ihre Bewerbung.	Erstellen Sie eine Zielgruppe für die UI-Ressourcen Ihrer Anwendung.	Cloud-Administrator
Erstellen Sie eine Zielgruppe für den API-Gateway-Endpunkt.	1. Erstellen Sie eine Zielgruppe mit einem IP-Adresstyp und fügen Sie dann die IP-Adresse des VPC-Endpunkts für den API-Gateway-Endpunkt zur Zielgruppe hinzu. 2. Konfigurieren Sie Integritätsprüfungen für Ihre Zielgruppen mit den Erfolgscodes 200 und 403. 403 ist erforderlich, da die API Authentifizierung verwenden und eine 403-Antwort zurückgeben könnte.	Cloud-Administrator
Erstellen Sie einen Application Load Balancer.	1. Erstellen Sie einen Application Load Balancer (intern) in einem routbaren privaten Subnetz. 2. Fügen Sie den 443-Listener zum Application Load	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Balancer hinzu und wählen Sie dann das Zertifikat von ACM aus.	
Erstellen Sie Regeln für Zuhörer.	Erstellen Sie Listener-Regeln, um Folgendes zu tun: 1. Leiten Sie den Host api.domain.com an die API Gateway Gateway-Zielgruppe weiter 2. Leiten Sie den Host ui.domain.com an die Zielgruppe für die UI-Ressourcen weiter	Cloud-Administrator

Route 53 konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine private gehostete Zone.	Erstellen Sie eine private gehostete Zone für domain.com.	Cloud-Administrator
Domaindatensätze erstellen.	Erstellen Sie CNAME-Einträge für Folgendes: • Eine API, deren Wert auf den DNS-Namen des Application Load Balancer gesetzt ist • Eine Benutzeroberfläche, deren Wert auf den DNS-Namen des Application Load Balancer gesetzt ist	Cloud-Administrator

Erstellen Sie einen privaten API-Endpunkt in API Gateway

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen privaten API-Endpunkt.	1. Um einen privaten API-Endpunkt zu erstellen, folgen Sie den Anweisungen unter Erstellen einer privaten API in Amazon API Gateway in der API Gateway-Dokumentation. 2. Konfigurieren Sie die Ressourcenrichtlinie so, dass nur API-Aufrufe vom VPC-Endpunkt aus zulässig sind. Weitere Informationen finden Sie unter Steuern des Zugriffs auf eine API mit API-Gateway-Ressourcenrichtlinien in der API Gateway Gateway-Dokumentation.	App-Entwickler, Cloud-Administrator
Erstellen Sie einen benutzerdefinierten Domainnamen.	1. Erstellen Sie einen benutzerdefinierten Domainnamen für api.domain.com. Weitere Informationen finden Sie unter Einrichten von benutzerdefinierten Domainnamen für REST-APIs in der API Gateway Gateway-Dokumentation. 2. Wählen Sie die erstellte API und die Phase aus. Weitere Informationen finden Sie unter Arbeiten mit API-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zuordnungen für REST-APIs in der API Gateway Gateway-Dokumentation.	

Zugehörige Ressourcen

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS PrivateLink
- AWS Certificate Manager

Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein

Erstellt von Sean Griffin (AWS) und Milena Godau (AWS)

Umgebung: PoC oder Pilot	Technologien: Web- und mobile Apps; Analytik	AWS-Dienste: AWS Lambda; Amazon QuickSight; Amazon API Gateway

Übersicht

Dieses Muster bietet Anleitungen für die Einbettung eines QuickSight Amazon-Dashboards in eine lokal gehostete Angular-Anwendung zur Entwicklung oder zum Testen. Die eingebettete Analysefunktion in unterstützt diese Funktionalität QuickSight nicht nativ. Es erfordert ein QuickSight Konto mit einem vorhandenen Dashboard und Kenntnisse von Angular.

Wenn Sie mit eingebetteten QuickSight Dashboards arbeiten, müssten Sie Ihre Anwendung normalerweise auf einem Webserver hosten, um das Dashboard anzeigen zu können. Dies erschwert die Entwicklung, da Sie Ihre Änderungen kontinuierlich auf den Webserver übertragen müssen, um sicherzustellen, dass sich alles korrekt verhält. Dieses Muster zeigt, wie Sie einen lokal gehosteten Server ausführen und QuickSight eingebettete Analysen verwenden, um den Entwicklungsprozess einfacher und effizienter zu gestalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Ein aktives QuickSight Konto mit Preisgestaltung für Sitzungskapazität
- QuickSight Embedding SDK ist installiert
- Angular CLI installiert
- Vertrautheit mit Angular
- mkcert ist installiert

Einschränkungen

- Dieses Muster bietet Anleitungen zum Einbetten eines QuickSight Dashboards mithilfe des Authentifizierungstyps `ANONYMOUS` (öffentlich zugänglich). Wenn Sie AWS Identity and Access Management (IAM) oder die QuickSight Authentifizierung mit Ihren eingebetteten Dashboards verwenden, gilt der angegebene Code nicht. Die Schritte zum Hosten der Angular-Anwendung im Abschnitt Epics sind jedoch weiterhin gültig.
- Für die Verwendung der GetDashboardEmbedUrlAPI mit dem `ANONYMOUS` Identitätstyp ist ein QuickSight Kapazitätspreisplan erforderlich.

Versionen

- Angular CLI versie 13.3.4
- QuickSight Einbetten der SDK-Version 2.3.1

Architektur

Technologie-Stack

- Eckiges Frontend
- Backend für AWS Lambda und Amazon API Gateway

Architektur

In dieser Architektur ermöglichen die HTTP-APIs in API Gateway der lokalen Angular-Anwendung, die Lambda-Funktion aufzurufen. Die Lambda-Funktion gibt die URL zum Einbetten des QuickSight Dashboards zurück.

Automatisierung und Skalierung

Sie können die Backend-Bereitstellung mithilfe von AWS CloudFormation oder AWS Serverless Application Model (AWS SAM) automatisieren.

Tools

Tools

- Angular CLI ist ein Befehlszeilenschnittstellentool, mit dem Sie Angular-Anwendungen direkt von einer Befehlsshell aus initialisieren, entwickeln, einrichten und verwalten können.
- QuickSight Das Embedding SDK wird verwendet, um Dashboards in Ihren HTML-Code einzubetten. QuickSight
- mkcert ist ein einfaches Tool zum Erstellen lokal vertrauenswürdiger Entwicklungszertifikate. Es erfordert keine Konfiguration. mkcert ist erforderlich, da nur HTTPS-Anfragen zum Einbetten von Dashboards QuickSight zulässig sind.

AWS-Services

- Amazon API Gateway ist ein AWS-Service für die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon QuickSight ist ein Geschäftsanalysedienst, mit dem Sie Visualisierungen erstellen, Ad-hoc-Analysen durchführen und Geschäftserkenntnisse aus Ihren Daten gewinnen können.

Epen

Generieren Sie eine EmbedUrl

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine EmbedUrl Richtlinie.	Erstellen Sie eine IAM-Richtlinie mit QuicksightGetDashboardEmbedUrldem Namen und den folgenden Eigenschaften. `{ "Version": "2012-10-17", "Statement": [`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	
	"Effect": "Allow",
	
	"Action": [
	
	"quicksight:GetDashboardEmbedUrl",
	
	"quickSight:GetAnonymousUserEmbedUrl"
	],
	
	"Resource": "*"
	}
	]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

So erstellen Sie die Lambda-Funktion:	1. Öffnen Sie in der Lambda-Konsole die Seite Funktionen.
	
	2. Wählen Sie Funktion erstellen.
	
	3. Wählen Sie Von Grund auf neu schreiben aus.
	
	4. Geben Sie für Function name (Funktionsname) `get-qs-embed-url` ein.
	
	5. Wählen Sie für Runtime (Laufzeit) die Option Python 3.9 aus.
	
	6. Wählen Sie Funktion erstellen.
	
	7. Kopieren Sie auf der Registerkarte Code den folgenden Code in die Lambda-Funktion.
	
	`import json`
	`import boto3`
	`from botocore.`
	`exceptions import`
	` ClientError`
	`import time`
	`from os import environ`
	
	`qs = boto3.client('quic`
	`ksight',region_nam`
	`e='us-east-1')`
	`sts = boto3.cli`
	`ent('sts')`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ACCOUNT_ID = boto3.client('sts').get_caller_identity().get('Account')
	DASHBOARD_ID = environ['DASHBOARD_ID']
	
	def getDashboardURL(accountId, dashboardId, quicksightNamespace, resetDisabled, undoRedoDisabled):
	  try:
	  response = qs.get_dashboard_embed_url(
	  AwsAccountId = accountId,
	  DashboardId = dashboardId,
	  Namespace = quicksightNamespace,
	  IdentityType = 'ANONYMOUS',
	  SessionLifetimeInMinutes = 600,
	  UndoRedoDisabled = undoRedoDisabled,
	  ResetDisabled = resetDisabled
	  )
	  return response
	
	  except ClientError as e:
	  print(e)
	  return "Error generating embeddedURL: " + str(e)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`def lambda_handler(eve nt, context):`
	`  url = getDashbo ardURL(ACCOUNT_ID,`
	` DASHBOARD_ID,`
	` "default", True, True) ['EmbedUrl']`
	`  return {`
	`  'statusCode':  200,`
	`  'url': url`
	`  }`
	
	8. Wählen Sie Bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Dashboard-ID als Umgebungsvariable hinzu.	Fügen Sie Ihrer Lambda-Funktion `DASHBOARD_ID` als Umgebungsvariable hinzu: 1. Wählen Sie auf der Registerkarte Konfiguration die Optionen Umgebungsvariablen, Bearbeiten, Umgebungsvariable hinzufügen aus. 2. Fügen Sie eine Umgebungsvariable mit dem Schlüssel hinzu`DASHBOARD_ID` . 3. Um den Wert von zu `DASHBOARD_ID` ermitteln, navigieren Sie zu Ihrem Dashboard QuickSight und kopieren Sie die UUID am Ende der URL in Ihren Browser. Wenn die URL beispielsweise lautet`https://us-east-1.quicksight.aws.amazon.com/sn/dashboards/<dashboard-id>` , geben Sie den `<dashboard-id>` Teil der URL als Schlüsselwert an. 4. Wählen Sie Speichern.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Berechtigungen für die Lambda-Funktion hinzu.	Ändern Sie die Ausführun gsrolle der Lambda-Fu nktion und fügen Sie ihr die QuicksightGetDashb oardEmbedUrlRichtlinie hinzu. 1. Wählen Sie auf der Registerkarte Konfiguration die Option Berechtigungen und dann den Rollennamen aus. 2. Wählen Sie Richtlini en anhängen, suchen Sie nach`Quicksigh tGetDashboardEmbed Url` , aktivieren Sie das entsprechende Kontrollk ästchen und wählen Sie dann Richtlinie anhängen aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lambda-Funktion.	Erstellen Sie ein Testereignis und führen Sie es aus. Sie können die Vorlage „Hello World“ verwenden, da die Funktion keine der Daten des Testereignisses verwendet. 1. Wählen Sie die Registerkarte Test. 2. Geben Sie Ihrem Testereignis einen Namen und wählen Sie dann Speichern. 3. Um Ihre Lambda-Funktion zu testen, wählen Sie Test. Die Antwort sollte in etwa so aussehen wie die folgende. `{ "statusCode": 200, "url": "\"https://us-east-1.quicksight.aws.amazon.com/embed/f1acc0786687783b9a4543a05ba929b3a/dashboards/... }` Hinweis: Wie im Abschnitt Voraussetzungen und Einschränkungen erwähnt, muss für Ihr QuickSight Konto ein Preisplan für Sitzungskapazität gelten. Andernfalls	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird bei diesem Schritt eine Fehlermeldung angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine API in API Gateway.	1. Wählen Sie in der API Gateway Gateway-Konsole Create API und dann REST API, Build aus. • Geben Sie als API-Name ein `qs-embed-api` . • Wählen Sie Create API (API erstellen) aus. 2. Wählen Sie unter Aktionen die Option Methode erstellen aus. • Wählen Sie GET und bestätigen Sie mit dem Häkchen. • Wählen Sie Lambda-Funktion als Integrationstyp. • Geben `get-qs-embed-url` Sie für Lambda-Funktion den Wert ein. • Wählen Sie Speichern. • Wählen Sie im Feld Add Permission to Lambda Function die Option OK aus. 3. Aktivieren Sie CORS. • Wählen Sie unter Aktionen die Option CORS aktivieren aus. • Geben Sie für Access-Control-Allow-Origin ein.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`'https://my-qs-app.net:4200'` • Wählen Sie „CORS aktivieren“ und ersetzen Sie die vorhandenen CORS-Header und bestätigen Sie. 4. Stellen Sie die API bereit. • Wählen Sie für Aktionen die Option Deploy API aus. • Wählen Sie für Deployment stage (Bereitstellungsstufe) [New Stage] ([Neue Stufe]) aus. • Geben Sie für Stage name (Stufenname) `dev` ein. • Wählen Sie Deploy (Bereitstellen) aus. • Kopieren Sie die Aufruf-URL. Hinweis: Es `my-qs-app.net` kann sich um eine beliebige Domain handeln. Wenn Sie einen anderen Domainnamen verwenden möchten, stellen Sie sicher, dass Sie die Access-Control-Allow-Origin-Informationen in Schritt 3 aktualisieren und in	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den nachfolgenden Schritten ändern. `my-qs-app.net`	

Erstellen Sie die Angular-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Anwendung mit der Angular CLI.	1. Erstellen Sie die Anwendung.
	`ng new quicksight-app --defaults`
	`cd quicksight-app/src/app`
	2. Erstellen Sie die Dashboard-Komponente.
	`ng g c dashboard`
	3. Navigieren Sie zu Ihrer `src/environments/environment.ts` Datei und fügen Sie `apiUrl: '<Invoke URL from previous steps>'` sie dem Umgebungsobjekt hinzu.
	`export const environment = { production: false, apiUrl: '<Invoke URL from previous steps>', };`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie das QuickSight Embedding SDK hinzu.	1. Installieren Sie das QuickSight Embedding SDK, indem Sie den folgenden Befehl im Stammordner Ihres Projekts ausführen.
	`npm i amazon-quicksight-embedding-sdk`
	2. Erstellen Sie eine neue `decl.d.ts` Datei in dem `src` Ordner mit dem folgenden Inhalt.
	`declare module 'amazon-quicksight-embedding-sdk';`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Ihrer Datei dashboard.component.ts Code hinzu.	`import { Component, OnInit } from '@angular/core';`
	`import { HttpClient } from '@angular/common/http';`
	`import * as QuicksightEmbedding from 'amazon-quicksight-embedding-sdk';`
	`import { environment } from "../../environments/environment";`
	`import { take } from 'rxjs';`
	`import { EmbeddingContext } from 'amazon-quicksight-embedding-sdk/dist/types';`
	`import { createEmbeddingContext } from 'amazon-quicksight-embedding-sdk';`
	
	`@Component({`
	`  selector: 'app-dashboard',`
	`  templateUrl: './dashboard.component.html',`
	`  styleUrls: ['./dashboard.component.scss']`
	`})`
	`export class DashboardComponent implements OnInit {`
	
	`  constructor(private http: HttpClient) { }`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`  loadingError = false;`
	`  dashboard: any;`
	
	`  ngOnInit() {`
	`  this.GetDashboardU`
	`RL();`
	`  }`
	
	`  public GetDashbo`
	`ardURL() {`
	`  this.http.get(envi`
	`ronment.apiUrl)`
	`  .pipe(`
	`  take(1),`
	`  )`
	`  .subscribe((data:`
	` any) => this.Dash`
	`board(data.url));`
	`  }`
	
	`  public async Dashboard`
	`(embeddedURL: any) {`
	`  var containerDiv`
	` = document.getElemen`
	`tById("dashboardCo`
	`ntainer") || '';`
	`  const frameOptions`
	` = {`
	`  url: embeddedURL,`
	`  container:`
	` containerDiv,`
	`  height: "850px",`
	`  width: "100%",`
	`  resizeHei`
	`ghtOnSizeChangedEv`
	`ent: true,`
	`  }`
	`  const embedding`
	`Context: Embedding`
	`Context = await`
	` createEmbeddingCon`
	`text();`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`this.dashboard = embeddingContext.embedDashboard(frameOptions); } }`	
Fügen Sie Ihrer Datei dashboard.component.html Code hinzu.	Fügen Sie nun folgenden Code in die Datei `src/app/dashboard/dashboard.component.html` ein: `<div id="dashboardContainer"></div>`	App-Developer
Ändern Sie Ihre app.component.html-Datei, um Ihre Dashboard-Komponente zu laden.	1. Löschen Sie den Inhalt der Datei. `src/app/app.component.html` 2. Fügen Sie Folgendes hinzu. `<app-dashboard></app-dashboard>`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie HttpClien tModule in Ihre app.module.ts-Datei.	1. Fügen Sie am Anfang der `src/app/app.module.ts` Datei Folgendes hinzu. `import { HttpClientModule } from '@angular/common/http';` 2. Fügen Sie `HttpClientModule` das **`imports`**Array für Ihr hinzu`AppModule` .	App-Developer

Hosten Sie die Angular-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie mkcert.	Hinweis: Die folgenden Befehle gelten für Unix- oder MacOS-Computer. Wenn Sie Windows verwenden, finden Sie im Abschnitt Zusätzliche Informationen den entsprechenden Befehl echo. 1. Erstellen Sie eine lokale Zertifizierungsstelle (CA) auf Ihrem Computer. `mkcert -install` 2. Konfigurieren `my-qs-app.net` Sie so, dass	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	immer auf Ihren lokalen PC umgeleitet wird.
	`echo "127.0.0.1 my-qs-app.net" | sudo tee -a /private/etc/hosts`
	3. Stellen Sie sicher, dass Sie sich im `src` Verzeichnis des Angular-Projekts befinden.
	`mkcert my-qs-app.net 127.0.0.1`	

Konfigurieren Sie QuickSight es so, dass Ihre Domain zugelassen wird.	1. Wählen Sie in QuickSight der oberen rechten Ecke Ihren Namen und dann Quicksight verwalten aus. 2. Navigieren Sie zu Domains und Einbettung. 3. `https://my-qs-app.net:4200` Als zulässige Domain hinzufügen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lösung.	Starten Sie einen lokalen Angular-Entwicklungsserver, indem Sie den folgenden Befehl ausführen. `ng serve --host my-qs-app.net --port 4200 --ssl --ssl-key "./src/my-qs-app.net-key.pem" --ssl-cert "./src/my-qs-app.net.pem" -o` Dadurch wird Secure Sockets Layer (SSL) mit dem benutzerdefinierten Zertifikat aktiviert, das Sie zuvor erstellt haben. Wenn der Build abgeschlossen ist, wird ein Browserfenster geöffnet und Sie können Ihr eingebettetes QuickSight Dashboard anzeigen, das lokal in Angular gehostet wird.	App-Developer

Zugehörige Ressourcen

- Angular-Webseite
- Einbetten von QuickSight Daten-Dashboards für anonyme (nicht registrierte) Benutzer (Dokumentation) QuickSight
- QuickSight SDK einbetten
- Tool mkcert

Zusätzliche Informationen

Wenn Sie Windows verwenden, führen Sie das Befehlszeilenfenster als Administrator aus und konfigurieren Sie mit dem folgenden Befehl, dass immer `my-qs-app.net` zu Ihrem lokalen PC umgeleitet wird.

```
echo 127.0.0.1 my-qs-app.net >> %WINDIR%\System32\Drivers\Etc\Hosts
```

Mehr Muster

- Greifen Sie über eine ASP.NET Core-App mithilfe von Amazon Cognito Cognito-Identitätspools auf AWS-Services zu
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- Automatisieren Sie die Identifizierung und Planung von Migrationsstrategien mithilfe von AppScore
- Erstellen Sie mithilfe von DevOps Praktiken und AWS Cloud9 eine lose gekoppelte Architektur mit Microservices
- Erstellen Sie mithilfe von AWS Amplify eine serverlose mobile React Native-App
- Erstellen und testen Sie iOS-Apps mit AWS CodeCommit CodePipeline, AWS und AWS Device Farm
- Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog
- ???
- Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale EC2-Instances bereit mit CodePipeline
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2-Instances
- Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Stellen Sie mit Amazon ECR und AWS Fargate Java-Microservices auf Amazon ECS bereit
- Stellen Sie Java-Microservices auf Amazon ECS mithilfe von Amazon ECR und Load Balancing bereit
- Bereitstellen von Java-Microservices auf Amazon ECS mithilfe von AWS Fargate
- Entdecken Sie die Full-Stack-Entwicklung von cloudnativen Webanwendungen mit Green Boost
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Go-Webanwendung mithilfe der binären Methode zu AWS Elastic Beanstalk

- Migrieren Sie mithilfe von AWS Transfer for SFTP einen lokalen SFTP-Server zu AWS
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Migrieren Sie mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie OpenText TeamSite Workloads in die AWS-Cloud
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS
- Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 EC2-Linux-Instance aus
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein
- Verwenden Sie die Network Firewall, um die DNS-Domänennamen von der Server Name Indication (SNI) für ausgehenden Datenverkehr zu erfassen
- ???

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.